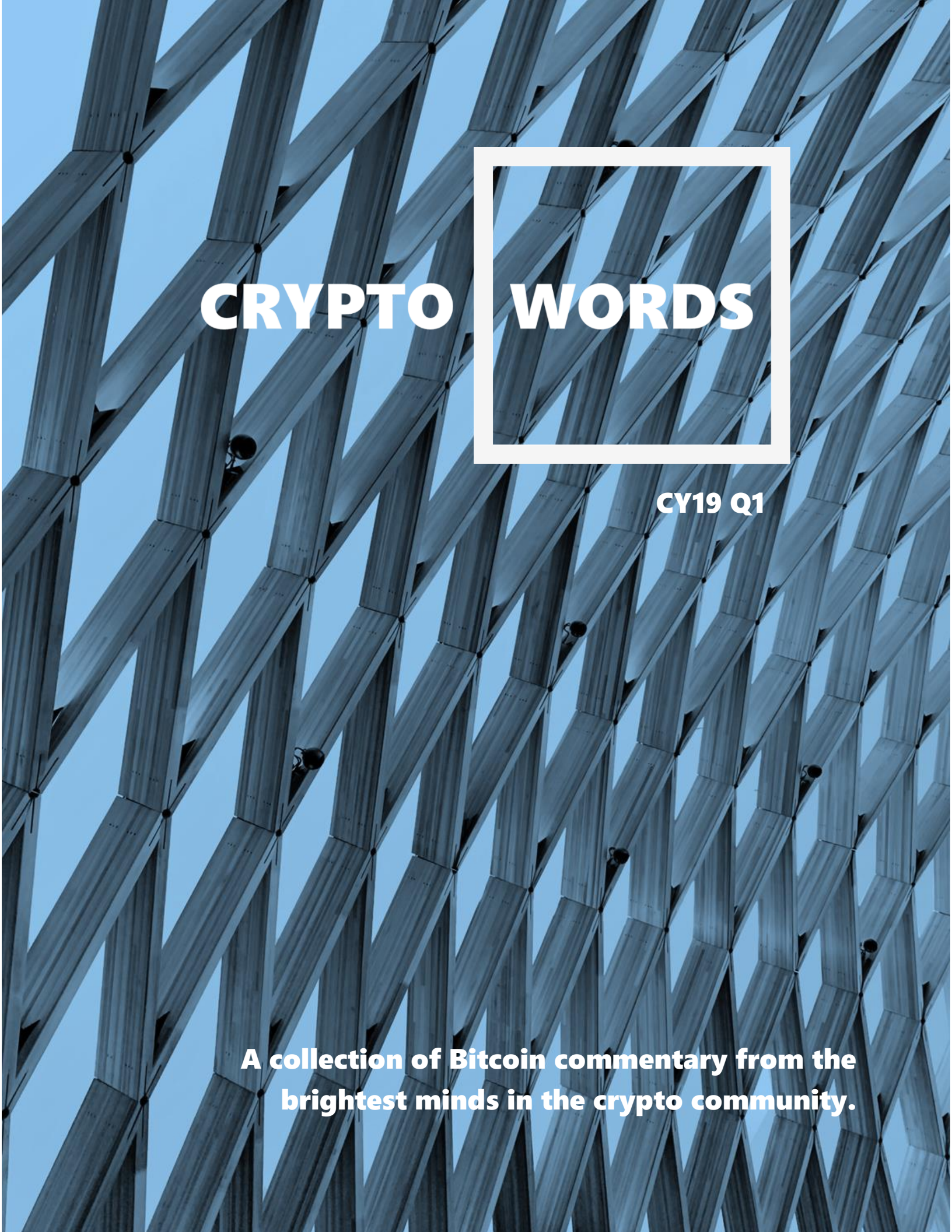




CRYPTO WORDS

CY19 Q1

**A collection of Bitcoin commentary from the
brightest minds in the crypto community.**

Contents

Goals and Scope	3
Crypto Theses for 2019	4
Cryptocurrency: The Canary in the Coal Mine	24
Tweetstorm: Bitcoin's 10 Year Anniversary as told by Vijay	27
Deconstructing Decentralized Exchanges	30
Planting Bitcoin—Species (1/4)	46
Planting Bitcoin - Season (2/4)	57
Planting Bitcoin—Soil (3/4)	66
Planting Bitcoin - Gardening (4/4)	70
Bitcoin: Winner Takes Most or Winner Takes All?	78
Maker Dai: Stable, but not scalable	86
Unpacking Bitcoin's Assurances	91
96 Theses for Crypto in 2019	99
Tweetstorm: Bitcoin as SoV	119
Are Crypto Lending And Institutional Custody Good For Crypto? First Principles	125
Quantum Narratives	131
Maker Investment Thesis	138
Grin and the Mythical Fair Launch	142
Money, Bitcoin and Time: Part 1 of 3	147
Money, Bitcoin and Time: Part 2 of 3	180
Money, Bitcoin and Time: Part 3 of 3	222
Against Szabo's Law, For A New Crypto Legal System	247
In Defense of Szabo's Law, For a (Mostly) Non-Legal Crypto System	259
A Conflict of Crypto Visions.....	271
Why Blockchain Differs From Traditional Technology Life Cycles	289
Blockchain Privacy: Equal Parts Theory and Theater	297
Why Monetary Maximalism could fall short of expectations.....	310
Politics, Power & Protocols	316
Demystifying Blockchain Not Bitcoin.....	321
Bitcoin is a hedge against the cashless society	336

Security Budget in the Long Run	340
Why Crypto is the Future and How it is Essential to us All.....	352
The Defensibility of Middleware Protocols.....	354
Bitcoin Delta Capitalization.....	357
Rehypothecation: BTC's path to becoming king of collateral.....	364
Tweetstorm: Power and Money.....	372
Cryptonetwork Governance as Capital	375
There is no such thing as decentralised governance	379
A Primer on Bitcoin Investor Sentiment and Changes in Saving Behavior	386
Bitcoin's Incentive System or When The Stars Align	397
Crypto Governance: The Startup vs. Nation-State Approach.....	401
Markets Are Eating The World.....	408
The Best Time to Buy & Build Tokens.....	436
Heterodox Economics and the Rise of Blockchain	445
Bitcoin Timestamp Security	462
What Do Wyoming's 13 New Blockchain Laws Mean?	470
Tweetstorm: Economic History.....	478
Why digital tokens need better tax treatment	479
Bitcoin Has a Branding Problem—It's Evolution, Not Revolution.....	482
The three core concepts of crypto	492
An Introduction to Blockchain Finality.....	494
Privacy and Cryptocurrency, Part I: How Private is Bitcoin?	500
Tweetstorm: Developer Activity	521
On Value Capture At Layers 1 and 2.....	529
Disclaimer:.....	535

Goals and Scope

Crypto Words is a quarterly journal of cryptocurrency, or crypto, established February 13, 2019. Its purpose is to document and advance commentary and research in disciplines of particular interest to the crypto community. The journal is broad in scope, publishing content from original research, essays, blog posts, and tweetstorms from a wide variety of fields, especially governance, technology, philosophy, politics, and economics, but also legal theory, history, criticism, and social or cultural analysis. Its broader mission is to capture the conversations and think pieces in the crypto space for current and future researchers. *Crypto Papers* hopes to continue and expand the tradition established by publications such as the [Journal of Libertarian Studies](#) and [Libertarian Papers](#).

History

There exists a gap in crypto publishing. For authors with commentary and scholarly papers on crypto topics, the choice of publication outlets is relatively limited. The number of journals that serve as outlets for crypto research is in any event too small, as the number of crypto thinkers continues to grow with every market cycle.

This generation of crypto thinkers have limited places to submit thought pieces for publication. Content is scattered across the web, and in some cases behind paywalls which prevent the free flow of information. With the advent of the Twitter and blogging, authors also now have the option of self-publishing: they post the content to their own site or some private site, link it in a blog post, or post a working paper. But this is obviously not the best way to document and publish. What is needed is a journal that takes full advantage of the possibilities of the digital age as a go to resource for think pieces in the crypto space.

Enter *Crypto Words*. Published independently, *Crypto Words* is a quarterly journal that welcomes submissions on a range of topics of interest to the crypto community. In addition to conventional research articles, we welcome review essays blog posts, tweets as well as papers in other formats, such as distinguished lectures. Finally, wherever possible, content on this site is licensed under a [Creative Commons Attribution 4.0 License](#). Authors retain ownership without restriction of all rights under copyright in their articles. *Crypto Words* is open access, and we encourage readers to “[read, download, copy, distribute, print, search, or link to the full texts of these articles...or use them for any other lawful purpose.](#)” We want our ideas read, spread, and copied.

Crypto Theses for 2019

My thoughts on the state of crypto in 2018 and where we're headed

By [Arjun Balaji](#)

Posted January 1, 2019

Tags: predictions, Bitcoin, Ethereum, Stablecoins, funds, regulation

What exploring cryptocurrencies in 2018 feels like.

As another year wraps up, I started writing an email to close friends and investors on the “state of crypto” and my forecasts. As it got longer, it turned into this sprawling post. A few notes:

- This write up contains wide-ranging theses and obvious biases (my own) and is by no means authoritative. Please don't nitpick.
- Where I make predictions, I try to be as specific as possible (inspired by [SlateStarCodex's format](#)). Not all predictions are quantifiable. Some will be off and many will likely be directionally incorrect. That's OK.
- Unless otherwise specified, my criteria for a liquid, actively-traded project “dying” is either (1) < \$100k volume/\$20m market cap or (2) primary development abandoned, whichever comes first.
- None of these predictions are normative; in many cases I see momentum in products or approaches I consider fundamentally flawed. *C'est la vie*—this is an attempt at a descriptive 2019 outlook.

Index

- Bitcoin
- Ethereum
- Other Tokens
- Private Projects
- Stablecoins
- Crypto-funds
- Product Potpourri
- Crypto Companies
- Regulation
- Closing thoughts on prices and adoption

Bitcoin

- 1) After a strong launch in 2018, I see Lightning Network growth continuing into 2019. I predict the number of Lightning nodes with channels will be $\geq 10,000$ from [~2,100 now](#) (60% confidence) due to the proliferation of node hardware and hosted solutions (e.g. [Nodl.it](#), [Casa's node](#)) and easy-to-deploy GUIs like Pierre Rochard's [node launcher](#). I predict network capacity will increase even more from ~\$2m notional to $\geq$ \$25m+ notional (75% confidence) due to the lifting of maximum channel limits, dual-funded channels, etc.
- 2) At least one major exchange will launch a Lightning Network hub for their users as confidence in the stability and security of the network grows over 2019 (50% confidence). If this occurs, my money is on Binance given their iteration speed and product chops or Coinbase, due to increased focus on adoption and "usage" of cryptocurrencies. I'm particularly excited about Cash App's potential here given 1) they're a business that understands Bitcoin 2) Jack sees Bitcoin as [a path to "financial inclusion"](#) and 3) Jack's [investment in](#) Lightning Labs' 2018 seed round.
- 3) A working implementation of [Schnorr signatures](#), for which Pieter Wuille released a [draft BIP](#) in July, will make its way into Bitcoin via soft fork by the end of 2019 with $\geq 5\%$ node adoption (75% confidence).
- 4) Low volatility and lower prices always attracts concern trolls and people who believe they can "change" Bitcoin for the better. **The last two years have seen a lot of forks where the codebase is changed but the UTXO set is kept intact. In 2019, I expect to see the opposite: forks with technology kept intact (to merge future upstream changes) where the monetary policy or UTXO set is modified;** an example being the Zclassic team forking Zcash to remove the Founder's Reward). I predict 2019 will see a major fork proposal from Bitcoin OGs "fixing" post-block reward fee market sustainability either by re-appropriating Satoshi's Bitcoin (e.g. my [tongue-in-cheek tweet-proposal](#) for "Bitcoin Freedom") or by adding predictable, low inflation in favor of the fee-market (50% confidence).
- 5) 2018 was a big year for Bitcoin privacy and fungibility R&D, with proposals for [Taproot](#) and [Craftroot](#) from Gregory Maxwell in Q1, a [draft BIP](#) for the [Dandelion protocol](#) in May, and an emergent path for a soft fork upgrade to Schnorr-based signatures. By the end of 2019, there will be a clear roadmap for "good enough" fungibility and privacy on Bitcoin's base layer across a meaningful set of trade-offs (e.g., speed, confidence level, etc.) (50% confidence).
- 6) 2018 saw [plenty of promising experiments](#) building products around, with, and on top of Lightning. I anticipate 2019 will see significantly improved UX for developers who want to build with Bitcoin, including [web3/Truffle-like](#) Javascript wrappers,

hosted node services, better docs, tutorials, etc. which makes me very excited about the potential for new products.

Ethereum

7) 2018 was a big year for proof of stake research with [June's deprecation](#) of [EIP 1011](#) (Hybrid Casper FFG), scrapping the hybrid PoW/PoS step in favor of moving to pure PoS. The next phase for Ethereum—first termed *Shasper* (Casper + Sharding), now called *Serenity* (Ethereum 2.0)—has [six distinct phases](#), which stretch over several years. There are 8+ dev teams working on independent implementations including:

- ChainSafe Systems, building a [JS implementation](#) called Lodestar
- 50-person ConsenSys-backed PegaSys, building an [enterprise-grade implementation](#) in Java
- An independent group called Harmony, building a [Java implementation](#) based on the original EthereumJ client
- Parity Technologies, building an [Ethereum 2.0 client](#) in Rust
- Prysmatic Labs, building a [Go client](#) (recently, Raul Jordan [announced](#) the team had full test coverage with the latest spec)
- Sigma Prime, building a [2.0 client](#) in Rust
- Status, makers of the Ethereum-based [messaging app](#), building the first [mobile-native client](#) in the language Nim
- Trinity, a team predominantly backed by the Ethereum Foundation, building [a client](#) in Python

Despite seeing major setbacks and changes to the Ethereum 2.0 roadmap, I think the first phase will ship some time in Q4 2019 (*70% confidence*), albeit with friction.

8) Augur, whose launch everyone awaited with bated breath, seems to have gained little traction (outside of niche markets around the election). I suspect it will be the breakout dApp of 2019, leaping from [~\\$1.5-2m notional at stake](#) to ≥ \$10m (*70% confidence*). My bullishness is due to (1) a full year elapsing with a working product (2) improved UX/choice of clients (3) increased brand awareness (4) demand in the market for a non-custodial prediction market (5) stablecoin integration and (6) better market-making and liquidity provisioning.

9) The “crypto-collectibles” narrative which gained major steam in Q1/Q2 (peaking in March’s [\\$12m raise for Cryptokitties](#)) will lose traction despite the orthogonal interest for tradable in-game items. While collectibles [are interesting](#), they feel like a solution looking for a problem (though worth noting: I’m not a tastemaker) and gamer adoption feels like a pipe-dream as companies are unlikely to replace their existing monopolies. I suspect several of 2018’s niche “X-for-Y” Cryptokitties imitators that are less well-funded will shut down next year (*85% confidence*).

10) Despite the hype going into the new year, consumer adoption of decentralized exchanges (DEXs) have materially lagged expectations. Relayers leveraging Ox—viewed by many as the best exchange protocol—in aggregate have traded < [\\$2m notional](#) most days in 2018. I predict December 2019’s aggregate volume on Ox will lag a single day’s volume from Coinbase (*90% confidence*). **The big problem with DEX adoption in 2018 is that it's unclear who the target user is.**

While non-custodial trading feels like a boon, the trade-offs presented (e.g. in matching/execution speed, the potential for front-running, decreased privacy, the difficulty of accounting, etc.) make it an unappealing product for institutional investors, not even considering the UX curve. Whether retail investor participation will be sufficient for long-term sustainability remains to be seen. In addition, many DEX protocols with fee-based tokens will get forked (like Ox has [by their top relayer](#)), though I predict we'll see a surge in cross-chain swaps and similar non-custodial trading options sans token.

11) A lot of early prominent projects promised new types of markets, e.g. for [computation](#) or [storage](#). Along with the “utility token” narrative, demand for these solutions appears dead, as it’s unclear whether (1) demand for un-censorable XYZ is compelling enough given increased cost relative to centralized alternatives or (2) any of these new marketplaces will be sufficiently bootstrapped to hit the economies of scale necessary for their adoption. Not a single one of the new decentralizing marketplaces promising to marshal distributed or idle resources pose a threat to AWS, Microsoft, Dropbox, etc.

12) I anticipate we’ll see major pushback from disenfranchised ETH miners, who will propose a contentious hard-fork (*60% confidence*). Ethereum’s roadmap is already relatively antagonistic to miners: January’s planned Constantinople upgrade (which, among other changes, reduces block rewards from 3 to 2) hurts miners currently at the margin, likely putting them out of business. While a supply reduction is generally bullish, the upgrade may be short-term bearish (given increased miner inventory sales) if it’s not already priced in.

13) “Governance tokens” will be less popular than ever by the end of 2019. To me, they appear misaligned incentive-wise: in practice, it feels like rational token holders should be oriented around (1) entrenching existing power structures (as original token holders have out-sized sway in future protocol decisions, including future value-capture design) and (2) maximizing token value rather than what’s often cited as the goal (maximizing token *utility*). The excitement around the governance token (e.g. “We don’t need to worry about value-capture, we just need to build something worth governing.”) was a by-product of a never-before-seen crypto bull market and will warrant meaningful skepticism in 2019 (*60% confidence*).

14) On the face of it, decentralized finance (a.k.a. “DeFi” or “Open Finance”), a dominant narrative of Ethereum in 2018, is compelling to me in spite of my Bitcoin bias. A goal of the cryptocurrency movement has always been to increase financial inclusion and the core premise of the “DeFi” movement—to provide crypto-native financial products to the unbanked—has obvious appeal. However, I don’t understand what product market fit looks like for the vast majority of “DeFi” products.

If these products (in many cases, novel non-custodial derivatives or leverage-oriented lending products) are designed for institutions, I struggle to understand how they’ll achieve product market fit for many of the reasons posed in 10 on DEXs.

Bootstrapping liquidity will be *extremely* difficult (i.e., I don’t want to trade an exotic non-custodial derivative with no liquidity and it’s unlikely a marginal trader will want to do the same—the classic chicken-and-egg problem). If these products are designed for retail investors, I don’t understand the product market fit either. The long-shot thesis may be that the globally unbanked are looking for easy entry points that DeFi can solve, e.g. exposure to US capital markets/equities with synthetic on-chain [CFDs](#), but I am doubtful. Most consumers in the world don’t have meaningful savings, mirroring Vanguard-type indices or more complex derivatives doesn’t feel like the right entry point for global adoption.

I believe some of the US-based teams working on the DeFi stack are taking on material risk and will face regulatory scrutiny in the US (70% *confidence*) given their move into structured products. This will test the runaway killer app of Ethereum: regulatory arbitrage (first with the offering of unregistered securities offerings and now with quasi-legal structured derivatives), as teams “move fast and break [the law].”

While engineers are discussing [“compounding financial primitives,”](#) I’m worried about compounding technical (or legal) risk.

Other Projects

15) Two years after pseudonymous Tom Elvis Jedusor posted a paper outlining the Mimblewimble architecture to the *#bitcoin-wizards* IRC channel, 2 different implementations, [Grin](#) and [BEAM](#), are set to launch in Q1 2019. Both subscribe to different design philosophies, from Grin’s Bitcoin-like immaculate conception to BEAM’s Zcash-like foundation model, in addition to differences in monetary policy, stance on ASICs, etc. I expect both will be meaningful in 2019’s privacy wars, with Grin seizing the lion’s share ($\geq 70\%$) of market interest in Mimblewimble (75% *confidence*). Though its monetary policy isn’t ideal for early adopters due to high early inflation, it wouldn’t surprise me if it finishes $\geq \$250\text{m}$ market cap (60% *confidence*).

16) Given both comments from Zooko about both [PoS](#) and the [Zcash Founder's Reward](#) and rumblings from the community, I think it's possible that (1) Zcash plans a multi-year transition to propose a move to a hybrid PoW/PoS system (50% confidence) or that (2) a change to the Founder's Reward (30% confidence) takes place. As the Founder's Reward runs out in 2020, with a lot of research and engineering work left, I can see a proposal to extend it (or lengthen the reward beyond 2020) emerging.

17) It's not a secret [I've been hoping](#) most un-differentiated “means-of-exchange” tokens (e.g. \$IOTA, \$DASH, \$BCN, \$XVG, etc.) will die for some time. With the exception of Litecoin (which has the benefit of an old brand, widespread integration, and Bitcoin “test-net” status) and Dogecoin (which will never die), I expect $\geq$ half these un-differentiated payment tokens will be flushed out over the next year (70% confidence) as (1) 2018's price action shows they are subject to the same volatility issues as Bitcoin (2) growth of the Lightning Network dampens need for a “faster Bitcoin” (3) they don't have interesting innovation keeping a large community engaged the same way other public blockchains do with privacy (e.g. Monero, Grin) or ecosystem products (e.g. Ethereum, EOS, Tezos).

18) From the days of the Silk Road, dark net markets (DNMs)—along with pornography—have been a hot bed for cryptocurrency innovation. DNMs have gotten [more sophisticated than ever](#), moving from centrally-run sites with single points of failure (e.g. DNS shut-down) to decentralized infrastructures, spider webs of Telegram chats and bots, and better reputation systems. There are still problems: bitcoins are still the pre-eminent cryptocurrency of choice (given lack of customer awareness) despite the lack of better, more private options and the fiat-to-bitcoin conversion is a honeypot for law enforcement agents.

It's no secret I don't think there are many real use cases of “blockchain” outside of quasi-legal applications. While it's directionally clear that the future of DNMs is in moving to a fully decentralized stack (with smart-contract-based escrows, etc.), the lack of privacy on most public blockchains makes this a pipe-dream for 2019. Despite this, DNMs serve as an important crypto mind virus entry-point for many—a painkiller rather than a vitamin.

19) With greater focus on the “fairness” of Bitcoin and other cryptocurrencies, it's inevitable we will see new distribution-focused blockchain experiments. While [I'm less enthused](#), 2019 will likely be the year a Valley-based blockchain project focused on the long-standing goal of “getting crypto in the hands of everyone in the world” comes out. This form of UBI (inb4 “universal blockchain income”) is compelling to many and will have some traction as cryptocurrency mind-share has exploded beyond its libertarian-anarchist roots to include ideologies across the political spectrum.

20) \$XRP, err, I mean Ripple Labs, Inc. will get a small fine/slap on the wrist from the appropriate regulatory authorities, who will finally confront the fact that [it's probably an unregistered security](#) (80% confidence). Thanks to the regulator-revolving-door, [Ben Lawsky](#) (a.k.a. Architect of the BitLicense: The World's Worst Crypto Regulation) is [now on their board](#). While it's unlikely anyone's going to jail, it's hard to see Ripple's egregiousness let them off scot-free.

21) Bitcoin Cash [split in 2018](#), with factions ABC and Satoshi's Vision (SV) emerging. While the ABC camp has kept the \$BCH ticker, BCHSV lives on. With Bitmain potentially seeing internal issues (rumored layoffs, balance sheet issues, IPO delays) and Craig Wright willing to [see "2014 prices"](#) to win, this could continue on despite the fact that no one cares. I'm more optimistic about Bitmain's business than most people, but think that Bitcoin's dominance v. both forks will grow from today (80% confidence). I also expect ABC's dominance v. SV (~64% right now) will grow to > 80% by the end of the year (70% confidence). Despite my qualms about Bitmain's strategic decisions, "Don't start a hash war with Bitmain" might be as prescient as "Never fight a land war in Asia."

22) 2018 was a big year for Bitcoin forks with Bitcoin's December peak sparking imitators like Bitcoin Gold (\$233m market cap), Bitcoin Diamond (\$140m market cap), and Bitcoin Private (\$41m market cap). They're all currently Top 25 in market cap and have survived everything from [51% attacks](#) and [exposés of covert pre-mines](#), but I think they're unlikely to stay in the top 25 by the end of the year (70% confidence, lest the crypto market's extreme inefficiency fails me).

23) Both EOS and Stellar have committed a significant amount of time to building out developer experience and core infrastructure over 2018. Despite [my skepticism](#) of their potential to be internet money, there's interest from some dev teams globally to interface with these networks [for decentralized applications](#). The groups hacking on both networks are extremely well-funded. While they aren't seen by many in the crypto cognoscenti as "legit" projects, some SV energy might push them to meaningful developer adoption (50+ launched dApps) in 2019.

24) I've been [whistling with schadenfreude](#) on "masternodes" for some time. They were the perfect bull market trade: lock up more and more coins as prices go up (even more right-tail vol thanks to the smaller float) but we haven't seen a true unwinding/liquidity crunch despite the drawdown. I would be very surprised if any masternode projects outside of DASH have the liquidity or community backing to extend life to 2020 (40% confidence... sigh).

25) [Token curated registries](#), once the hottest "crypto-economic primitive" on the scene, make less sense to me now than they did before 2018. They strike me as a prime example of 2017's excesses (and desire to tokenize everything). The model feels

extremely convoluted and it wouldn't surprise me to see the industry move away from the TCR en masse (60% confidence).

26) Formal on-chain governance, which saw significant hype in 2017 from projects like [Tezos](#), [Decred](#), and [Aragon](#) left a lot to be desired. While the goal of formal governance systems is to enable smooth upgrades with input from a range of stakeholders, most suffer from elementary issues, cementing plutocratic regimes rather than enabling open participation. Most experiments with formal governance feel primitive due to the lack of proper tooling (e.g. for anonymous voting). There were some new announcements, including Commonwealth Labs' [work with Edgware](#) (a chain on Parity Substrate) but the long-term viability of formal governance systems remains unclear. In 2019, I think we'll see some non-trivial core protocol decisions decided on-chain for the first time.

27) One thing to be more excited about: with more research in formal governance systems, DAOs could make a comeback over the course of 2019. Widely written off as a failed concept due to [The DAO](#), two years later, there are new attempts. One DAO launch which looked cool this year is the [Moloch DAO](#), which aims to contribute to Ethereum infrastructure and solve the tragedy of the commons problem in the ecosystem's open-source (infrastructure) development. I've [stated before](#) that "crypto projects should have a plan to dissolve into some future decentralized governance model." I see crypto projects re-architecting Swiss foundations into DAOs as the first potential "killer use case" and think we will see iterations of this in 2019.

Private Projects

Note: I'm not an investor in any of the projects or companies mentioned in this section.

28) Despite sustained drawdowns in public crypto markets, private valuations (particularly for projects coming from Silicon Valley) haven't quite adjusted. Fred Wilson [recently noted](#) the relationship between public market valuations in the equities market:

There is a big difference between the private markets and the public markets. They do not move in lockstep. For years now, the late-stage private markets have been trading at valuations that are well in excess of their public market comps. That is true for a number of reasons. First, private market investors have longer time horizons and are looking for a three to five year return, not an immediate one. Second, private market investors get a liquidation preference which in theory protects them from losses. **Finally, deals in the private markets clear in an auction like environment where the highest bidder wins the deal. All of these factors mean that a hot**

company can raise capital in the private markets at valuations well in excess of where they can raise capital (and trade) in the public markets.

Most compelling for crypto is the last argument: starved for alpha, [investors pattern-matched](#) to find “the next Ethereum.” While several crypto-funds still have these investments marked at cost, it’s hard to believe investments made at $\geq$ \$500m valuations (and in many cases, in excess of \$1b) will represent gains for investors when the broad public crypto-market has drawn down so significantly. In 2019, I expect that many teams will re-raise at lower valuations or see material drawdowns when listing (*90% confidence*).

29) Some of these networks include Dfinity, Hashgraph, Algorand, Filecoin, Ncent, Thunder Token, etc. I anticipate less than 50% of these networks will launch in 2019 (*70% confident*).

30) The last quarter of 2017 and the first half of 2018 saw sky-high private valuations thanks to a potent combination of new crypto fund/whale money and a path to liquidity that divorced fundamentals and due-diligence in favor of memes and FOMO. As fast paths to liquidity have all but disappeared, I anticipate we’ll see projects return to more “traditional” approaches to raising money (read: equity) and focus on protocol-adjacent business models rather than building new base-layer protocols.

31) A launch of [Handshake](#) ([technical overview](#)) could be an interesting 2019 development. Though I’m skeptical of their need for a token, replacing the ICANN root server is an interesting problem and it’s clear the current DNS/Certificate Authority system is broken. One potential 2019 development: Handshake serves as a crude but effective solution for sites with regulatory or speech-related risk, which is enough to serve as an effective bootstrapping mechanism.

32) One thing I’m not looking forward to in 2019: the battle of messaging app crypto-tokens, with Telegram (TON), Signal (Mobilecoin), and even Whatsapp jumping into the fray. While none of them are interesting as a potential non-sovereign money competitor, I’m most interested in seeing what Facebook does: a [stablecoin designed for remittance](#) could make a meaningful impact while on-boarding millions of people to the cryptocurrency UX (as well as normalizing it in India, a country which [has had 2018 legal bouts](#) around Bitcoin). I’m least excited for Telegram Open Network, who had a [red-hot \\$1b sale](#) on the backs of crypto mania, Telegram’s traction, and many many pages of techno-babble.

Stablecoins

33) 2018 was definitely “year of the stablecoin” with Paxos Standard’s [PAX](#), Gemini’s [GUSD](#), Circle’s [USDC](#), Carbon’s [CUSD](#), and TrustToken’s [TUSD](#); though none of these

are true decentralized stablecoins (I prefer the term “price-stable asset backed token” or “fiat-coin” if that’s a mouthful).

Since these tokens allow traders to treat exchanges like banks, it should be no surprise that [they are under KYC/AML-scrutiny](#), like banks. **Fiat-coins are not permission-less**, though [aggregating demand for the product](#) at the exchange-layer makes perfect strategic sense for exchanges. Even the briefest taint of an *unsavory* transaction can charge Tyler and Cameron to personally shut down your account.

Holding fiat-coins leaves you at the whim of the issuer to control your financial fate: we’ve just swapped one God for another. While [Tether dominance has fallen](#) to new lows due to concerns over credit risk and the emergence of these new projects, it’s unclear what product market fit for fiat-coins looks like. Is the use-case as an intermediary safe-haven or settlement currency for traders? Is it a new “digital dollar” with its own ecosystem of products?

In 2019, I anticipate Tether’s dominance of the fiat-coin ecosystem dips below < 50% (75% *confidence*) with total fiat-coin (counting TUSD, USDT, USDC, PAX, GUSD) exceeds 4b in market-cap from ~2.5b now (80% *confidence*).

34) Despite my reservations about the long-term viability of the model, [MakerDAO](#) saw serious growth in 2018 (with [~1.8m ether locked](#) as of this post). While the system is robust—a by-product of excess collateralization in the system (currently ~370%)—use generally seems limited to demand for margin in ether, though the team has shared other [use cases for CDPs](#). Continued deposits of ether in CDPs [have affected ether price](#), it wouldn’t surprise me to see ether in CDPs exceed 3% of total ether in 2019 (60% *confident*) though less volatile collateral or the emergence of centralized options like [Compound Finance](#) may be more appealing.

35) After marquee stablecoin project Basis [returned money to investors](#), we lost one of the most interesting experiments in cryptocurrencies. Is it possible for a group of venture capitalists and clever twenty-somethings to bootstrap a price-stable currency based purely on belief (spoiler: probably not for now)? Despite the set-back, teams like [Reserve](#) are working on similar [seigniorage shares](#) models with plans on decentralizing over time. I think it’s unlikely we see a a seigniorage shares-based stablecoin project launch with > \$1b in total issuance in 2019 (80% *confidence*).

36) Fear over Tether’s backing was higher than ever in 2018 with concerns about [banking relationships](#), [enablement of price manipulation](#), and a constant [stream of concerns](#) over a proper “audit” of funds (though this may be [impossible to provide in any conclusive way](#)). The year ended with a [Bloomberg story](#) hinting that all the reserves may in fact be there. I predict it’s highly likely Tether in fact has all the US dollar deposits they claim they do (85% *confidence*) but that due to other investigations around criminal activity (e.g. money laundering, market manipulation,

etc.), consumers may have their funds locked by authorities in a long withdrawal process, [similar to online poker sites](#) after the infamous “Black Friday” (30% confidence).

Crypto-funds

37) My favorite fundamental indicator is still price action. Earlier this year, [I said](#) about crypto funds:

Early in the cycle, many progressive funds will allocate to managers to “get smart” on the space (see: Passport Capital, Union Square Ventures, a16z, Sequoia, and others allocating to crypto-funds). This comes out of a recognition that **the new asset class is different than the one that they're used to** but could potentially become much more relevant to their strategy ... As initial hype subsides, a second generation of capital allocators will emerge who are more experienced, taking away capital from the gun-slinging fund managers who rode the first wave. It's highly unlikely that the very best fund managers in a new asset class were also the first to spot it. We're starting to see this now, with Matt Huang and Fred Ehrsam's new fund, a16z's newly announced crypto-fund, and several more unannounced funds raising money in today's crypto bear market.

This has roughly held up as new second-generation funds have raised from (1) more credible LPs [\[including the Yale endowment\]](#) (2) with longer lock-ups and (3) more credible GPs.

With that said, I think funding will slow down in 2019 given (1) lack of momentum in public crypto markets (2) limited investable opportunities given the size of the market and (3) proliferation of beta exposure vehicles. The third point is critical: **many of the largest funds are overweight BTC/ETH, with capital allocators paying excessive fees for beta** (particularly with long-only models). While experienced GPs will have no trouble raising and often argue that BTC/ETH allocation is a portfolio decision, I suspect many LPs will opt for exposure directly through low-cost single/multi-asset investment products.

38) With the blood this year, the opportunity for crypto fund differentiation finally emerged— though returns look less than stellar ([Vision Hill's benchmarking](#) was a positive development). More funds are starting to figure out where they “fit” in the landscape (e.g. fundamental long-only v. long/short v. “generalized mining” etc.) v. generically labeling themselves “crypto funds.” I expect we’ll see similar institutionalization in 2019 top-to-bottom of the entire crypto-fund pipeline, from back-office ops to custody. In addition, many funds will be one-and-done after the last year's price action and will see too many redemptions to continue (the death

zone AUM-wise is probably ~\$25m unless you skimp majorly on services/legal/salaries).

39) Concentration will become *en vogue* with consolidation of funds (due to shut-downs and re-allocation of LP capital) as “blue-chip” funds (of the fundamental long-only/long-short flavor) have heavy overlap with ownership in the same 20-25 names. I anticipate this will help greatly with decreased cross-asset correlation over the course of 2019.

40) Investing strategies from traditional capital markets like activist models, e.g. [Layer1's](#), have been extremely under-explored. While early models look something like Blockstream-meets-trading-firm and questions remain (e.g. is a model where wins are socialized but losses are not sustainable?), I'm excited about the development. **One activist model I'm particularly interested in seeing: a fund pursuing legal arbitrage to attempt to secure treasuries from projects where the aggregate value of treasury funds exceed market cap.** With the current market landscape, creativity is necessary.

Product Potpourri

41) I've been skeptical of enterprise blockchains and promised I wouldn't spend any more time on them after [my experience](#) at a meet up last year. That said, it looks like corporate interest in capital-b Blockchain is slowing with depressed crypto prices using things like [earnings call mentions](#) as a useful proxy. Who would've thought? Turns out investment in enterprise or “permissioned” blockchain efforts were only cool while crypto prices (and corporate interest) was mooning.

In many cases, we're in Year 3 or 4 of the “Blockchain, not Bitcoin” experiments that started in the aftermath of the 13-14 Bitcoin bubble. We've already started to see the first casualties as [noted execs](#) are abandoning projects ranging from R3, Hyperledger, and other efforts from Microsoft, IBM, etc. I expect most of these teams to see layoffs or shut down in 2019 (75% confidence) on the back of limited adoption and even more limited utility.

42) A positive development of 2018 is the number of new, cheap node-in-a-box hardware products, ranging from boutique consumer products like [Coinmine's](#) to barebones hardware like [Nodl.it's](#). While costs range wildly based on feature-richness and form factor and there are concerns about commodification (from an investors' perspective), this is undoubtedly good for users who want self-sovereignty when interacting with public blockchains. The average industry cost for a full-node box should trend to ~\$150 USD (though it can be run even more cheaply [on a Raspberry Pi](#)).

43) Security tokens saw extreme hype going into 2018 with [hundreds of millions](#) of dollars in investment to exchanges, token standards, issuers, and more. [My thesis remains steady that nearly all value generated by tokenized securities will be captured by 1\) underwriters 2\) asset holders \[who benefit from the illiquidity premium\] 3\) early investors in STOs who can arbitrage sophistication 4\) infrastructure providers.](#)

A little STO inside baseball: as it stands, the space has little traction and is teeming with underwriters—who often stand to *directly* benefit from the deal from advantageous pricing as principal investors *in addition to* underwriting fees—hyping up future retail investor interest. Incentives are often misaligned.

Despite grandiose claims of \$80T TAMs, I’m skeptical that security tokens have found investor-market-fit. It’s unclear who the “right” audience for STOs is. It’s not institutions, who lack any effective way to hedge or manage risk of these long-only products (or take custody, for that matter). Howard Marks' comment in a [2015 letter on liquidity](#) comes to mind:

It’s one of my standing rules that “No investment vehicle should promise greater liquidity than is afforded by its underlying assets.” If one were to do so, what would be the source of the increase in liquidity? Because there is no such source, the incremental liquidity is usually illusory, fleeting and unreliable, and it works (like a Ponzi scheme) until markets freeze up and the promise of liquidity is tested in tough times.

With investor-market-fit uncertain, a potential macro cycle shift, and lack of institutional-grade infrastructure, and the roadmap to deployment looking uncertain, I’m skeptical the world will be tokenized in 2019. I would be surprised if the actively traded market of (novel) tokenized securities exceeds \$2b in the next year.

44) There are a wide range of different institutional-grade custody offerings funded in Q4/Q1 of last year set to launch in 2019, either with direct self-custody products or by providing the technology back-end for other custodians. I suspect we’ll see a major custody product offering from a traditional sell-side firm (excluding Fidelity Digital Assets) by the end of the new year (*60% confidence*). I also think we’ll see the first crypto-native custody solution be granted broker-dealer/qualified custodianship status, a major step in the maturation of the asset class (*75% confidence*).

45) I’m bullish on efforts like [Lolli](#) and [Cash App](#), beautiful products from companies who grok consumer UX and are making meaningful strides to help consumers understand and buy, earn, move, and store cryptocurrencies directly. **I suspect these and new consumer products will lead to millions of people interfacing with a cryptocurrency for the first time in 2019.**

Crypto Companies

46) As [described earlier](#): Coinbase is fighting a multi-front war. Fidelity, Gemini, and a slew of Wall St. firms are competing for any institutional business. In the event there is an STO battleground to fight over, tZero, Templum, Harbor, Securitize, ASX/Malta/Gibraltar, and others are in fray. The profitable consumer business faces constant pressure from Robinhood, Circle, and Binance.

While their regulatory moat remains strong, Coinbase appears to be going into 2019 heavily focused on [increasing consumer usage/adoption](#) and [aggressively expanding token listings](#) (perhaps motivated by dampened trading volume in a crypto bear market). In 2018, Coinbase launched both their [venture arm](#) and [expanded their M&A activity](#) (acquiring Paradex, [Earn.com](#), and acqui-hiring many smaller teams) in an effort to become the “Google of crypto.”

While I’m skeptical of the strategy to list tokens with dubious utility other efforts, a few facts remain true going into 2019: (1) Coinbase is still synonymous with “place to buy crypto” for millions of consumers. (2) They have a war chest to rival many of the largest companies in the space while (3) having a sizable regulatory moat in the US and (4) top-of-the-line product teams (at least relative to other crypto companies).

In 2019, I expect to see continued expansion into crypto-native consumer products that allow consumers to interface directly with protocols in addition to improvements to exchange infrastructure (as the bear market offers ample time to prepare for the next cycle of adoption).

Coinbase has already launched their Earn.com-based “education” service. Other product moves from them could include: a more consumer friendly wallet ([Toshi](#) refreshed) which allows customers to stake and interface with dApps/Lightning, increased focus on lending (Coinbase is a bank after all), and productization of the OTC workflows as they [expand their institutional presence](#) with sales and trading (other OTC desks lack the product and engineering chops).

I also strongly suspect that Coinbase shifts to a more Bitcoin-friendly position in 2019.

47) On the subject of exchanges, after a year spent acquiring [fastest unicorn ever](#) status, I suspect Binance will have a much tougher 2019. What Binance has in engineering chops [they forego in regulatory attack surface area](#).

I suspect 2019 will see (1) Binance more comprehensively close access to US participants (75% confidence) after facing regulatory action (2) launch a full-on DEX (80% confidence) (3) launch multiple global fiat on-ramps (80% confidence) while (4) becoming the dominant exchange in Africa (90% confidence). While regulatory action will slow down growth from prospective US customers, I doubt they’ll see a

full shut-down given their Malta domicile (30% confidence). I would peg a prospective shutdown of BitMEX (given shades of market manipulation/excess leverage) significantly higher (70% confidence).

48) 2018 was the year of the shitty exchange tokens following the runaway success of Binance's token in 2017 (success always breeds imitators), with many resorting to shady "transaction mining" from companies like [Fcoin](#), [catex](#), [ZBC](#), [coinall](#), [coinex](#), [Cashierest](#), and [abcc](#).

This is a new type of scam: instead of taking fees from customers, these shady third-tier exchanges choose to give back the notional value of trading fees to customers in the form of their native exchange token. This is clearly unsustainable, with a couple of these businesses already shutting down.

Many of these native tokens saw huge jumps in initial volumes from curious traders but are now cesspools of wash-trading given easy gamification. Not only does offering a token represent a serious liability, it represents major counterparty risk as the exchange-token scheme could collapse at any moment. I suspect $\geq 75\%$ of the exchanges offering these trans-mining schemes will shut down in 2019 (85% confidence).

49) Consensys has had a rough year with major drawdowns in ether and other ERC-20 tokens (held in treasury/launched by Consensys subsidiaries), ending the year with [lay-offs](#) and plans of [spinning off](#) most of their less-favorite children. This is a bearish sign and I suspect the majority of projects that are spun off will have trouble raising follow-on financing due to cap-table concerns and broader theses shifts in the ecosystem.

50) Given Consensys' contributions to Ethereum infrastructure (including [Infura](#), [MetaMask](#), [Truffle](#), etc.), it raises meaningful questions about the sustainability of open-source development and how important non-core protocol-adjacent work (e.g. developer infrastructure, etc.) will be funded. Historically, we've seen a few different models:

- A company like [Blockstream](#) or [Lightning Labs](#) (taking cues from Docker, Redis Labs, SUSE, and others), focused on delivering value-added services on top of an open-source protocol. While **their primary orientation is profit-seeking, a large part of the company's resources is committed to maintaining the project**. Historically, this has been seen as unsuccessful (if not on an absolute basis, certainly a questionable risk-adjusted bet) for clear reasons: (1) It was unclear for many years what, if any, services would emerge as potential profit centers. (2) Unlike other new technologies (e.g., a web framework or database), a bet directly on the technology, without layered execution risk, is possible.

Despite this, some of the largest contributions to Bitcoin have come from similar teams, indicating that their work was integral.

- An exploratory research group like [Chaincode Labs](#) (which I believe is entirely self-funded), which has free reign to work on anything they'd like. This sort of patronage model allows for intellectual freedom, including hosting "mercenary" contributors or community members like tenured professors. While the freedom is optimal, funding these types of initiatives is often quite difficult: it requires recurring charitable donation.
- A formal "foundation" which has wider-ranging set of responsibilities, including interaction with regulators, organizing the network launch, etc. This is—of course—sub-optimal and unlikely to be of any interest to communities like Bitcoin's (who have historically pushed back against any formal "Foundation" designation given the many charlatans who've attempted to profit).
- Direct fees from a crypto-network used to support core protocol and protocol-adjacent work, the approach taken by teams like Decred and Zcash.

While economists like Elinor Ostrom have tried to [answer this question](#) in other domains, I suspect we'll see significant iteration on different funding models in 2019.

51) While the news of [Bakkt's](#) launch (delayed twice) and the announcement of [Fidelity Digital Assets](#) were eagerly promoted by the broad crypto-community, I suspect their Q1 launches will have less demand than expected with adoption trickling in over the course of the year. It remains ambiguous to me who the anticipated customer is for Bakkt's bitcoin-settled futures product. Fidelity's DNA [appears to be deeply-rooted](#) around Bitcoin's cypherpunk roots, they will go a long way to combating common worries around [rehypothecation](#) during the financialization of Bitcoin.

52) *[Disclosure: I'm an advisor to The Block.]* 2018 saw the emergence of a number of new media properties (and media-adjacent companies/projects) including [The Block](#), [Messari](#), [BREAKER](#), [Token Daily](#), and [TruStory](#). While they have various flavors of ideology and differing goals, they all go a long way to legitimizing coverage of an industry plagued with fake news, disingenuous PR, and blatant scams. While regulators have their hands full with low-hanging fruit, these companies are often the first to [expose foul play](#)—they will continue to play an important role in uncovering the deep underbelly of long-tail crypto projects as the industry continues disciplined self-regulation.

53) Bitmain, once the unstoppable inspiration of 1000 "mining is centralized" thought-pieces (a behemoth [staring at a \\$12b 2018 IPO price](#)), doesn't appear to be immune from crypto bear market woes. The bearish case for Bitmain is straightforward: they've suffered immensely from a costly bet on Bitcoin Cash (and an ensuing pissing contest, err, "hash war"), lost some top engineering talent (who are now competitors), and are victims of depressed crypto prices along with other

miners. Bitmain has lost technological superiority—their latest, the S15 (23 TH/s) has formidable competition from both BitFury's [Tardis](#) (80 TH/s) and Ebang's [Ebit 11+](#) (37 TH/s).

Despite additional rumblings that Jihan Wu and Micree Zhan will be replaced with new leadership, I believe Bitmain's obituaries are premature. 2018 saw many people come at the king, though some early competitors are [already shutting down](#) due to the difficulty and prohibitive cost of 7nm ASIC manufacturing. Bitmain may [never be Ghash](#) but shutting down this year feels like a long shot (85% confidence).

54) I've [been bearish](#) on Overstock (and tZero's) prospects for some time. I think it's highly likely that Overstock successfully spins out their retail business (85% confidence) by 2019's end but that their blockchain efforts continue to sputter given a lack of profitability and slower-than-anticipated adoption of security tokens.

55) After seeing the \$1b in revenue some OTC trading desks were generating in 2017, banks leapt at the opportunity to capture juicy spreads and generous commissions, most notably led (and later [supposedly shuttered](#)) by Goldman. I suspect demand for Wall St. offerings for spot BTC trading will be ~0 given the existing landscape of institutional-grade options (which execute the majority of spot bitcoin trading). It would surprise me if any tier-one bank opened an OTC spot or derivatives trading desk in 2019 (50% confidence).

56) A large exchange (top-10 in volume) will be hacked in 2019. The bear market is prime time for hackers, particularly with more fringe exchanges laying off some staff amidst difficulties (50% confidence).

57) As part of broader market consolidation in the bear market, I think we'll see strategic acquisitions by larger companies or early movers in both on-chain analysis (e.g. Chainalysis, Elliptic, Coinmetrics) and custody products like Anchor (60% confidence).

58) Rage over payment system censorship felt like it reached a tipping point in 2018 with Mastercard (downstream [via Patreon](#)), [SWIFT](#), and even [PayPal demonstrating](#) that payment networks like [other web-based messaging services](#) are susceptible to top-down decisions to cut off free flow of money at any point. Bitcoin can potentially catch a lot of these leaks as we saw with late 2018 examples from fringe social-networks [like Gab](#) or [controversial personalities](#) like Jordan Peterson. I anticipate this trend will continue into 2019.

Regulation

59) 2018 also saw many different proposals (from the BIS, IMF, and others) around central bank digital currencies (CBDCs) peaking with [this paper](#).

The core argument for CBDCs [some economists make](#) are that by moving private deposits to CBDCs, a more safe narrow-banking system emerges replacing the current commercial and private banking infrastructure (which in turn allows central banks *greater* control of the economy). Other economists like Ken Rogoff [have made historical arguments](#) in favor of moving to digital cash systems (phasing out large bills) citing both financial efficiencies and greater oversight into money laundering (and downstream crime).

Personally I find CBDCs terribly uninteresting, another attempt to extend to the financial system's Foucauldian panopticon. "CBDCs, not cryptocurrencies" is just the latest of the already-tiring "Blockchain, not Bitcoin" trend. However with the world largely trending towards digital payments, I think CBDCs in some form are inevitable though I doubt we see large-scale consumer-ready deployments in 2019 (75% *confidence*).

60) We've already started to see the first [regulatory actions](#) come to ICO teams in 2018, with the SEC going after low-hanging fruit, establishing a clear pattern through the process. While no large projects have faced serious regulatory scrutiny, I anticipate the SEC will shift focus here in 2019 with a top-25 project (by market cap) facing injunction (60% *confidence*).

61) 2018 saw more Bitcoin ETF proposals than ever with [SolidX-VanEck Bitcoin Trust](#), [ProShares Bitcoin ETF](#) (they also filed a [Short Bitcoin ETF](#)), [GraniteShares Bitcoin ETF](#) (corresponding [short ETF](#)), and others, including more esoteric multi-asset ETFs from companies like Bitwise Investments. Despite outstanding concerns over market manipulation of BTC spot prices, I think it's likely we see a Bitcoin spot ETF approved by the end of the year (70% *confidence*), with my bet on VanEck to grab first approval.

62) One place we've seen little regulatory action is with "crypto influencers" facing fines or other actions, though regulators have started [clamping down on celebrities](#). Naming names is rude, but this SHA-256 hash has my list of influencers that are more likely to get rekd, with a reveal coming in 2020:

a6c061624f97399d08fb58dbd23801ab9d03a9329128f5147a9873c9daf906a1

63) Along with excitement over CBDCs, I think it's likely some country (likely smaller) will announce a pilot or experiment around a blockchain-based identity system (50% *confidence*).

Some closing thoughts on prices and adoption

With this year marking the start of a crypto recession, the focus for many technologists has been around *adoption* and *usage*.

In my view, the only thing that can drive crypto *adoption* is (1) bitcoins or other cryptocurrencies serving as an escape valve for people who are in uncertain monetary regimes (and willing to stomach Bitcoin's volatility), e.g. Venezuela, Iran, etc., (2) people buying into the idea that Bitcoin is effectively a call option on becoming a future store-of-value, or (3) people buying the idea that Ethereum, Dfinity, Tezos, and other crypto-networks represent a radical shift in the way computing works ("Web 3.0") ahead of what will likely be a multi-year validation process.

There may be others, but those three things represent to me the majority of factors that could "drive crypto adoption in the short-term."

As people's interest fade and near-term sell pressure drops off (which we've seen over the last several months), we'll enter a prolonged phase of virtual boredom (read: this is right now) which lasts months, if not years, where many spend time speculating on what's "next" for adoption (post-13/14 cycle this was new protocols like Ethereum, merchant/payment processing tools, etc.) while the majority of people involved in the previous bubble leave.

I don't really worry about questions like short-term adoption drivers. People will buy cryptocurrencies for one of the reasons above, or they won't. Gradually as the market bottoms out, prices becomes more appealing and perhaps renewed interest leads to another cycle, serving a self-fulfilling prophecy. Or maybe the price dips below a point of "no confidence" (i.e., BTC prolonged < \$1k) at which point no one has faith and only HODLers of last resort are left (like we saw last cycle). Either way though, the digital sound money genie is out of the bottle.

As I've [noted before](#), **cryptocurrencies are still in the "risk basket" (along with venture capital) for institutional capital allocators**. Particularly considering a broader macro "risk off" scenario over the next 12-18 months, I doubt bitcoin prices will make new all-time-highs in 2019 (95% *confidence*) and think there's a strong chance we don't break \$8k BTC (60% *confidence*).

I think it's unlikely that BTC will be a crisis alpha in the next recession the way many people are hoping (I've also noted [my own signs](#) of late-cycle behavior). That said, the flight-to-quality to bitcoin and other "blue chip" cryptocurrencies will likely continue into 2019.

Either way, I'll be here studying, investing, and sharing my learnings. Whatever small role I can play in the experiments around non-sovereign money is among the most important projects I'll work on in my lifetime.

“Every day that goes by and Bitcoin hasn’t collapsed due to legal or technical problems, that brings new information to the market. It increases the chance of Bitcoin’s eventual success and justifies a higher price.”—Hal Finney

Perhaps we can use some of [Hal's ambition](#) going into 2019.



Cryptocurrency: The Canary in the Coal Mine

What Crypto Can Tell Us About Macro Markets in 2019

By [Jill Carlson](#)

Posted January 1, 2019

Over the last quarter, the market has rejected risk assets across the board in a sudden reversal of the year's trend. The S&P 500 erased its 9% gain over a matter of weeks in October. The Nasdaq index retraced from an 18% gain to end the year down 5%.

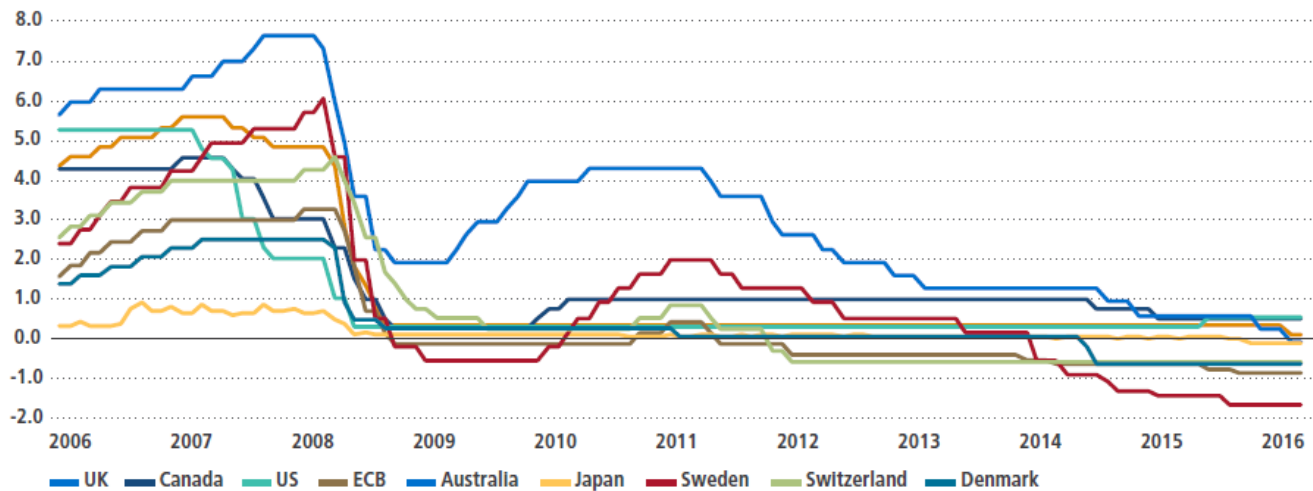
But no market has felt more pain recently than that of cryptocurrencies. The aggregate market cap of cryptocurrencies, which topped out at \$830 billion last January, has since crumbled to \$130 billion. Much of this unwind has occurred only in the last two months, with the crypto market as a whole getting marked down over 40% quarter-to-date.

The cryptocurrency market is admittedly miniscule relative to other asset classes. Cryptocurrency (no matter how big the drawdown) is unlikely to have any impact on broader markets any time soon. Bitcoin has demonstrated no substantial correlation to any other asset, whether equities or gold. Nonetheless, what has been happening with this nascent asset class over the last year may reveal some important macro trends.

Two years ago, at the end of 2016, the cryptocurrency market stood at \$15 billion in value. Trading volumes across all cryptocurrencies hovered in the double-digit millions. What led to the asymptotic spike in prices over the course of 2017? While it may be possible to point to certain headlines and technology developments as catalysts, most would probably dismiss the phenomenon as a speculative bubble. They may not be wrong in this characterization, but they may also miss the macro context in which all of this occurred.

We have seen many search for yield trades play out over the last 8 years. With central banks around the world pumping liquidity into the economy, traditionally risky assets have seen their premiums sucked out of them. Emerging markets stocks, bonds, and currencies have benefited from this trend. High beta equities, most notably in the tech sector, have boomed with the FAANG stocks leading the way. This trend has also driven money further out along the risk spectrum into alternative asset classes, ranging from art to cars to venture capital.

FIGURE 1: GLOBAL CENTRAL BANK RATES



Source: Bloomberg as of 17 October 2016

With rates like these, who needs hedges? Image from Pimco's 2016 Negative Interest Rate Report. <https://global.pimco.com/en-gb/resources/education/investing-in-a-negative-interest-rate-world>

The cryptocurrency boom of 2017 may have been the illogical conclusion of this global search for yield. It certainly followed this trend, starting as money poured into the relatively lower beta cryptocurrencies (like bitcoin and ethereum). Over time capital found its way into brand new assets as well, the products of initial coin offerings (ICOs) into which investors dumped an estimated \$20 billion in the last year and a half, often with little in the way of investor rights or protections. Talk about "risk on"...

But the story has changed since then. If you bought bitcoin at the peak last December and sold today you would be realizing an 80+% loss. Many of bitcoin's brethren, including many ICOs, have performed far worse with some cryptocurrencies getting marked down 95+% this year. The last major legs lower of this correction in October and November have coincided with the broader market sell off.

Perhaps cryptocurrency, the last mover on the way up, is the leading indicator of a broader market fall. If the cryptocurrency boom of 2017 was partly the result of the longest expansionary period the economy has seen in a century, perhaps the bursting crypto bubble of 2018 is the canary in the coal mine that the search for yield has run its course.

The recent downturn across asset classes has been blamed on a global growth slowdown, rising interest rates, and continued political uncertainty. Whether this

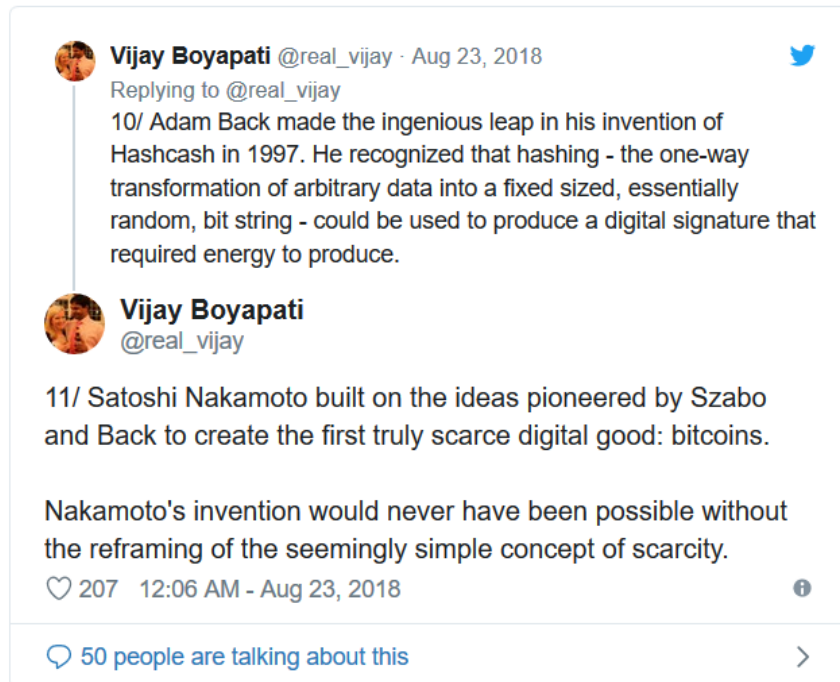
plays out in 2019 remains to be seen, but if it does, it will manifest first as capital leaves what it perceives to be the riskiest assets.

Tweetstorm: Bitcoin's 10 Year Anniversary as told by Vijay

By [Vijay Boyapati](#)

Posted January 2, 2019

1. 10 years ago today, in an unknown location, a mysterious figure whose identity is still unknown, tapped a key on his keyboard, spurring his CPU into action. In doing so, Satoshi reified his vision for a decentralized digital cash that he'd published 3 months earlier.
2. The fan in his computer began spinning to keep the CPU, burning from the burden of work it had been given, from overheating.
The CPU in Satoshi's computer was searching for a special pattern, much like a digital needle in a haystack, that would secure [#Bitcoin](#)'s first block.
3. Here is that needle:
0x000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f
It is the hash of Bitcoin's "Genesis Block", which created the first 50 bitcoins ever to be mined (by a quirk of Bitcoin's protocol these 50 bitcoins can never be spent).
4. With a brilliant leap of imagination, Satoshi had done what no one else had been able to do, and which many thought impossible. He had ingeniously incorporated [@adam3us](#)'s Hashcash design as a way of securing transactions on a network not controlled by anyone.
5. By burning energy in search of digital needles-in-haystacks, Satoshi's proof-of-work design allowed, for the first time ever, scarcity to be brought to the digital realm:



6. Since the creation of Bitcoin's genesis block on January 3rd, 2009 at 6:15pm (GMT), the Bitcoin network has seen the steady and remarkably reliable creation of blocks for a decade, allowing millions of people to store and transfer value without let or hindrance.
7. While many are obsessed with making price predictions about [#Bitcoin](#) in 2019, one thing we can actually predict with high certainty is that Bitcoin blocks will continue to be created approximately every 10 minutes with remarkable reliability.
8. As the Bitcoin network continues to function reliably well into the next decade, there will be near-universal confidence that it will be available forever, much as people believe the Internet is a permanent feature of the modern world.
9. Slowly but inexorably the world's population will come to recognize the benefit of opting out of the status quo monetary order and returning to a world of true individual financial sovereignty.
10. 10 years hence we will look back at the now 20 year old Genesis Block and recognize its creation as the beginning of a new monetary epoch. With the tap of a key on his keyboard Satoshi set in motion a sequence of events that set our world financially free.

Addendum: If you're interested in learning more about the genesis block I highly recommend [the fantastic 2013 post](#) by the brilliant @SDLerner.

Deconstructing Decentralized Exchanges

The goal of this Essay is to explain the architectural structure of decentralized exchanges, and the performance and security tradeoffs associated with various architectural choices.

by [Lindsay X. Lin](#)

Posted January 5, 2019

Introduction

Decentralized exchanges are becoming a critical tool for purchasing and selling an increasing percentage of cryptocurrencies. The term “decentralized exchange” generally refers to distributed ledger protocols and applications that enable users to transact cryptocurrencies without the need to trust a centralized entity to be an intermediary for the trade or a custodian for their cryptocurrencies.

Decentralized exchanges provide a number of important benefits, including (1) lower counterparty risk (i.e., no need to trust a centralized exchange to secure and manage private keys), (2) the potential for lower transaction fees, and (3) a more diverse array of trading pairs that can unlock access to riskier or less liquid cryptocurrencies. As demand for these features increases, decentralized exchange technology may witness tremendous growth in usage, development, and adoption within the next couple of years.

Additionally, decentralized exchange usage is being fueled by concurrent regulatory and industry trends, including (1) a surge in the quantity of distinct cryptocurrencies that makes comprehensive listing impractical, (2) regulatory risks of listing cryptocurrencies on centralized exchanges, and (3) users’ desire to avoid centralized exchanges’ Know-Your-Customer requirements for more private and less censorable transactions.

Decentralized exchanges can differ dramatically in terms of technology, trustlessness, security, legal implications, economic implications, and more. These differences render some exchanges more or less suitable for specific use cases. The goal of this Essay is to explain the architectural structure of decentralized exchanges, and the performance and security tradeoffs associated with various architectural choices. By understanding these technical differences, the reader will have a better grasp of which decentralized exchanges are optimized for which use cases.

Architecture of a Decentralized Exchange

The term “decentralized exchange” is used colloquially to describe both blockchain-based exchange protocols, as well as applications that leverage the protocols. A decentralized exchange protocol generally describes a software program, hosted on or integrated into one or more distributed ledgers (e.g., Ethereum), that enables peer-to-peer transactions that are automatically settled on the distributed ledger. Users retain sole custody of their private keys throughout the transaction process.

A decentralized exchange application builds on top of a decentralized exchange protocol, and adds an on-chain or off-chain order book database and a graphic user interface (GUI) and/or APIs so that the information is easily accessible.

Overall, a decentralized exchange application can be broken down into the following components:

1. The blockchain platform & technical implementation
2. The counterparty discovery mechanism
3. The order matching algorithm
4. The transaction settlement protocol

A decentralized exchange application may not be fully decentralized in all four components. Note that for many decentralized exchange applications, one or more components may be off-chain/centralized, or otherwise feature economic incentives which would promote a tendency towards centralization.

We will discuss each of these components and provide examples of how some decentralized exchange protocols implement these components.

1. Platform & Technical Compatibility

Most decentralized exchange protocols generally operate with tokens that feature the same technical implementation and are on the same distributed ledger platform. For example, AirSwap, EtherDelta, and Ox are independent protocols that are operable only with standardized ERC-20 tokens on the Ethereum blockchain. Beyond Ethereum, Stellar’s decentralized exchange is operable with tokens issued on the Stellar network, and BitShares’ OpenLedger DEX is operable only with tokens issued on the BitShares blockchain platform. Off-chain cryptocurrencies and assets could also be traded through the Stellar decentralized exchange or OpenLedger DEX if an “anchor” issues tokens onto the network that represent ownership of a defined unit of the off-chain cryptocurrency. However, this requires users to trust that the anchor has sufficient reserves of the off-chain cryptocurrency to satisfy all redemptions of the tokens.

A few decentralized exchanges are beginning to use atomic swaps to enable users to atomically trade cryptocurrencies that exist on different blockchain networks (e.g. exchanging Bitcoin for Dogecoin, cryptocurrencies from separate blockchains). However, atomic swaps still require that the transacted cryptocurrencies adhere to certain common technical standards. For example, in BarterDEX, a cross-chain decentralized exchange that enables users to transact cryptocurrencies from different blockchains, atomic swaps are only available for cryptocurrencies from blockchains that have implemented features that mirror the Bitcoin reference implementation, such as BIP65 (Check LockTime Verify) and other standard Bitcoin API methods. In practicality, this means that cryptocurrencies that were built off the Bitcoin reference implementation, such as Litecoin and Dogecoin, or cryptocurrencies that forked from Bitcoin, such as Bitcoin Cash and Bitcoin Gold, will be the easiest to make compatible for atomic swaps with Bitcoin.

Cross-chain swap technologies like PolkaDot and Cosmos are also building tools and protocols that could eventually be integrated into decentralized exchange applications that can atomically swap tokens from different blockchains. However, given the current latency of most cross-chain atomic swaps (with transaction confirmations dependent on the confirmation times of both cryptocurrencies' underlying blockchains), most popular decentralized exchange applications currently focus exclusively on token trading within one chain. As PolkaDot, Cosmos, and other interchain swap tools and protocols are refined and developed in conjunction with Lightning, Raiden, and other transaction performance-enhancing upgrades, some day users may enjoy liquid and low latency cross-chain decentralized exchanges.

2. Counterparty Discovery Mechanisms

Counterparty discovery mechanisms enable buyers to discover sellers who are willing to execute transactions on mutually acceptable terms. On traditional cryptocurrency exchanges such as Binance, Bittrex, and Kraken, users have the option of submitting both market orders and limit orders, and these orders are automatically matched with unidentified counterparties using the exchange's central limit order book which aggregates all user orders.

Most decentralized exchanges also have order books. These order books may exist on-chain, hosted on a distributed ledger, or off-chain, hosted by third parties. Most decentralized order books display the separate orders of each counterparty, rather than the aggregated orders of all counterparties. Users normally will need to identify a particular order, and thus a particular counterparty, in order to trade.

Some decentralized exchanges do not have order books and instead feature a reserve-based model. A reserve provides a supply and demand of various tokens that

are readily available to be executed based on the reserve's quoted buy and sell prices for that token. These reserves are created by on-chain smart contracts that enforce the trade execution and settlement process. The trade price may also be programmatically determined by a smart contract.

For the rest of this Essay, the term "Maker" will refer to the party that provides an order, and the term "Taker" will refer to the party that fills it.

On-chain order book

On-chain order books are hosted directly on the distributed ledger: all orders are submitted to the distributed ledger network and are confirmed by the network. Anyone can host and access a copy of the order book, and anyone may submit their own orders to be included in the order book as long as the distributed ledger is public.

Examples of on-chain order books include the Bitshares and Stellar decentralized exchanges. In the Stellar network, users submit orders which are hosted on a persistent and public on-chain order book in the Stellar distributed ledger. Information about this order book is broadcast to all Stellar validator nodes and is viewable by the public. When two orders intersect in price, the trade is automatically executed and settled by the Stellar network. The BitShares decentralized exchange operates under a similar model, but for the BitShares blockchain and network.

Benefits:

1. **Less censorable:** There is lower reliance on a centralized party to host and operate the order book. There may be a centralized GUI for the order book, but any independent party would be able to create separate GUIs and populate it with the on-chain data. Assuming that hosting and operating of the order book is distributed across independent, non-colluding validator nodes, there is no centralized point of attack, compromise, or liability that would result in the order book being shut down or specific orders being restricted by a centralized party.
2. **Less trust required:** Decentralized, on-chain order book hosting means that one does not need to trust centralized, off-chain actors to accurately and reliably publish or broadcast order books.

Trade-offs:

1. **Order book inherits performance, cost, and security characteristics of the underlying blockchain:** The speed and cost of submitting or removing an offer on an on-chain order book are limited by the speed and cost of interacting with the underlying blockchain. Users must pay for each order book update on

the network, wait for the network to reach consensus on their updates, and then wait for secure confirmation of the updates. If the blockchain is compromised by an attack, the order book may be compromised. Therefore, slower and higher fee blockchains are less favorable for hosting a user-friendly on-chain order book.

2. **Slower updates:** In the absence of second-layer technologies like the Lightning Network or Raiden Network, on-chain order books are generally updated based on the information contained in the latest block or ledger. This creates latency which could range from minutes to seconds depending on the platform. In contrast, off-chain order books can support almost-instantaneous updates given that most only need to alter a centralized database to reflect the update.
3. **Stale orders:** On-chain decentralized exchanges generally support resting orders, where the desired price and quantity have been fixed by the Maker upon creation of an offer. In a resting order, the offer must be proactively canceled by the Maker if she no longer wishes to trade on those terms if, for example, the price has changed dramatically. Since updates to on-chain order books can have delays due to the speed of transaction validations of the underlying network, on-chain order books could create an environment where resting orders are exploited when there is high price volatility. However, as usage of on-chain order books grows, we expect to see growth and adoption of trading tools (such as trading bots) to help users programmatically automate the submission and cancellation of order upon market price changes.

Off-chain order books

Off-chain order books are order books that are hosted by a centralized entity outside of a distributed ledger. The centralized entity helps parties discover other parties who make offers on the asset and can restrict access to view or submit to the order book.

The practicality of using an on-chain or off-chain order book depends significantly on the performance of the chain. Decentralized exchanges normally do not employ on-chain order books given that every order and adjustment to an on-chain order book would require an update to the blockchain, thereby incurring transaction fees and wait time. On certain chains, transaction fees are negligible and wait times are on the order of seconds. Under these circumstances, an on-chain order book is practical to use for moderate volumes of intermittent orders. Comparatively, on the Ethereum blockchain, transaction fees are non-negligible and wait times are on the order of minutes. Using an Ethereum on-chain order book would likely incur expensive transaction fees and debilitating wait times. For this reason, four of the most prominent decentralized exchanges in Ethereum—Ox, AirSwap, EtherDelta, and IDEX—employ off-chain order books. As of October 2018, Ox, AirSwap, EtherDelta, and IDEX support ERC-20 tokens.

- In the Ox ecosystem, entities called “Relayers” host, manage, and publish off-chain order books. Makers will submit buy and sell orders directly to a Relayer, and the Relayer will aggregate all received orders into its order book. Takers discover Makers’ orders by querying the Relayer’s order books. Upon finding a suitable order, a Taker will fill the order by submitting information pursuant to the Ox protocol to the Ox exchange contract on the Ethereum blockchain. Given that all Relayers use the Ox protocol for settlement, a Relayer may choose to share its order books with other Relayers, thereby unlocking thicker order books and greater liquidity.
- On the AirSwap platform, a Maker will submit an “intent to trade” in a certain trading pair to an entity called the “Indexer.” The Indexer will aggregate information about the Makers and their intents to trade. Takers who wish to trade in a certain trading pair will query the Indexer to discover the identities of suitable Makers, using the Indexer as a counterparty discovery mechanism. Once a Taker finds a suitable Maker, they will negotiate off-chain on the terms of the trade, potentially using the input of an off-chain “Oracle” that will suggest fair pricing for the trade. Once the Maker responds with an order that is satisfactory to the Taker, the Taker will submit the order to the Ethereum blockchain.
- On the EtherDelta web application, in order to make or fulfill an order, Makers and Takers will deposit tokens from their Ethereum wallet into EtherDelta’s on-chain smart contract. Makers will submit orders to be publicly broadcast on the EtherDelta off-chain order book, and the order book will ping the blockchain to verify that the Maker has sufficient balance deposited in the smart contract to fulfill the order. Takers will then select an order and click “Buy” on the web application, causing the EtherDelta smart contract to perform the trade.
- On the IDEX web application, in order to make or fulfill an order, users will deposit tokens from their Ethereum wallet into an IDEX smart contract. Users then use the IDEX application interface to place buy and sell orders on an off-chain order book. IDEX and EtherDelta have similar structures in that they both integrate an off-chain order book with an on-chain smart contract for settlement, but IDEX adds on a “transaction processing arbiter” that helps to manage the order of pending trades so that trades are confirmed in the correct order. Therefore, as users trade, the IDEX application interface will update their displayed balances in real-time, but the on-chain settlement may occur with a delay given that transactions are queued. By controlling the order of transactions, IDEX separates trade execution from trade settlement, facilitating a smoother user experience.

There are both benefits and tradeoffs to having an off-chain order book.

Benefits:

- **Performance improvements:** Off-chain order books are better able to accommodate quick order turnover. Instead of waiting for a block to be mined and confirmed (or, alternatively, a ledger to be updated) to update the order book, off-chain services can update ledgers almost instantaneously.
- **Cost improvements:** There is no need to pay a transaction fee in order to submit or update an order.
- **Fewer blockchain-originated risks to the order book:** Given that the order books are hosted off-chain, the order books would not be vulnerable to blockchain-originated vulnerabilities such as 51% attacks (where users may reverse transactions) and front-running (where users may submit higher transaction fees for their offers to be included or updated faster than others').
- **Compatible with all ERC-20 tokens:** Any token that has the ERC-20 technical implementation can be traded on these decentralized exchange protocols. The token does not necessarily need to be approved, audited, or reviewed by anyone to be traded.

Trade-offs:

- **Higher degree of trust required:** Users must rely on the hosts of the off-chain order book to properly broadcast orders. These hosts could fail to accurately display and update orders, such that users would not be able to rely on them to discover counterparties. In the worst case scenario, these hosts could choose to arbitrarily censor valid orders or manipulate markets by strategically displaying inaccurate or outdated orders. Additionally, hackers could change the off-chain order book interface to manipulate users into sending cryptocurrency to the hackers' cryptocurrency accounts.
- **Greater restrictions:** As a centralized entity, the operator of the off-chain order book may be subject to greater legal and regulatory requirements, such as the implementation of Know-Your-Customer requirements, obtainment of requisite authorizations and licenses needed to trade cryptocurrencies classified as securities, and the implementation of rules and policies against market manipulation. While these requirements are helpful in preventing unlawful and abusive uses of the order book, these requirements may raise concerns about transaction privacy, open accessibility, and user experience.
- **Inaccurate order books:** Given that there is a mismatch in timing between a Maker's submission of an order and a Taker's fulfillment of an order, any given order displayed on an off-chain order book may be outdated by the time that the Taker wishes to fill the order. For example, the Maker may already have withdrawn the tokens that she wanted to trade, yet her order is still posted on a Relayer. Therefore, the Taker may attempt to fill an order by submitting a transaction to the blockchain, only to realize that the order is no longer valid. This could delay the Taker and consume significant amounts of transaction fees.

No (or hidden) order book: liquidity reserves

To solve the issue of low liquidity, some decentralized exchange protocols, such as KyberNetwork, Bancor, and Omega One build up and/or leverage liquidity reserves that are readily accessible when users wish to exchange tokens. The performance of these models depends on reserve depth/breadth and accurate pricing.

- In KyberNetwork, “Reserve Contributors” contribute tokens to build up “Reserves” of a variety of tokens. Each Reserve has a conversion rate for each trading pair, managed dynamically by a Reserve Manager. If a user wants to exchange token A for token B, she will send tokens to the KyberNetwork smart contract and the KyberNetwork will find her the most favorable rate, as determined by Reserve Managers. If such rate meets the user’s pre-defined minimum requirements, the smart contract will send the corresponding amount of token B to the sender’s pre-specified address. The user can view and approve the worst-case rate prior to sending any tokens.
- In Bancor, users can exchange tokens for other tokens through smart contracts called “Smart Tokens,” which store reserves of ERC-20-compliant tokens and ether. To illustrate, users who wish to exchange token A for token B would need to find a Smart Token contract holding both tokens in reserve (i.e., Smart_Token_AB). The user would send token A to Smart_Token_AB, thereby buying some number of Smart_Token_AB tokens based on token A’s formulaic price. Next, the user would send the Smart_Token_AB tokens to its smart contract, thereby destroying those tokens and pulling out a number of B token based on token B’s formulaic price. Prices are programmatically determined through a formula that factors in the reserve supply of each token plus a constant reserve ratio.
- Omega One aims to aggregate liquidity across cryptocurrency exchanges by treating the entire centralized and decentralized exchange landscape as a potential reserve. Users who want to trade token A for token B will deposit token A in the Omega One’s on-chain smart contract and submit an order to trade token B subject to timing and pricing limits. Omega One will then use its own centralized and decentralized exchange accounts to purchase token B and trade it with the user’s token A in a swap via the smart contract.

Benefits:

- **Lower friction to trade:** The reserve model enables users to enter trades more easily given that the supply and demand sides (i.e., the reserve) have fixed terms and are readily available to trade upon those terms. This removes the potential friction involved in discovering counterparties and negotiating.

Trade-offs:

- **Requires trust in a smart contract or third party:** The model requires a party to trust in the security, accuracy, and fairness of the smart contract or third party that is performing the reserve and/or order fulfillment functions. Given that smart contracts are complex, difficult to audit, and may have unanticipated security vulnerabilities, users could lose funds if the smart contract is hacked or misbehaves. Models that rely on third parties to provide liquidity, such as KyberNetwork and Omega One, require users to trust these third parties to act reliably and fairly.
- **Uncertain pricing:** Given that there is high volatility in token prices, some models require users to trust a centralized party to provide fair and updated pricing. Meanwhile, models that rely on deterministic pricing algorithms could be easily exploited by arbitrageurs.
- **Tendency to favor large reserve contributors:** Reserve models that rely on users to fund reserves may incentivize larger reserve contributors to participate more than smaller reserve contributors since lower spreads on trades will require higher volume to be profitable. In that case, users may need to depend on the participation of large reserve contributors for liquidity, leading to more centralized control of reserve supply.
- **Reserves may be available and liquid only for the most popular tokens:** Tokens that are new or exotic may not have reserves available or may have insufficient reserves to fulfill trades based on a user's desired price and quantity. Only commonly traded tokens are likely to have deep, liquid reserves.

3. Matching Mechanisms

Matching is the process through which buy orders are paired with sell orders that have mutually acceptable terms. Decentralized exchanges may feature automatic matching or require Takers to manually identify and fill an order. Automatic matching occurs when a computer algorithm is used to pair and execute buy and sell orders. "Manual" order filling is the process through which Takers identify a resting order on the order book and actively perform actions to execute that particular order.

On centralized exchanges, all user orders are aggregated, and users are able to submit market orders and limit orders. A market order is a buy or sell order that is executed instantaneously based on the current market price, and a limit order is a buy or sell order where a user will specify a maximum purchase price or minimum sale price, and will only be matched with orders that offer a price that is at or more favorable than the specified price. Market orders allow users to obtain market price for their orders without having to specify a desired price, thereby increasing the speed and ease of trade, whereas limit orders allow users to obtain market price for their orders while protecting them from trades that are less favorable than a specified minimum or maximum price.

By comparison, most non-reserve-based decentralized exchange protocols do not have market orders or limit orders. These protocols often feature manual order filling whereby Makers will submit resting orders that specify a fixed price and volume, and Takers will fill these orders based on the Makers' specified terms. Therefore, if prices of the trading assets change significantly after a Maker places an order, and the Maker does not have an opportunity to correct the price, the order may get filled at a price that is less favorable to market price. However, developers of off-chain order books, user interface applications, and bots for these protocols can implement off-chain logic that mimics automatic order filling by allowing a user to specify desired parameters off-chain, and programmatically selecting the most favorable order that meets the user's specified parameters.

Reserve-based decentralized exchange protocols may feature automatic matching services that function similar to limit orders. Prior to execution, the user may query a smart contract or an off-chain party about the reserve's current exchange rate, and some protocols have built-in guarantees that the user will receive an exchange rate that is at least as favorable as a stated exchange rate or a user's specified exchange rate.

Analyzing a decentralized exchange's order matching algorithm is important because this will affect its ease of use, ability to provide fair exchange rates, and wait time between order creation and order fulfillment (i.e., the latency of order fulfillment). Moreover, the algorithm also informs the arbitrage opportunities that could arise from manipulating the prioritization and speed of matching through mechanisms such as front-running.

Manual order filling

With manual order filling, Takers must proactively find and accept a counterparty order. This mechanism introduces more latency into order filling, but generally requires less trust and provides users more control given that users do not have to rely on a centralized or smart contract-based matching algorithm.

For example, in Ox, Takers discover Makers' orders via Relayers. If a Taker wishes to accept an order, she will submit a counterorder to the Relayer and digitally sign and send the completed transaction to an on-chain smart contract that will settle the transaction. If a Maker's orders are not actively monitored, Takers could exploit stale orders upon changes in the fair market price of the underlying token. However, off-chain bots and services could help the Maker programmatically manage its orders based on market price fluctuations.

In AirSwap, users can query Indexers to find addresses of counterparties. Users must negotiate with counterparties privately to reach agreement on transaction terms and

fulfill an order. This mechanism helps to protect Makers from losing money on stale orders (e.g., orders that are not reflective of current price movements).

On EtherDelta, Makers will post resting orders onto the order book, specifying a desired price and quantity for a trade. A Taker must manually select a Maker's order from the order book and submit the order on the web application. Even if there are buy and sell orders that intersect on their desired terms, EtherDelta will not automatically match and execute these orders. The absence of an automatic order matching creates more latency and friction, given that Takers must manually identify suitable trades. However, no central party is needed to fairly and reliably match orders.

Automated order filling

With automated order filling, an algorithm will match orders automatically. Automated order filling reduces the amount of user time and effort needed to identify suitable trades, thereby reducing order filling latency. However, this approach requires users to trust the matching mechanism to execute securely and provide them a favorable price.

Decentralized exchanges employing liquidity reserves have automated order filling. In KyberNetwork, Reserve Managers feed dynamic exchange rates into the KyberNetwork smart contract and orders are filled at the current exchange rate. In Bancor, orders are fulfilled automatically based on a deterministic pricing formula built into the smart contract. In Omega One, orders are fulfilled automatically based on the best rate found across multiple exchanges.

IDEX is a non-reserve-based decentralized exchange that employs automated order filling. On IDEX, users may submit limit and market orders because the application has built-in off-chain order matching algorithm that helps match orders on the off-chain order book. The user will be matched with the most favorable order that is available on the order books, provided that it is more favorable than the user's stated baseline price. This off-chain matching logic significantly improves the user experience; at the same time, users must trust IDEX's order matching algorithm to fairly and reliably match orders.

On the Stellar decentralized exchange protocol, users may also submit limit orders to the on-chain order book. The Stellar decentralized exchange has an on-chain order matching algorithm that matches orders based on a first-in-price, first-in-time principle: orders are automatically filled such that, when an acceptable counterorder is found, the earliest submitted order made will be filled. The on-chain order matching algorithm is built into the Stellar network protocol, meaning that there is no need to trust a centralized party to perform the order matching.

4. Transaction Settlement

All decentralized exchanges feature on-chain settlement. On-chain settlement is a necessary element that enables users to eliminate the need to trust a centralized party (such as a centralized exchange) to control user assets, settle trades, and ensure that account balances are correct. On-chain settlement helps users publicly verify on the ledger that their trades were settled according to their desired terms.

The performance of any decentralized exchange is limited, at the very minimum, by the latency involved in securely confirming a transaction on the underlying chain. Therefore, the speed of confirming a transaction in a distributed ledger network is the bottleneck for decentralized exchanges.

Some distributed ledgers feature significantly higher latency than others. A secure settlement confirmation on the Bitcoin network may take hours, whereas a secure confirmation on Ethereum generally takes minutes under current limitations. Confirmations on certain more recent platforms can require a few seconds. Therefore, the final settlement time would depend heavily on the confirmation latency of the underlying chain.

Different Exchanges, Different Use Cases

Each decentralized exchange presents a different array of latency, security, liquidity, privacy, interoperability, and trust tradeoffs. Therefore, different exchanges will excel in different use cases and requirements.

Access

First and foremost, different decentralized exchanges offer access to different cryptocurrencies.

Many cryptocurrencies issued in 2017 and 2018 are ERC-20 tokens; in order to purchase these tokens, one must use an decentralized exchange protocol that is compatible with the ERC-20 technical standard, such as 0x or IDEX. Similarly, as some new ICOs are held on competing platforms such as Stellar and Waves, one may be pushed to use their respective decentralized exchanges to transact tokens issued on those platforms.

Security

With respect to the technical security of Ethereum smart contract-based exchange protocols, the smart contract driving the exchange protocol may be vulnerable to accidents and security vulnerabilities. The degree to which a smart contract will function as intended and will not be vulnerable to exploits remains somewhat uncertain given the difficulty of thoroughly auditing Ethereum's Turing-complete smart contracts. By contrast, distributed ledgers with on-chain native decentralized

exchange functionality should in theory have significantly lower attack surface given that protocols are more thoroughly audited and require network consensus to change and exploit.

The security of a decentralized exchange is limited also to the security of the underlying distributed ledger. For example, if a proof of work blockchain is attacked, such as through a “51 percent” attack, settled transactions may be reversed despite a large number of block confirmations. Under any consensus mechanism, the network’s validator nodes could also collude to “fork” to an alternate state of transactions (and orders, in the case of an on-chain order book), adopt a technical standard that is incompatible to the decentralized exchange protocol, censor (i.e. ignore) orders submitted by certain addresses, modify order settlement, matching, and reserve smart contracts, and more. Therefore, the ultimate security of a decentralized exchange is dependent on the security of the underlying distributed ledger.

Transactions that require strong security conditions should be settled using thoroughly audited smart contracts and distributed ledger platforms with a consistent history of guaranteed functionality.

Liquidity

Many new cryptocurrencies may only be available for purchase or sale through decentralized exchanges, given that centralized exchanges have been slow to list new tokens due to regulatory risk. Therefore, many cryptocurrencies may only be attainable and tradable over decentralized exchanges. However, a decentralized exchange would not be practically useful for users if it did not have robust order books or other mechanisms that enable users to transact cryptocurrencies without significant price slippage.

The use of interoperable decentralized exchange protocols enable applications that use the same protocol to be able to pool together liquidity for “networked liquidity.” For example, Relayers built on 0x may pool together their order books to build a thicker order book. Any token issued on the Stellar platform can be exchanged with any other token issued on Stellar, generating a network-wide order book. While liquidity on decentralized exchanges is currently significantly lower than on popular centralized exchanges, interoperable protocols will hopefully spur greater networked liquidity.

Latency

The latency of a decentralized exchange depends on the speed of the underlying distributed ledger. For example, if it takes 3 minutes to confirm one transaction in Ethereum, then an order would be settled in 3 minutes at a minimum given that the

ultimate settlement of a trade must be on-chain. This latency will likely improve as the Ethereum network adopts new technologies to increase throughput and lower validation time.

Some distributed ledger networks permit significantly faster on-chain settlements due to the use of different consensus mechanisms. For example, an order or settlement on Stellar can be securely confirmed in 5 seconds due to the speed of the Stellar Consensus Protocol. The on-chain order books on Stellar would be slower to update than the off-chain order books on Ethereum-based decentralized exchanges, but third parties could eventually develop off-chain order books for the Stellar decentralized exchange, as well.

Even the lowest latency decentralized exchanges currently cannot compete with the near-instantaneous settlement speeds of centralized exchanges. For users who engage in high-frequency trading activities, centralized exchanges such as Coinbase Pro, Bittrex, Kraken, and Poloniex may still be the best choice, given that market orders can potentially be placed and settled in seconds. Moreover, until the stable release of cross-chain atomic swaps, centralized exchanges are still the best platforms for trades swapping tokens that were issued across multiple chains.

Cost

The cost of using a decentralized exchange application includes the costs of (1) fees to the decentralized exchange application, (2) fees of making and/or taking orders, (3) fees involved in interacting with any smart contracts enabling the decentralized exchange protocol, and (4) fees involved in settling a transaction to the distributed ledger. These costs may include blockchain network transaction costs (e.g. using ETH for transaction fees for settling a transaction on the Ethereum) or fees for using a certain protocol (e.g. paying ZRX tokens to OX Relayers for trading fees). Settlement on some blockchains may cost more than a settlement on others.

Whereas centralized exchanges tend to charge fees that are a percentage of the total transaction size, the cost of using a decentralized exchange tends to be fixed per transaction: a high-value transaction would incur the same fees as a microtransaction. Therefore, those who are submitting high-value transactions may save transaction fees by using a decentralized exchange.

Trust Level

Different decentralized exchange applications require different levels of user trust. Users may need to trust: (1) the decentralized exchange application creator and operator to perform activities such as hosting and publishing order books or performing order matching, (2) the underlying decentralized exchange protocol, including relevant smart contracts, and (3) the security, miners, and validators of the

underlying distributed ledger. Users must trust each part of the exchange application stack to perform its job fairly, reliably, and securely. If any part of the stack fails, users may be unable to reliably and securely submit and fill orders, match with orders that meet their specified criteria, and confirm the settlement of trades. Moreover, users may find that trusted parties could censor some of their transactions or act in a self-interested manner to the users' detriment.

Some users may want to minimize trust in the decentralized exchange application layer: therefore, they would want to minimize reliance on the application to host and publish order books and/or perform order matching. Therefore, these users may choose applications that have on-chain order books. They may also choose applications that do not have automatic order matching.

Some users may want to minimize trust in the decentralized exchange protocol by making sure that the protocol has a minimal attack surface. These users may choose to only interface with highly audited protocols such as Ox protocol, or an on-chain, difficult-to-modify protocol such as the Stellar protocol.

Lastly, some users may want to minimize trust in the security, miners, and validators of the underlying distributed ledger. Different users will have different opinions on which distributed ledgers have the most favorable, trust-minimized characteristics; factors such as the ledger's security and exploits history, audit history, consensus mechanism, governance mechanisms, and distribution of miners and nodes could all contribute to this calculus.

Practically speaking, many users may not be overly concerned about trusting decentralized exchanges given that users do not relinquish control over their private keys. Ultimately, most users may prefer a better user experience rather than optimizing for trust minimization. Users must decide on the level of trust that is necessary for their personal use cases for a decentralized exchange.

Conclusion

The term "decentralized exchange" encompasses diverse applications and protocols that differ in architecture, but all enable users to transact cryptocurrencies without relinquishing control over their private keys to an intermediary.

Decentralized exchanges are still in an early development stage; their higher trade latency, lower liquidity, and less intuitive user interfaces make them less attractive for mainstream retail users. However, as centralized exchanges continue to experience security exploits and delay the listing of new cryptocurrencies, more users will elect to adopt decentralized exchanges despite their high friction. It is worthwhile to invest in the development and growth of the decentralized exchange ecosystem to

promote liquidity in an increasingly diverse token ecosystem, greater user control of cryptocurrencies, more privacy features, and lower risk of censorship.

Planting Bitcoin—Species (1/4)

Sound Money (sanum pecuniam)

By [Dan Held](#)

Posted January 6, 2019

Foreword

I wrote this series, “Planting Bitcoin”, to paint the origin story of Bitcoin leading up to the 10 year anniversary (10/31/2018). I felt that this story hadn’t been told in a comprehensive and easy to read manner. I’d like to thank [Jill Carlson](#) for incepting this idea on the road trip back from Tahoe in early 2018.

Introduction

Bitcoin’s origin is akin to planting a tree. It wasn’t just Satoshi’s selection of the species (code), but the season (timing), soil (distribution), and gardening (community) that were essential to its success. It had to grow to be strong, mighty, and huge. It had to survive droughts, storms, and predators. Its deep roots had to support the weight of becoming a new world reserve currency.

What is Money

Money is most easily defined as the medium in which value is transferred. But Money is not just paper in your hand; or numbers in your bank account, Money represents something much more fundamental:

- Money is a primitive form of [memory](#) or record-keeping. It is the collective memory of who has the ability to allocate wealth.
- Money, which is the representation of the work required to acquire goods and services, can also be viewed as [stored energy](#).
- Money is the central information utility of the world economy. As a medium of exchange, store of value, and unit of account, money is the critical vessel of information about the conditions of markets.

The main functions of money are Store of Value (SoV), Medium of Exchange (MoE), and Unit of Account (UoA). No money starts by providing all three functions, each new species of money follows a distinct evolutionary path that we will cover later. Let’s first start by identifying the newest species of money, Bitcoin.

Species

“These protocols can’t be described comprehensively as static objective things. They’re best thought of as live systems” – [Ari Paul](#)

Bitcoin is a new form of life, a new species of money called “cryptocurrency.” More importantly, it is “sound money,” or using proper taxonomy, “sanum pecuniam.” Sound money is [defined](#) as money that has a purchasing power determined by markets, independent of governments and political parties which is essential for individual freedom.

“I had to write all the code before I could convince myself that I could solve every problem, then I wrote the paper.” – [Satoshi Nakamoto](#)

The code of life is written into an organism at its inception. Satoshi carefully architected Bitcoin’s DNA, or genetic code, to be the best sound money ever created. We can think of Bitcoin’s genetic code as representing instructions that have been written to incentivize the organization and coordination of cellular function.

“I believe I’ve worked through all those little details over the last year and a half while coding it, and there were a lot of them”- [Satoshi Nakamoto](#)

Bitcoin’s genetic code:

- Satoshi needed a way for the Bitcoin to spark itself into existence, so he coded in its DNA a fixed supply (21M Bitcoins). An increase in Bitcoin’s price inevitably leads to a corresponding increase in participants (users), security (mining), and developers. This becomes a self-reinforcing [feedback loop](#).
- Bitcoin’s mining function, Proof of Work (PoW) is both its metabolism and defense mechanism. Bitcoin [eats energy](#) to generate new coins and build digital walls to protect the network. PoW also makes Bitcoin anti-fragile, or in other words, as it grows larger, it becomes more resistant to attack.
- A new Bitcoin block is found every 10 minutes, this genetic code enables Bitcoin’s cells to effectively communicate and coordinate with each other despite enormous distances. It is the [internal clock](#) that sets the metabolic rate.

“It lives and breathes on the internet. It lives because it can pay people to keep it alive. It lives because it performs a useful service that people will pay it to perform. It lives because anyone, anywhere, can run a copy of its code. It lives because all the running copies are constantly talking to each other. It lives because it is radically transparent: anyone can see its code and see exactly what it does. It

can't be changed. It can't be argued with. It can't be tampered with. It can't be corrupted. It can't be stopped. It can't even be interrupted. If nuclear war destroyed half of our planet, it would continue to live, uncorrupted." — [Ralph Merkle](#)

Bitcoin's genetic code manifests itself via traits (characteristics of an organism) that may or may not be visible.

Traits

In biology, a trait or character is a feature of an organism. According to Charles Darwin's theory of evolution by natural selection, organisms that possess heritable traits that enable them to better adapt to their environment compared with other members of their species will be more likely to survive, reproduce, and pass more of their genes on to the next generation.

Money is no different. Money has traits that enable it to survive and thrive as a Store of Value (SoV), Medium of Exchange (MoE), and Unit of Account (UoA). Bitcoin is a new species that has vastly superior traits to its predecessors. Below we dive deeper into those traits between different species of money.

Traits of Money	Bitcoin	Gold	Fiat
Verifiable	High	Moderate	Moderate
Fungible	High	High	High
Portable	High	Low	High
Durable	Moderate	High	Low
Divisible	High	Low	Moderate
Scarce	High	Moderate	Low
Established History	Low	High	Low
Censorship resistant	High	Moderate	Low
Unforgeable Costliness	High	High	Low
*Openly Programmable	High	Low	Low
*Decentralized	High	Moderate	Low

**Bitcoin's birth introduced two new traits, "Openly programmable" and "Decentralized"*

(The sections below, on the attributes that make for a sound money, are largely borrowed from [Vijay Boyapati](#)'s article "[The Bullish Case for Bitcoin](#)")

Verifiable

Fiat currencies and gold are fairly easy to verify for authenticity. However, despite providing features on their banknotes to prevent counterfeiting, nation-states and their citizens still face the potential to be duped by counterfeit bills. Gold is also not immune from being counterfeited. Sophisticated criminals have used [gold-plated tungsten](#) as a way of fooling gold investors into paying for false gold. Bitcoins, on the other hand, can be verified with absolute mathematical certainty.

Fungible

Gold provides the standard for fungibility. When melted down, an ounce of gold is [nearly](#) indistinguishable from any other ounce. Fiat currencies, on the other hand, are only as fungible as the issuing institutions allow them to be. While it may be the case that a fiat banknote is usually treated like any other by merchants accepting them, there are instances where large-denomination notes have been treated differently to small ones. For instance, India's government, in an attempt to stamp out India's untaxed gray market, completely demonetized their 500 and 1000 rupee banknotes. Bitcoins are fungible at the network level, meaning that every bitcoin, when transmitted, is treated the same on the Bitcoin network. However, because bitcoins are traceable on the blockchain, a particular bitcoin may become tainted by its use in illicit trade and merchants or exchanges may be compelled not to accept such tainted bitcoins. Despite this, there is no alternative pricing for "tainted Bitcoins" so it remains highly fungible.

Portable

Bitcoins are the most portable store of value ever used by man. A single USB stick can contain a billion dollars, easily carried anywhere, transmitted near instantly. Fiat currencies, being fundamentally digital, are also highly portable. However, governments can control the free flow of capital. Cash can be used to avoid capital controls, but then the risk of storage and cost of transportation become significant. Gold, being physical in form and incredibly dense, is by far the least portable. When bullion is transferred between a buyer and a seller it is typically only the title to the gold that is transferred, not the physical bullion itself (It cost Germany \$9.1 million to [repatriate](#) their gold).

Durable

Gold is the king of durability—the vast majority of gold that has ever been mined or minted, including the gold of the Pharaohs, remains today and will for near eternity (it can only be destroyed through nuclear transmutation). While fiat currency exists both in physical and digital forms, we will only consider the durability of its digital form... the durability of the institution that issues them. Many fiat issuing governments have come and gone over the centuries, and their currencies disappeared with them. If history is a guide, it would be folly to consider fiat currencies durable in the long term—the US dollar and British Pound are relative anomalies in this regard. Bitcoins, having no issuing authority, may be considered durable so long as the network that secures them remains in place. Given that Bitcoin is still in its infancy, it is too early to draw strong conclusions about its durability. However, there are encouraging signs that the network displays a remarkable degree of [“anti-fragility.”](#)

Divisible

Bitcoins can be divided down to a hundred millionth of a bitcoin and transmitted at such infinitesimal amounts. Fiat currencies are typically divisible down to pocket change, which has little purchasing power, making fiat divisible enough in practice. Gold, while physically divisible, becomes difficult to use when divided into small enough quantities that it could be useful for lower-value day-to-day trade.

Scarce

The attribute that most clearly distinguishes Bitcoin from fiat currencies and gold is its predetermined absolute scarcity: only 21 million bitcoins can ever be created (the number of units is arbitrary, as Bitcoins can be subdivided into 210 quadrillion satoshis). This gives the owner of bitcoins a known percentage of the total possible supply. Gold, while remaining quite scarce through history, is not immune to increases in supply. If it were ever the case that a new method of mining or acquiring gold became economic, the supply of gold could rise dramatically (ex: [sea-floor](#) or [asteroid mining](#)). Finally, fiat currencies, while only a relatively recent invention of history, have proven to be prone to constant increases in supply. Nation-states have shown a persistent proclivity to inflate their money supply to solve short-term political problems.

Established history

No monetary good has a history as long and storied as gold, which has been valued for as long as human civilization has existed. Coins minted in the distant days of antiquity [still maintain significant value today](#). The same cannot be said of fiat

currencies, which are a relatively recent anomaly of history. From their inception, fiat currencies have had a near-universal tendency toward eventual worthlessness. The use of inflation as an insidious means of invisibly taxing a citizenry has been a temptation that no states in history have been able to resist. Bitcoin, despite its short existence, has weathered enough trials in the market that there is a high likelihood it will not vanish as a valued asset any time soon. Furthermore, the [Lindy effect](#) suggests that the longer Bitcoin remains in existence the greater society's confidence that it will continue to exist long into the future. The [median](#) age of a human is ~30 years old, which means Bitcoin has been around for nearly 33.3% of the average human life. If Bitcoin exists for 20 years, there will be near-universal confidence that it will be available forever, much as people believe the Internet is a permanent feature of the modern world.

Censorship resistant

One of the most significant sources of early demand for bitcoins was their use in the illicit drug trade. Silk Road was a testament to this resistance. The key attribute that makes Bitcoin valuable for proscribed activities is that it is “permissionless” at the network level. When bitcoins are transmitted on the Bitcoin network, there is no human intervention deciding whether the transaction should be allowed. As a distributed peer-to-peer network, Bitcoin is, by its very nature, designed to be censorship-resistant. This is in stark contrast to the fiat banking system, where states regulate banks and the other gatekeepers of money transmission to report and prevent outlawed uses of monetary goods. A classic example of regulated money transmission is capital controls. A wealthy millionaire, for instance, may find it very hard to transfer their wealth to a new domicile if they wish to flee an oppressive regime (Russian assets in the UK being frozen). Although gold is not issued by states, its physical nature makes it difficult to transmit at distance, making it far more susceptible to state regulation than Bitcoin. India's [Gold Control Act](#) is an example of such regulation. If your mission is to disrupt central banks, you need to have sovereign level censorship resistance.

“Bitcoin’s advantages lie not in its speed, convenience, or friendly user experience. Bitcoin’s value comes from it having an immutable monetary policy precisely because nobody can easily change it” —
[Saifedean Ammous](#)

Unforgeable Costliness

Money that is costly to create. Due either to its original cost (gold mining) or the improbability of its history (art)—and that it is difficult to fake this costliness. Bitcoin's PoW ensures the cost to mine a Bitcoin is near equivalent to how much it would cost to purchase one on an exchange. The [unforgeable costliness](#) pattern includes the following basic steps:

“(1) find or create a class of objects that is highly improbable, takes much effort to make, or both, and such that the measure of their costliness can be verified by other parties.

(2) use the objects to enable a protocol or institution to cross trust boundaries”
- Nick Szabo

Openly Programmable

Bitcoin is open-source; its design is public, it is usable by anyone/anywhere/anytime. Developers can freely program applications on top of the Bitcoin protocol without having to ask anyone for permission.

“It is dynamic, upgradable and extendable. It does not need throwing out and replacing with each new iteration, it will continuously improve.” — [Neil Woodfine](#)

Decentralized

In its simplest definition, decentralization means a lack of centralized control. Or the degree to which an entity within the system can resist coercion and still function as part of the system. Coercion doesn't necessarily mean force, it means negative incentives to align with an authority. Decentralization is an important trait for money because any centralized control could threaten any one of the other traits (especially [scarcity](#) and [censorship resistance](#))

Decentralization is also important because it enables greater [social scalability](#). The challenge is that [natural systems](#) inherently evolve towards centralization (hierarchies). We see this emergent property in cryptocurrencies as well. Hierarchy is an emergent property of networks. When we consider more complex systems, we must contend with more [complex relationships](#) between the layers. Quantifying decentralization is an especially [thorny](#) issue.

Decentralization is such a misunderstood concept, because people apply it to a whole system, when really it needs to be applied to multiple layers within the system: The Protocol, The Politics and The Practical.—Sarah Lewis

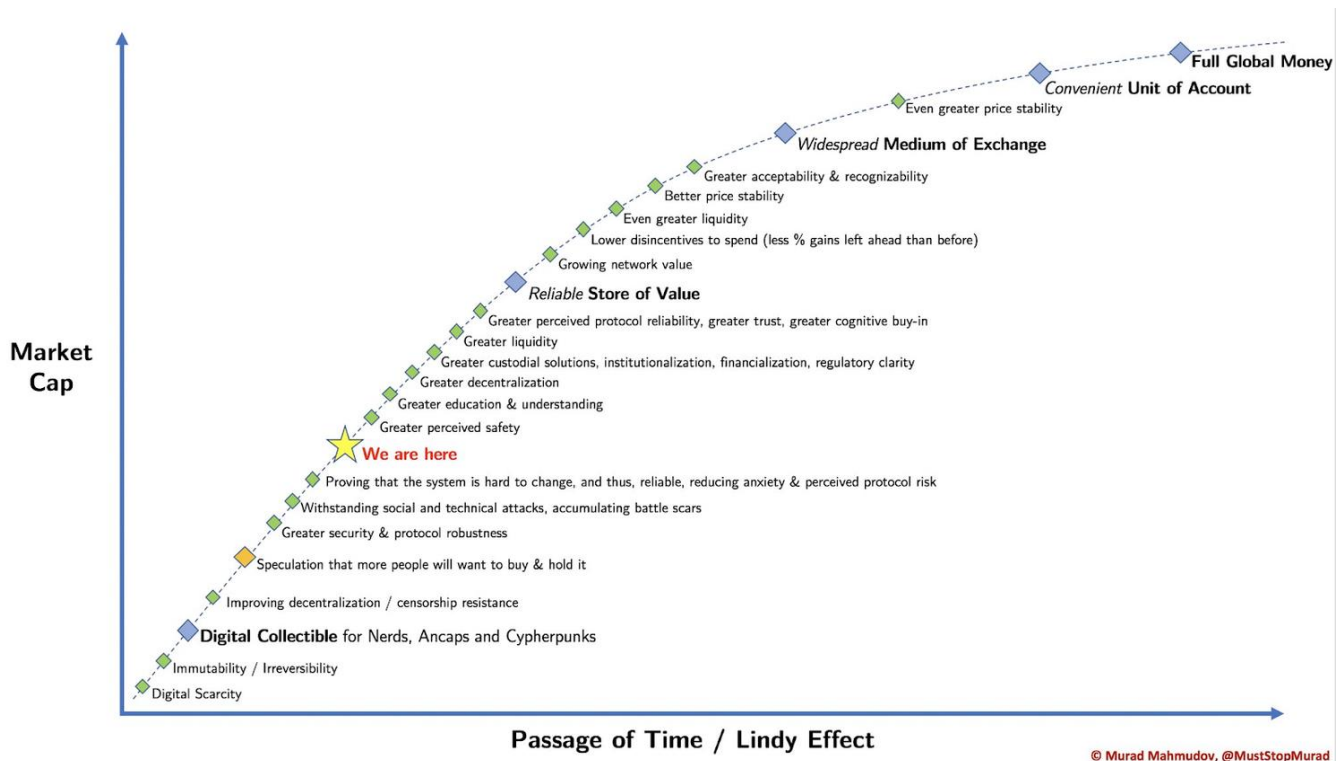
Evolution

For a species of money to survive, it needs to be competitive on every attribute and be exceptionally better on a few of them. Attributes don't sum, they multiply.

When Gold was first introduced, the bead makers (an example of a more primitive form of money) probably tried to convince the ignorant population that gold was no substitute for beads. But it turned out that gold had traits that were more advantageous. It did not matter what anyone thought. Gold was destined to be a more powerful currency than shells or beads.

The fact that gold has remained a valued commodity for thousands of years speaks to the importance of these specific traits. In fact, the combination of traits possessed by gold and other precious metals eventually provided the foundation for the next evolution in money, fiat currency. In money's next evolution of species, fiat currency fulfilled several critical traits to an even greater degree than gold. Paper was more portable and could be more easily transacted. That is not to say it was entirely superior. In many cases, fiat currencies lacked durability, and as we will see, would eventually become less and less scarce (due to inflation) The critical flaw: its supply was controlled by kings and governments and increasingly used as a tool to wield power and control. Upon every new iteration of species, they each evolve in the following four stages (taken from "[The Bullish Case for Bitcoin](#)"):

1. **Collectible.** In the very first stage of its evolution, money will be demanded solely based on its peculiar properties, usually becoming a whimsy of its possessor. Shells, beads and gold were all collectibles before later transitioning to the more familiar roles of money.
2. **Store of value:** Once it is demanded by enough people for its peculiarities, money will be recognized as a means of keeping and storing value over time. As a good becomes more widely recognized as a suitable store of value, its purchasing power will rise as more people demand it for this purpose. The purchasing power of a store of value will eventually plateau when it is widely held and the influx of new people desiring it as a store of value dwindles.
3. **Medium of exchange:** When money is fully established as a store of value, its purchasing power will stabilize. Having stabilized in purchasing power, the opportunity cost of using money to complete trades will diminish to a level where it is suitable for use as a medium of exchange.
4. **Unit of account.** When money is widely used as a medium of exchange, goods will be priced in terms of it. I.e., the exchange ratio against money will be available for most goods.



Bitcoin's stage in the evolutionary process is shown below, provided by [Murad Mahmudov](#)

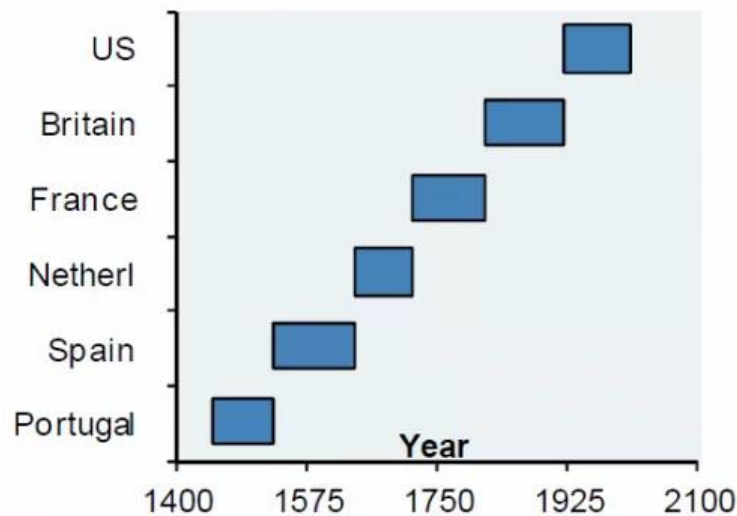
Survival and Extinction

Extinction can most simply be described as the failure of a species to compete in an environment to such a degree that it eventually ceases to exist. The inability to compete itself may be the result of two primary causes; increased competition from superior species or a dramatic change in environment.

“Charles Darwin’s theory of natural selection originated to provide an evidence-based explanation of the past. We now leverage this theory to look forward and understand its implications on the future of currency. Given the ever-changing conditions of the future, will gold and fiat currencies continue to compete or go the way of the dinosaur?” —Ryan Walker [“On the Origins of Money: Darwin and the Evolution of Cryptocurrency”](#)

According to a study of 775 fiat currencies by [DollarDaze.org](#) the average life expectancy of a fiat currency is 27 years. The study also indicated the most common causes of any given currencies extinction are hyperinflation, monetary reform, war and independence. Looking towards the fittest of fiat currencies, those that become reserve currencies, we find that most last just under 100 years. (Note: US currency only starts from 1933 because USD was redeemable for gold prior to that)

(c37) Reserve currency status does not last forever



JPM, Hong Kong Monetary Authority, December 2011

With fiat currencies being so susceptible to failure, gold has long served as an alternative as it is more scarce and durable. In terms of scarcity, fiat currencies can be printed and inflated at the will of their authorities.

“While Bitcoin is a new invention of the digital age, the problems it purports to solve—namely, providing a form of money that is under the full command of its owner and likely to hold its value in the long run—are as old as human society itself” — [Saifedean Ammous](#)

The currencies are in a state of hyper-evolution as they continue to take on a varied array of distinctive traits that set them apart from one another within their own competitive ecosystem (fiat/crypto).

Equally as threatening to traditional forms of money, the conditions of the environment in which currencies compete is in a constant state of change. Undertones of growing distrust in centralized entities encourage populations to consider alternative stores of value.

Sovereignty, once a trait that was necessary for the survival of a currency, may now be falling out of favor. Centralized failures such as the US financial crisis of 2008 or hyper-inflated fiat currencies such as Zimbabwe dollars or Argentinian pesos compound these sentiments. The most profound of these conditions is the growing awareness throughout the world that decentralized trust is possible.

Instead of becoming anti-fragile, which is the property of growing stronger in a volatile and stressful environment, central banks have removed danger and mortality from failure, which causes competition to stagnate or degrade.

Sometimes stressors are so strong that they are fatal for a species of money. While this is devastating for the money itself, the population comprised of those that survive are fitter on average. This isn't because any of the survivors grew stronger from the stress, but simply because the weaker monies were removed.

"We humans regularly underestimate high-impact, [long-tail events](#). Careful consideration of long tail events is especially important in the design of a protocol that has the potential to become the backbone of the global economy" – [Hugo Nguyen](#)

It is interesting to imagine what Charles Darwin would make of the current state of money. History would have us believe that the existence and survival of any entity, be it plant, animal, corporation, or money is subject to the laws of natural selection.

With this understanding, it is hard to imagine Darwin contesting the opinion that Bitcoin possesses the necessary traits to become the dominant species of money.

Bitcoin has been perfectly honed for its environment through its exceptional genetic code and the manifestation of that code in the form of superior traits.

Bitcoin is the apex predator of money and is constantly evolving. None of the previous monetary life forms stand a chance.

Links

- <http://pricesandmarkets.org/wp-content/uploads/2015/02/Luther-Olson-4.pdf>
- <https://blog.picks.co/pow-is-efficient-aa3d442754d3>
- <https://twitter.com/AriDavidPaul/status/1053007190552956928>
- <http://www.aei.org/publication/sound-money-vs-stable-money/>
- <https://satoshi.nakamotoinstitute.org/emails/cryptography/6/#selection-209.0-221.16>
- <https://satoshi.nakamotoinstitute.org/emails/cryptography/15/#selection-111.0-113.67>
- <http://p2pfoundation.ning.com/forum/topics/bitcoin-open-source?commentId=2003008%3AComment%3A9562>
- <https://grisha.org/blog/2018/01/23/explaining-proof-of-work/>
- <https://mobile.twitter.com/SauceryCoin/status/1049184561974800384>
- <https://medium.com/u/9efdc740067f>
- <https://medium.com/@vijayboyapati/the-bullish-case-for-bitcoin-6ecc8bdecc1>

- <http://www.cbc.ca/beta/news/canada/ottawa/fake-gold-wafer-rbc-canadian-mint-1.4368801>
- https://en.wikipedia.org/wiki/Gold_fingerprinting
- <https://www.dw.com/en/germany-repatriates-gold-reserves-ahead-of-schedule/a-40208045>
- <https://en.wikipedia.org/wiki/Antifragility>
- <https://news.nationalgeographic.com/2016/07/deep-sea-mining-five-facts/>
- <http://web.mit.edu/12.000/www/m2016/finalwebsite/solutions/asteroids.html>
- https://en.wikipedia.org/wiki/Hoxne_Hoard
- https://en.wikipedia.org/wiki/Lindy_effect
- <http://www.worldometers.info/world-population/>
- https://en.wikipedia.org/wiki/The_Gold_%28Control%29_Act,_1968
- <https://medium.com/u/becf6824fd89>
- <http://unenumerated.blogspot.com/2008/08/>
- <https://twitter.com/nwoodfine/status/981435332506906626>
- https://inflationdata.com/Inflation/Inflation/Cumulative_Inflation_by_Decade.asp
- <https://www.swift.com/our-solutions/compliance-and-shared-services/financial-crime-compliance/sanctions-solutions/sanctions-screening>
- <http://unenumerated.blogspot.com/2017/02/money-blockchains-and-social-scalability.html>
- <https://journals.plos.org/ploscompbiol/article/file?id=10.1371/journal.pcbi.1004829&type=printable>
- <https://twitter.com/SarahJamieLewis/status/1029217138601418753>
- <https://twitter.com/coindesk/status/1048786254245126144>
- <https://medium.com/u/e1c7b66721d6>
- <https://www.coindesk.com/origins-money-darwin-evolution-cryptocurrency/>
- <http://dollardaze.org/>
- https://en.wikipedia.org/wiki/Long_tail
- <https://medium.com/u/3efc6d31e61c>

Planting Bitcoin - Season (2/4)

Central Banks and the 2008 Financial Crisis

By [Dan Held](#)

Posted January 6, 2019

"The root problem with conventional currency is all the trust that's required to make it work. The central bank must be trusted not to debase the currency, but the history of fiat currencies is full of breaches of that trust. Banks must be trusted to hold our money and transfer it electronically, but they lend it out in waves of credit bubbles with barely a fraction in reserve." — Satoshi Nakamoto

Introduction

In my last article, "[Species](#)," I covered why Satoshi's design of Bitcoin's genetic code made it the best species of money ever created.

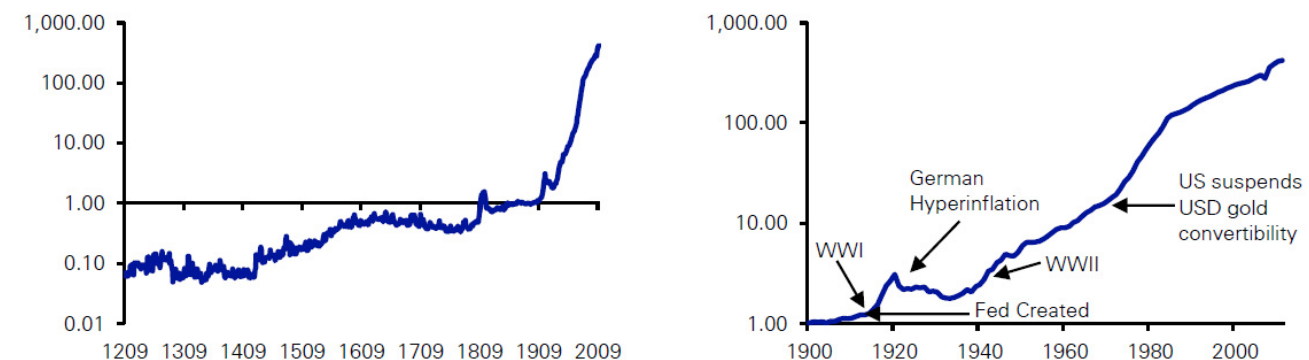
Satoshi had begun crafting Bitcoin's genetic code in [2007](#) but had waited for the right moment to plant the seed, the right moment in which the world would understand and embrace what he had created. In this article, I will dive into the moment in which Satoshi precisely chose to plant the Bitcoin seed.

Central Banks

From the founding of the Bank of England, central banks have been used as a means for states to fund their policies without risking the popular ire caused by direct taxation. When the capital provided by central banks is misallocated by either the state or in a market distorted by artificially low interest rates, an inevitable collapse occurs. The central bank is the root of these periodic market dislocations.

"I believe the root cause of every financial crisis, the root cause, is flawed government policies" — [Henry Paulson](#) (US Treasury Secretary during the 2008 financial crisis and former Goldman Sachs CEO)

Figure 18: Global Median Inflation Series since 1209 (left) and 1900 (right)



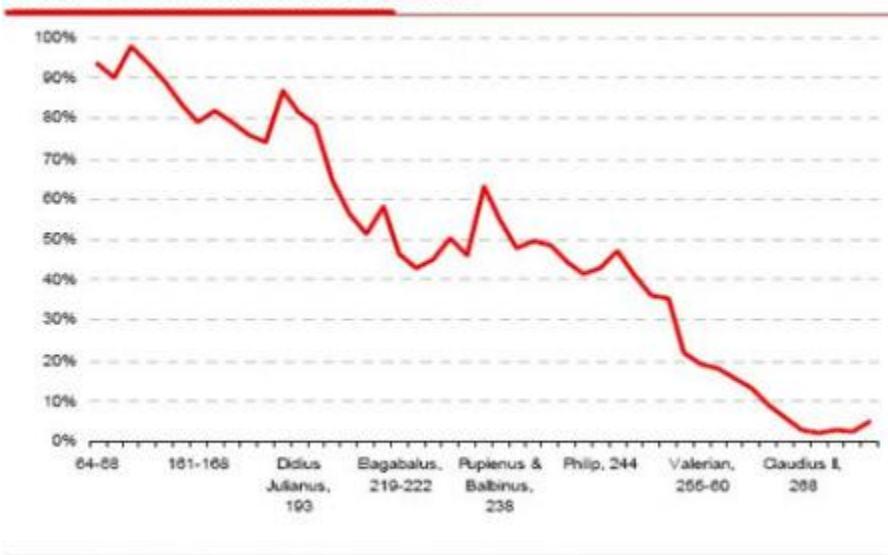
Source: Deutsche Bank, GFD

(There hasn't been a year of global deflation since 1933)

With the recent market dislocation, investors were bailed out. Unfortunately, you cannot subsidize irresponsibility and expect people to become more responsible. Prior to the 20th century, ordinary people could always flee to gold to save themselves from the effects of the [failed](#), inflationist, policies of the central bank. This ended across much of the world in the 20th century as gold was outlawed.—[Vijay Boyapati](#)

“In the absence of the gold standard, there is no way to protect savings from confiscation through inflation. There is no safe store of value.” — [Alan Greenspan](#) (Former Chairman of the Federal Reserve)

Silver content of a Roman denarius



Source: <http://www.tulane.edu/~august/handouts/601cprin.htm>

The standard Roman silver coin

Early 2007

Satoshi Nakamoto, after years and years of research, starts [coding](#) up Bitcoin.

2008 Financial Crisis

“The problem had grown so big that the end was bound to be cataclysmic and have big social and political consequences” — Michael Lewis (Big Short)

January

Fed tries to stop the housing bust

The Federal Market Open Committee began lowering the fed funds rate (to 3.0%). There were [57 percent more foreclosures](#) than 12 months earlier

February

Bush signs tax rebate as home sales continue to plummet

February 13: President [Bush signed a tax rebate](#) bill to help the struggling housing market. The bill increased limits for [FHA loans](#) and allowed [Freddie Mac](#) to repurchase jumbo loans.

March

Fed begins bailouts

March 14: The Federal Reserve held its first emergency weekend meeting in 30 years.

March 17: The Federal Reserve announced it would guarantee [Bear Stearns'](#) bad loans.

March 18: The Federal Open Market Committee lowered the fed funds rate by 0.75 percent to 2.25 percent. It had halved the interest rate in six months. That same day, federal regulators agreed to let Fannie Mae and Freddie Mac take on [another \\$200 billion](#) in subprime mortgage debt.

April–June

The Fed buys more toxic bank debt

June 2: The Fed auctions totaled \$1.2 trillion. In June, the Federal Reserve lent \$225 billion through its Term Auction Facility.

July

IndyMac bank fails

July 11: The [Office of Thrift Supervision closed](#) IndyMac Bank. Los Angeles police warned angry IndyMac depositors to remain calm while they waited in line to withdraw funds from the failed bank.

July 23: Secretary Paulson made the Sunday talk show rounds. He explained the need for a [bailout](#) of Fannie Mae and Freddie Mac. The two agencies themselves held or guaranteed [more than half of the \\$12 trillion](#) of the nation's mortgages.

August

August 18: Satoshi [registers](#) Bitcoin.org through [anonymousspeech.com](#)

September *Global panic*

September 7: Treasury nationalizes [Fannie and Freddie](#) and will run the two until they are strong enough to return to independent management. The [Fannie and Freddie bailout](#) initially cost taxpayers \$187 billion.

September 15: Lehman Brothers files for chapter 11 bankruptcy, the [largest bankruptcy filing in U.S. history](#) with over \$600B in assets. The bankruptcy triggered a one-day drop in the Dow Jones Industrial Average of 4.5%, the largest decline since the September 11, 2001 attacks. Later that day, [Bank of America officially announced](#) it would purchase struggling Merrill Lynch for \$50 billion.

*"It's terrible. Death. Like a massive earthquake." — Kirsty McCluskey
a Lehman trader in London*

September 16: Fed buys AIG for \$85 Billion. The company had insured trillions of dollars of mortgages throughout the world. If it had fallen, so would the global banking system. On that same day, the [Reserve Primary Fund](#) "broke the buck." It didn't have enough cash on hand to pay out all the redemptions that were occurring.

*"I asked my wife to please go to the ATM and take as much cash as she could. When she asked why, I said it was because I didn't know whether there was a chance that banks might not open." —
[Mohamed El-Erian](#) (One of the most powerful economists/leaders in finance)*

September 17: Economy on the brink of collapse. Panic spreads. Investors withdrew a record \$144.5 billion from their money market accounts. During a typical week, only about \$7 billion is withdrawn. If it had continued, businesses couldn't get money to fund their day-to-day operations. In just a few weeks, shippers wouldn't have had the cash to deliver food to grocery stores.

October *Bailouts*

October 3: Bitcoin whitepaper PDF likely [created](#) (not the first time it was written, but the first time it was prepared for publishing)

The same day, the [bank bailout bill](#) allowed Treasury to buy shares of troubled banks. It was the fastest way to inject capital into the frozen financial system. Despite this, global stock markets continue to collapse.

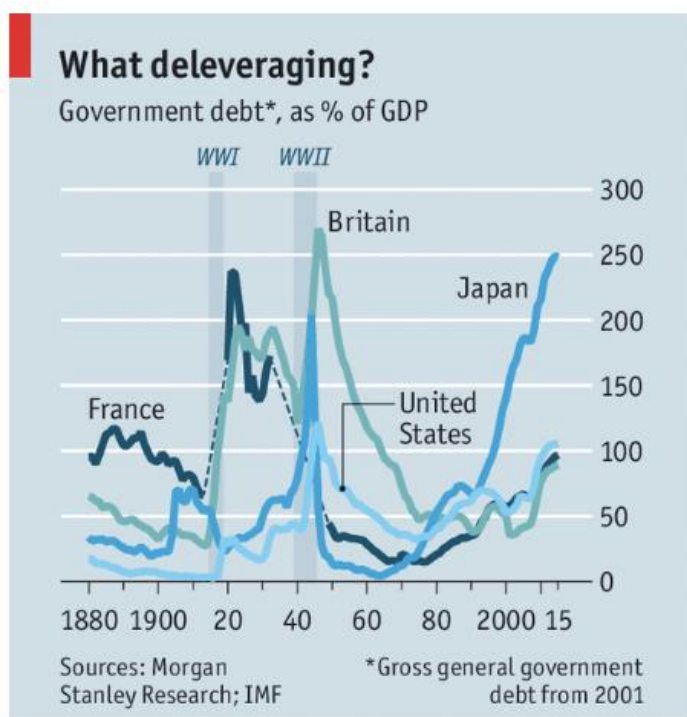
"Just as our politics are falling apart, our portfolios are falling apart, too." — Ben Hunt

October 7: The Federal Reserve agreed to issue short-term loans for businesses that couldn't get them elsewhere, to the tune of \$1.7 Trillion.

October 13: Treasury Secretary Hank Paulson sits down with 9 major bank CEOs. The total bailout package looks more like \$2.25 trillion, well more than the original \$700 billion available.

"September and October of 2008 was the worst financial crisis in global history, including the Great Depression" — Ben Bernanke

October 14: The governments of the EU, [Japan](#), and the United States again took unprecedented [coordinated action](#). The EU committed to spending \$1.8 trillion to guarantee bank financing, buy shares to prevent banks from failing, and take any other steps needed to get banks to lend to each other again. This was after the UK committed \$88 billion to purchase shares in failing banks and \$438 billion to guarantee loans. In a show of solidarity, the Bank of Japan agreed to [lend unlimited dollars](#).



Economist.com

Debt/GDP ratios are at wartime highs. Central banks haven't unwound their 2008 trade

October 21—Fed lends \$540 Billion to bail out money market funds which are continuing to meet a barrage of redemptions.

"People feel like nothing in the country is working—the president, Congress, corporations." (October 15,

2008) [Reuters](#)

October 31: Satoshi publishes the Bitcoin whitepaper

Walking on the street in a city Satoshi looks around and notices a businesswoman on her blackberry, hailing a cab. He passes a newspaper stand and sees Miley Cyrus' (known as Hannah Montana) controversial photos in [Vanity Fair](#), she's 15.

George Bush's approval rating is at a record low of 21%, Congress is at 10%—just above its all-time low. Lehman Brothers had just collapsed a month prior.

"Is now the time? Is the world ready?" Satoshi thought to himself. He had spent the last few years coding up Bitcoin then writing the whitepaper. He had patiently waited to release it to the world, but the moment had to be right... there was only one shot at this. "Is the whitepaper easy enough to read? I want to make sure this resonates with the cypherpunks, I'm hoping cash will be most understandable to the other members on the mailing list who have previously created e-currencies."

"When the moment is ripe, a fanatic leader galvanizes the ripe population and pushes it to a point of no return. The leader translates the ideals published by the "men of words [cypherpunks]" into doctrines [whitepaper] promising sudden and spectacular change." — Eric Hoffer, author of "[The True Believer](#)" (via [Tony Sheng](#))

He returned to his home and reviewed the whitepaper for any glaring mistakes the 47th time, he couldn't find any. He leaned back and stared at the wall. He realized this was the moment, it was time to plant the seed. He popped open his e-mail client, checked the draft e-mail to the cryptographer (cypherpunk) e-mailing list and pressed send. There was no going back.

"Indeed, Bitcoin rose like a phoenix from the ashes of the 2008 global financial catastrophe — a catastrophe that was precipitated by the policies of central banks like the Federal Reserve." — [Vijay Boyapati](#)

With the 2008 financial crisis, trust had been lost in a world that ran on trust.

Bitcoin was launched in a time of absolute necessity, Satoshi planted the seed at precisely the right moment.

Links

- https://www.huffingtonpost.com/2013/08/27/hank-paulson-cause-of-financial-crisis_n_3822417.html
- <https://mises.org/library/how-central-banking-increased-inequality>
- <https://medium.com/u/9efdc740067f>
- https://en.wikipedia.org/wiki/Alan_Greenspan
- <https://satoshi.nakamotoinstitute.org/emails/cryptography/15/>
- <http://www.realtor.org/rmodaily.nsf/pages/News2008022602>
- <https://www.thebalance.com/bush-economic-stimulus-package-3305782>
- <https://www.thebalance.com/fha-loan-basics-315656>
- <https://www.thebalance.com/what-is-freddie-mac-3305985>
- <https://www.thebalance.com/bearn-stearns-collapse-and-bailout-3305613>
- <http://www.washingtonpost.com/wp-dyn/content/article/2008/03/20/AR2008032003018.html>
- <https://www.stlouisfed.org/financial-crisis/full-timeline>
- <https://www.thebalance.com/what-was-the-fannie-mae-and-freddie-mac-bailout-3305658>
- <https://www.cnn.com/id/25799253>
- <https://open.spotify.com/user/txdan2010/playlist/3X0JDW2W59uQ6Yx2J2X3XW?si=YpoSB0bLSSuaUoUhh7ACIA>
- <https://www.businessinsider.com/bitcoin-history-cryptocurrency-satoshi-nakamoto-2017-12>
- <https://bitcointalk.org/index.php?topic=103369.msg1135218#msg1135218>
- https://money.cnn.com/2008/09/07/news/companies/fannie_freddie/index.htm?eref=edition_business
- https://en.wikipedia.org/wiki/Chapter_11,_Title_11,_United_States_Code#Largest_cases
- <https://www.cnn.com/id/26708319>
- <https://www.thebalance.com/reserve-primary-fund-3305671>
- <https://www.businessinsider.com/tales-of-the-financial-crisis-2009-9>
- <https://www.gwern.net/docs/bitcoin/20081003-nakamoto-bitcoindraft.pdf>
- <https://www.thebalance.com/what-was-the-bank-bailout-bill-3305675>
- <https://www.thebalance.com/japan-s-economy-recession-effect-on-u-s-and-world-3306007>
- <https://www.theguardian.com/business/2008/oct/13/creditcrunch-marketturmoil>
- <https://ftalphaville.ft.com/2008/10/15/17051/boj-offers-unlimited-dollars-to-banks/>

- <https://www.reuters.com/article/us-financial-usa-poll/u-s-mood-plummets-as-crisis-deepens-reuters-poll-idUSTRE49E3ML20081015>
- <https://www.cbsnews.com/news/top-pop-culture-moments-of-2008/>
- <https://www.tonysheng.com/mass-movement>
- <https://medium.com/u/be4506861043>

Planting Bitcoin—Soil (3/4)

By [Dan Held](#)

Posted January 6, 2019

Introduction

In my last article, "[Season](#)," I covered the precise moment in which Satoshi planted Bitcoin, the 2008 Financial Crisis. In this article, I cover the Cypherpunks or the "Soil" in which he planted the Bitcoin seed giving it the best chance for survival.

Cypherpunks

Sending the Bitcoin whitepaper to the cryptography mailing list on October 31, 2008 was the obvious choice. This was the right group to gather feedback from, the right channel to engage with. The list was predominately populated by the [Cypherpunks](#)* who were activists advocating widespread use of strong cryptography, as a route to social and political change.

*"Cypherpunks" is a play on the word 'cipher' or 'cypher', for encryption; and cyberpunk a genre of sci-fi.

The group was originally comprised of Eric Hughes, Tim May, and John Gilmore. At first, the meetings were in-person meetings in the San Francisco Bay Area, but they decided to expand the group via the cryptographer mailing list which would allow them to reach other Cypherpunks. The mailing list was a place to exchange ideas freely through the use of encryption methods, such as PGP, to ensure complete privacy. The basic ideas behind this movement can be found in the [Cypherpunk manifesto](#) written by Eric Hughes in 1993. The key principle which underpins the manifesto is the importance of privacy and finality in transactions—[PetriB](#)

"Therefore, privacy in an open society requires anonymous transaction systems. Until now, cash has been the primary such system." — [A Cypherpunk's Manifesto](#)

We want the ability to ensure that others cannot use the information in the history of our transactions [against us](#). For example: a purchase indicating that someone is wealthy, an embarrassing purchase, or one that would make you subject to spam or harassment. We do not want our financial purchase to haunt us further down the road. We want an endpoint beyond which we do not have to worry about further contingencies. **In the world of payments, this is closely related to the concept of "finality"**—ideally we want to be able to state with certainty that at some point the

payment has been made, the debt has been cleared, and the funds are secure. But recent developments have increased the ability for more powerful parties to clawback funds (via trusted third parties, legal funds, etc).

We hope that existing laws would provide protection against these difficulties. However, we can remove that moral hazard by not having to trust third parties or more powerful adversaries which can revert transactions solely based on their capabilities. This is what the Cypherpunks were fighting for with cryptography. They were the “[Men of words](#),” or anti-establishment intellectuals that laid the foundation for individuals like Satoshi to come along.

*“The words of **anti-establishment intellectuals sow the seeds for revolution**. They present ideas and sometimes discredit the establishment, **paving the way for a charismatic leader to package their thinking into a movement**.” — [Tony Sheng](#)*

Elliot Alderson, the “Cypherpunk” in the fictional show “Mr. Robot.” He joins a group that aims to destroy all debt records by encrypting the financial data of the largest conglomerate in the world, E Corp.

Elliot Alderson, the “Cypherpunk” in the fictional show “Mr. Robot.” He joins a group that aims to destroy all debt records by encrypting the financial data of the largest conglomerate in the world, E Corp.

The first attempts at making an anonymous transacting system were made by Cypherpunks on that cryptographer mailing list, including:

- Adam Back, the inventor of [hashcash](#), the proof-of-work (PoW) system used by several anti-spam systems. A similar PoW system is used in bitcoin
- Nick Szabo, designed a mechanism for a decentralized digital currency he called “bit gold.” Bit gold was never implemented, but has been called “a direct precursor to the Bitcoin architecture”
- Wei Dai, who published “b-money”, an “anonymous, distributed electronic cash system”
- Hal Finny, who created the first reusable proof of work system before Bitcoin (And in January 2009 he became Bitcoin network’s first transaction recipient). He was also a developer of the secure communication method known as Pretty Good Privacy (PGP)
- David Chaum, founded DigiCash (1989) as a form of centralized “electronic money” that deployed the same kinds of cryptographic protocols—public key cryptography—that support the nature of bitcoin transactions. It is often called “Chaumian eCash.”

Satoshi cites many of these Cypherpunks in the Bitcoin whitepaper and references their influence on Bitcoin's development in public statements made post code launch.

*"Bitcoin is an implementation of **Wei Dai's b-money** proposal... and **Nick Szabo's Bitgold** proposal" — [Satoshi Nakamoto](#)*

In fact, Satoshi thought he was late to cryptocurrency! While the Cypherpunks had attempted many times to genetically code a species of money that would survive, none had been successful.

*"A lot of people **automatically dismiss e-currency as a lost cause because of all the companies that failed since the 1990's**. I hope it's obvious it was only the centrally controlled nature of those systems that doomed them. I think this is the first time we're trying a decentralized, non-trust-based system." — [Satoshi Nakamoto](#)*

He had written the whitepaper to fit his target audience, the Cypherpunks. That's why he uses the words "electronic cash", "proof-of-work," etc. which was previously used terminology in the other Cypherpunk whitepapers. He uses an ecommerce example to make it easier for everyone to comprehend. He's crafting a narrative that will resonate with the Cypherpunks, to get them interested and involved. **Bitcoin was the holy grail—it had solved the problem of finality and provided a small measure of privacy.** The source code implementation was his product spec.

*"The **functional details** are not covered in the paper, but the sourcecode is coming soon." — [Satoshi Nakamoto](#)*

The following things not described in the whitepaper, but are included in the source code: 21M hard cap, 10 minute blocks, 1 MB block caps. Those were incredibly important components of Bitcoin. The whitepaper was merely a teaser.

*"If the Bitcoin Whitepaper is the **Declaration of Independence**, the Source Code is the **Constitution**" — [Pierre Rochard](#)*

In true Cypherpunk fashion, the publication of Satoshi's whitepaper (October 2008) was quickly followed by code release in January 2009. The notion that good ideas need to be implemented, not just discussed, is very much part of the culture of the mailing list.

*"**Cypherpunks write code.** We know that someone has to write software to defend privacy, and since we can't get privacy unless we all do, we're going to write it. **We publish our code so that our fellow***

Cypherpunks may practice and play with it. Our code is free for all to use, worldwide...We know that software can't be destroyed and that a widely dispersed system can't be shut down. — A
Cypherpunk's Manifesto

Importantly, Satoshi didn't [premine](#) any Bitcoins. Satoshi gave the Cypherpunks a two month heads up before mining the Genesis block. To prove fairness, he included a proof of no [premine timestamp](#) in the [Genesis Block](#) of the Bitcoin blockchain. It carried a strong political message. What he was trying to accomplish was clear—they were building a new financial system. Bitcoin wasn't merely digital cash, it was an alternative to banks.

"The Times 03/Jan/2009 Chancellor on brink of second bailout for banks" — Genesis Block

Links

- <https://www.coindesk.com/the-rise-of-the-cypherpunks/>
- <https://www.activism.net/cypherpunk/manifesto.html>
- <https://medium.com/@Petri.basson>
- <https://research.stlouisfed.org/publications/review/2018/07/16/payment-systems-and-privacy>
- <https://www.tonysheng.com/mass-movement>
- <https://medium.com/@tonysheng>
- <https://en.wikipedia.org/wiki/Hashcash>
- <https://bitcointalk.org/index.php?topic=342.msg4508#msg4508>
- <http://p2pfoundation.ning.com/forum/topics/bitcoin-open-source?commentId=2003008%3AComment%3A9493>
- <http://www.metzdowd.com/pipermail/cryptography/2008-November/014863.html>
- <https://medium.com/u/1206face71fc>
- <https://blog.picks.co/bitcoins-distribution-was-fair-e2ef7bbbc892>
- https://en.bitcoin.it/wiki/Genesis_block

Planting Bitcoin - Gardening (4/4)

By [Dan Held](#)

Posted January 6, 2019

Introduction

In my last article, "[Soil](#)," I covered the Cypherpunks or the "Soil" in which he planted the Bitcoin seed giving it the best chance for survival.

Satoshi's design of Bitcoin's genetic code made it the best species of money ever created, he waited for exactly the right moment to plant the seed, and had planted it in the most fertile soil. Now it was time to nurture Bitcoin's development.

Early Development

"The project needs to grow gradually so the software can be strengthened along the way." — [Satoshi Nakamoto](#)

Satoshi chose to be anonymous, which fit the ethos of the Cypherpunks. **People can project hopes and dreams on an anonymous individual, ensuring maximal narrative fit.** That's why a book is often better than the movie. His anonymity was a critical component of the founder story—dev worship is a dangerous thing for an open source project aiming for decentralization. Volunteers need to rely on trusting the objective reality of the code, rather than focusing on the merits of the project leader.

*"It is high time for everyone involved in BTC to stop concerning themselves with the question of the identity of Nakamoto, and accept that **it does not matter to the operation of the technology, in the same way that the identity of the inventor of the wheel no longer matters**" - [Saifedean Ammous](#)*

As a subtle jab to central banks, and as a nod to his admiration of the gold standard, he [chose](#) his birthday (on his p2p foundation website profile) as the date **the US made gold ownership illegal** through Executive Order 6102, April 5th. And he [chose](#) 1975 as his year of birth which is the year when the US citizens were allowed to own gold again.

*"[with Bitcoin] **we can win a major battle in the arms race** and gain a new territory of freedom for several years." — [Satoshi Nakamoto](#)*

In his public statements, he usually focused on ordinary, mainstream, users, with his tone sometimes even excited in suggesting many ways bitcoin could be made more convenient or useful for commerce or other things. Satoshi was practical, which made interactions very easy and comfortable. He tended to avoid philosophical discussions and political arguments.

Additionally, Satoshi took steps to signal to the Cypherpunks, and future members, that Bitcoin wasn't a scam. The conservative deescalation of his mining contributions, never spending any of his coins, nor using his influence for any purpose, shows that he wanted the world to make up their own mind about his project and judge it on its own terms. **And unlike every other founder in history, Satoshi never cashed out.**

"Bitcoin benefited from an extremely rare set of circumstances. Because it launched in a world where digital cash had no established value, they circulated freely. That can't be recaptured today since everyone expects coins to have value. Not only was it fair, but it was historically unique in its fairness. The immaculate conception." [Nic Carter](#)

Many of the early Cypherpunks became core developers in the Bitcoin protocol like Hal Finney and Adam Bach. The caliber of the early development team attracted talented (soon to be "core") developers.

*"Gifted people tend to want to work with other top people and work on something that matters, that they believe in. **Motivation matters.** Protocol design and coding is partly an artistic, aesthetic endeavour; people do their best work on a mission: uncensorable global internet money" — Adam Bach*

The Gardener Leaves

Satoshi showed a great level of restraint and took a long-term perspective on issues, as when Satoshi resisted the calls for bitcoin to market itself as a funding mechanism for Wikileaks after PayPal famously froze its account. This, Satoshi argued, would only bring down legal and regulatory hammers that much faster. Satoshi recognized the need to carefully cultivate Bitcoin.

*"I make this appeal to WikiLeaks not to try to use Bitcoin. Bitcoin is a small beta community in its infancy. You would not stand to get more than pocket change, and **the heat you would bring would likely destroy us at this stage.**" — Satoshi Nakamoto*

The connection to Wikileaks at such an early stage, at the height of what could be called public resistance against the Iraq war, probably gave Bitcoin a very different dimension. So he did not mince his words nor hide his intention for leaving in what can be called the last public statement where he says the US government was headed towards Bitcoin.

*"It would have been nice to get this attention in any other context. WikiLeaks has kicked the hornet's nest, and **the swarm is headed towards us.**"* — [Satoshi Nakamoto](#)

In April 2011, Gavin Andresen notified Satoshi that he was meeting with the CIA. **Any further involvement might give away his identity which would endanger the long-term success of the project.** Bitcoin now had enough support that he could walk away, and so he did.

"Satoshi left because he didn't want its influence to affect the protocol development creating a single point of failure. The very idea of "Satoshi Vision" itself is against Satoshi's vision for Bitcoin" — [Frederico Tenga](#)

Social Scalability

Satoshi was able to walk away because Bitcoin had trust minimization baked into the protocol. This is what made it socially scalable.

"Power and scale breed conflict and corruption, that the purest part of any revolution is the beginning." — [Dhruv Bansal](#)

It is easy to start with good intentions, however as things scale that becomes harder and harder to maintain. **Bitcoin was specially architected to be trust minimized.** Satoshi set it up so that there is no one person or group whose power can be coveted, usurped, or broken.

"Bitcoin is a social breakthrough, not a technological one"—Alex Hardy

Bitcoin needed to be the universal language for money. You are communicating with strangers worldwide, which you neither know nor trust that agree you own an abstraction of value.

"Bitcoin is a distributed incentive structure we collectively engineer and freely opt-into. It's political technology, the first of its kind. This leaderless-ness is one part of what gives Bitcoin — in particular,

beyond other cryptocurrencies today — such robustness.” — [Dhruv Bansal](#)

HODLing, the Hero's Journey

“In the beginning of a change the patriot is a scarce man, and brave, and hated and scorned. When his cause succeeds, the timid join him, for then it costs nothing to be a patriot.” — Mark Twain

Satoshi built Bitcoin for the believers in a new financial system, the HODLers, the revolutionaries. The ones who were disenfranchised with the existing financial system. The ones who would be attracted by the prospect of sudden and spectacular change in their life.

We must heed the call for a Hero's Journey (the HODLer) that is rooted in HODL. **It's not just a meme, it is representative of foundational values upon which stronger cultural memes are eventually developed.** This supports Bitcoin's cultural foundation.

“Over and over again, the financial system was, in some narrow way, discredited....The rebellion by American youth against the money culture never happened.” — Big Short

The Hero at the beginning of their Journey has values that do not agree with the values that the Hero ends up with at Journey's end. That is the entire point of undertaking the Journey, but is also what makes it so frightening. **The Hero must let go of his/her former self in the pursuit of this transformed version of themselves.** The Journey's end is unknown, but what is known is that the Journey inspires the acquisition of new knowledge, the relinquishing of outdated paradigms and the abandoning of the familiar. The HODL Journey in Bitcoin sketches a map that becomes clearer with the acquisition of knowledge.

Satoshi needed to bootstrap the network with an incentive mechanism—the block reward which (a) controlled currency supply of Bitcoin and (b) created an incentive for people to participate in the network. **Each cycle brings aboard a new set of true believers; a new set of HODLers.** They, in their turn, become strong advocates for the adoption of Bitcoin as a store of value. Contagious Freedom. [Vijay Boyapati](#)

***“Hodling bootstrapped Bitcoin into existence. Hodling increases value, which increases demand, hash rate, and network security, which, in turn, attracts new hodlers and devs. This self-reinforcing feedback loop drives Bitcoin's network effects, security, and value.”** — [@TobiasAHuber](#)*

Satoshi had encoded in Bitcoin DNA a mechanism to incentivize the participants, through the shared belief in Bitcoin manifested via HODLing.

*“In this sense, it's more typical of a precious metal. Instead of the supply changing to keep the value the same, the supply is predetermined and the value changes. As the number of users grows, the value per coin increases. **It has the potential for a positive feedback loop; as users increase, the value goes up, which could attract more users to take advantage of the increasing value.**” —*

[Satoshi Nakamoto](#)

Early HODLers believed in Bitcoin despite overwhelming negativity and false information (ex: labeled as a currency for money launderers and drug dealers, price fluctuations). HODLers had stronger risk appetite to weather the volatility of being a first mover. They're practitioners of skin in the game.

In terms of the Hero's Journey, “HODL!” is the mentor's advice to the Hero in his Journey. Its roots are firmly based on the futility of trying to beat the market (Efficient Market Hypothesis and Hayekian Distributed information both dictate that the market can't be systematically outperformed).

The increase in Bitcoin's price has corresponding virality. And as it expands, HODLing becomes popular with people with a lower risk appetite, pulling in more and more network effect into the Bitcoin black hole—[Dan McArdle](#)

Via the Lindy Effect, the longer Bitcoin remains in existence the greater society's confidence that it will continue to exist long into the future. **It slowly seeps further into the psyche of those in charge.**

“Protocols die when they run out of believers.” — [Naval](#)

The faith in a new financial system is what binds everything together. Bitcoin is not just a software project. It's a method of coordination for a large group of people who face powerful adversaries. Bitcoin isn't just a technological breakthrough, it's also a social one.

*“When people are ripe for a mass movement, they are usually ripe for any effective movement, and not solely with a particular doctrine or program. All mass movements are competitive, and the gain of one in adherents is the loss of all the others....A stable and sustainable ideology must be the foundation of all cryptocurrencies. **No amount of cryptography, or consensus protocol development will help a***

cryptocurrency with an unstable and bankrupt ideology. Stable ideologies allow communities to thrive". [Kay Kurokawa](#)

A simple example in religion is the Christian tenet that "there is one true god". This belief strengthens the religion because it weakens membership in competing religions. **Communities with unstable ideologies will eventually collapse.**

*"Unlike Bitcoin, nobody needs to explain why gold is valuable. Gold is simple. Bitcoin is complicated. So in the long run, the argument goes, Bitcoin can never replace gold... It's true that the stories we tell matter, but those stories can change. **Stories don't win over everything. Eventually, raw utility supplants tradition. Bitcoin is a serious improvement over gold and starts to displace its role, the market will respond and re-price accordingly...** To the digital native of the future, Bitcoin wallets will probably seem more natural than vaults full of useless metals painstakingly drilled out of the earth." —*
[Haseeb Qureshi](#)

Money is a winner-take-all technology, driven by network effects. The crypto with the most HODLers, therefore, is the most demanded by consumers and will be the ultimate winner.

"Bitcoin is digital gold in the eyes of [HODLers]. To some extent this group already operates on a Bitcoin Standard: investments are evaluated on their ability to yield a return in Bitcoin." [Tuur Demeester](#)

HODL forces us to extend our gaze beyond the present. It forces our present selves to contend with an alternate reality. **HODL asks us to reconfigure our present set of preferences to permit the consideration of a future Bitcoin-based digital economy.**

HODL is a noble basis for a Journey. Through the sacrifice of current consumption, **HODLing is a net benefit for everyone as it increases every coin's purchasing power.**

"No Hero fights alone; All for one, one for all. Your call to HODL need not be the same as mine; indeed, they can be very different. Yet, in the end, they all redound to the benefit of each other." — [Prateek Goorha](#)

Bitcoin promises an alternative for citizens across the world to keep their savings in a form of money that can neither be confiscated nor diluted. If Bitcoin grows much larger, it may force governments to become a voluntary organization. **Through HODLing, we may finally be free.**

'The secret to happiness is freedom; the secret to freedom is courage' — Thucydides

Those who opt-in to Bitcoin, are trading something abundant for something scarce, **trading the past for the future, trading financial dependence for financial sovereignty.**

Conclusion

Satoshi architected the perfect genetic code necessary to a new species of money, Bitcoin. He then waited for the precise moment to plant the new species, the 2008 Financial Crisis. At that moment, he distributed the whitepaper to the only group that cared—the Cypherpunks. And finally, he nurtured Bitcoin to a stage where it no longer needed him.

Many digital cash systems came and went over the years before Bitcoin and after Bitcoin. Most were just whitepapers, some wrote and developed code, some even built a community, but it will be extremely difficult to repeat the success of Bitcoin's planting.

"Let the future tell the truth, and evaluate each one according to his work and accomplishments. The present is theirs; the future, for which I have really worked, is mine." — Nikola Tesla

Links

- <https://bitcointalk.org/index.php?topic=1735.msg26999#msg26999>
- <https://medium.com/@saifedean>
- <http://p2pfoundation.ning.com/profile/SatoshiNakamoto>
- <http://www.metzdowd.com/pipermail/cryptography/2008-November/014823.html>
- https://medium.com/@nic_carter
- https://www.youtube.com/watch?v=dTILX-_JzTs
- <https://bitcointalk.org/index.php?topic=2216.msg29280#msg29280>
- <https://mobile.twitter.com/FedericoTenga/status/1019726734210555904>
- <https://medium.com/@shrubvandal>
- <https://medium.com/@vijayboyapati>
- <https://twitter.com/TobiasAHuber>
- <http://p2pfoundation.ning.com/forum/topics/bitcoin-open-source?commentId=2003008%3AComment%3A9562>
- <https://medium.com/@robustus>
- <https://twitter.com/naval>
- <https://medium.com/@kaykurokawa>

- <https://hackernoon.com/we-already-know-blockchains-killer-apps-f2d443eba35>
- <https://medium.com/@tuurdemeester>
- <https://medium.com/@goorha>

Bitcoin: Winner Takes Most or Winner Takes All?

Exploring market share capture in cryptocurrencies

By [Misir Mahmudov](#) and [Yassmine Elmandjra](#)

Posted January 7, 2019

This series will explore how the winner-takes-all or winner-takes-most notion applies to the cryptocurrency market. In Part I, we will provide a high-level overview on the evolution of monetary systems up to the inception of cryptocurrencies, shedding light on the limitations of previous forms of money. In Part II, we will explain why the clear winner, likely Bitcoin, should capture most, if not all cryptocurrency market share. In Part III, we will apply this reasoning to the global economy and determine the extent to which the cryptocurrency market may capture a share of global base money.

Part I: The Quest for a Global Money

Before the rise of any universal monetary standards, barter was a common means of direct exchange. Subject to the problem of coincidence of wants, civilization came to understand the impracticability of barter. In an attempt to provide a solution to this impracticability, indirect exchange emerged and was made possible with intermediary goods such as seashells, glass beads, and cattle. Over time, modern technologies (like mass utilization of hydrocarbon fuel energy and importation) considerably advanced manufacturing and transportation, making the world increasingly connected. Exploration and intercontinental trade became more prevalent, and the standard traits of money evolved to accommodate a more global context. This ultimately undermined existing media of exchange, as the lack of absolute scarcity and low costs of production could not provide money guarantees and were exploited by increasingly advanced technologies. Specifically, outside groups learned how to easily reproduce region-specific forms of money. Unaware of the absolute abundance of their money, nations suffered severe wealth dilution. [1]

As the limitations in existing forms of money began to manifest, specific properties of monetary goods emerged that better fulfilled money's store of value and medium of exchange functionalities, including scarcity, durability, portability, fungibility, verifiability, divisibility, and established history. Through a process of monetary natural selection, goods competed with each other based on these demanded attributes and in the 19th century, the world converged to gold as the global monetary standard.

With the rise of gold, other forms of commodity money took form. Silver as a money was popularized because of the high costs associated with using gold in day-to-day

trade. Silver's lower value per unit weight relative to gold made it easier to use for smaller transactions. [2] For centuries, the gold to silver ratio remained between 12 and 15 and was recognized as the bimetallic standard. But this bimetallic standard ended up as nothing but a temporary phenomenon adopted to overcome insufficient technology. With the introduction of paper money backed by gold, which gave people the ability to trade any amount of value represented in gold terms, silver's monetary role was subsequently reduced. The graph below shows how rapidly the gold to silver ratio soared after the popularization of paper money.



Gold / Silver Ratio <https://www.goldbroker.com/news/gold-and-silver-correlation-988>

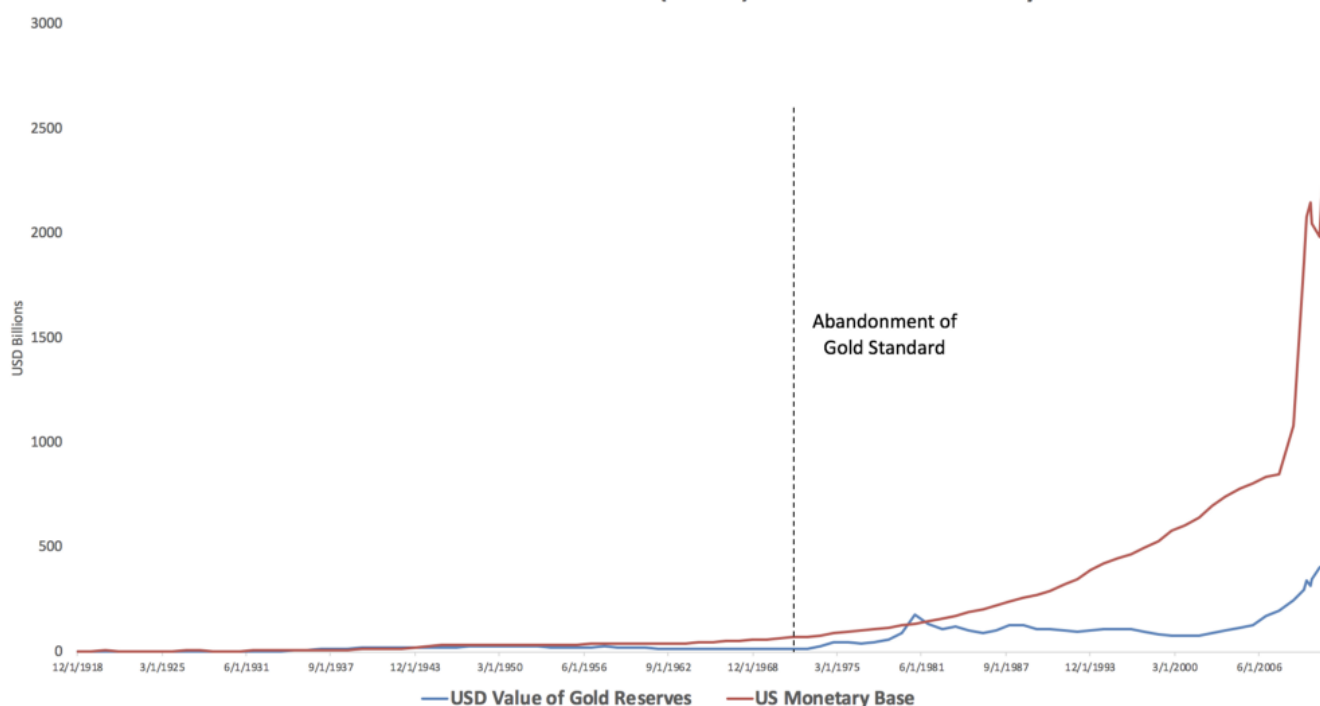
Through financialization, gold's limitations to serve as a global money began to surface. In particular, gold's physical nature and high value per unit weight made it vulnerable to centralization and its detrimental effects. With gold's lack of portability and the high friction in using a scale to measure the amount of gold in every transaction, the state intervened to establish standardized units by minting (coining)

gold coins. As citizens got acclimated with the conferred legitimacy and the infrastructure built around standardized units, the state felt comfortable engaging with what is known as '[coin clipping](#)', a form of debasement whereby jurisdictions would reduce the content of gold in a coin and use the excess gold to finance expenditure at the cost of citizens.

Later, goldsmiths, who provided services for custodying precious metals, introduced promissory notes (IOUs) that were redeemable for metals. These notes (paper money) eventually became commonly used in exchange. The goldsmiths understood that they could lend out more notes than gold they had stored in their vaults because people were unlikely to simultaneously redeem their gold reserves. This practice became known as fractional reserve banking. Goldsmiths, which later became banks, issued receipts in excess of the represented metal and generated massive profits as a result.

The 18th and the 19th centuries saw the formalization of the Gold Standard as the proliferation of banknotes and the less sound nature of silver made itself known. The Gold Standard was a monetary system whereby a country's monetary supply was directly linked to the value of its gold reserves, putting a cap on a nation's ability to inflate supply. By the 20th century, states began exploiting the limitations of gold and abusing the practice of fractional reserve banking, ultimately removing its viability as a global money. The US was able to centralize gold reserves, often forcefully confiscating gold from its citizens, [3] and began printing money in excess of their underlying reserves. Instead of attempting to redeem themselves, the US under Richard Nixon cancelled the convertibility of the dollar into gold and officially abandoned the Gold Standard in 1971. Ties between gold and paper money were in turn severed, marking the beginnings of fully unbacked fiat currencies. Below is a chart of the US monetary base expansion relative to the value of US gold reserves.

Value of US Gold Reserves (USD) vs. US Monetary Base



Currencies... Currencies Everywhere.

Today, there exists over 180 currencies across 195 countries. The reason for such an anomaly is simple: there is no free market for currencies. Currency markets have been restricted by governments in order to maintain financial control. There are numerous laws and institutions set up for the exact purpose of inhibiting a free market monetary system. This includes enforced borders, legal tender laws, capital controls, state decrees, seigniorage privileges, local control, local monopolies on violence, debt extinguishing laws, capital gains taxes, implicit bailout guarantees for banks, central banks and dozens of other artificial barriers. This type of legislation forces people around the world to keep using inferior currencies under the threat of direct or indirect violence or repercussions. The centralized nature of the financial system and flows allows governments and institutions to impose these restrictions and greatly limit people's ability to express their true demand for superior, more competitive currencies. Fiat money's soundness is now dependent on an authority's ability to enforce legitimate monetary policy. People living in countries like Venezuela are unable to reliably store their wealth due to hyperinflation induced by irresponsible monetary policy and limited availability of more reliable currencies due to strict capital controls. In addition, as the only form of legal tender, citizens are obliged to pay taxes in and accept the inferior currency in exchange for goods and services. The more competitive currencies, like the dollar, that do make their way into countries like Venezuela, are sold at large premiums as the high demand is not met.

by the controlled supply. Until recently, citizens of countries like Venezuela had no way to opt out of this system and were forced to adopt easy money.

The government's control of money has made it vulnerable to gross mismanagement. In an [interview](#) in 1984, Friedrich Hayek famously said: *"I don't believe we shall ever have a good money again before we take the thing out of the hands of government. We can't take it violently out of the hands of government, all we can do is by some sly roundabout way introduce something that they can't stop."* And, in [Free Market Monetary System](#), Friedrich Hayek notes that *"the monopoly of government of issuing money has not only deprived us of good money but has also deprived us of the only process by which we can find out what would be good money. We do not even quite know what exact qualities we want ... because we have never been allowed to experiment with it. We have never been given a chance to find out what the best kind of money would be."*

Enter Bitcoin: The Experiment That Allows Us To Experiment

In 2008, Satoshi Nakamoto proposed Bitcoin, an alternative financial system free from top-down control. Bitcoin, ["a system for electronic transactions without relying on trust"](#), was not created to fit existing governments and financial systems.

Bitcoin is the experiment that allows us to experiment. Unlike any money of the past, Bitcoin is borderless, permissionless, censorship-resistant, and easily verifiable. As such, Bitcoin may precisely be this "sly roundabout way" that bypasses prohibitive mechanisms and legacy financial institutions that restrict people's access to a free market for money. Bitcoin is often referred to as digital gold because it maintains and improves upon most of gold's properties, including scarcity and unforgeable costliness. Given its digital nature, bitcoins are easily divisible, portable and unseizable, which enables it to be much better protected from the threats of centralization and the fate experienced by gold. First introduced by [Vijay Boyapati](#) and then further expanded upon by [Dan Held](#), below is a table assessing Bitcoin, gold and fiat's ability to fulfill the traits of money.

Traits of Money	Bitcoin	Gold	Fiat
Verifiable	High	Moderate	Moderate
Fungible	High	High	High
Portable	High	Low	High
Durable	Moderate	High	Low
Divisible	High	Low	Moderate
Scarce	High	Moderate	Low
Established History	Low	High	Low
Censorship resistant	High	Moderate	Low
Unforgeable Costliness	High	High	Low
*Openly Programmable	High	Low	Low
*Decentralized	High	Moderate	Low

<https://medium.com/@danhedl/planting-bitcoin-56bd1459cb23>

The Rise of Cryptocurrencies

[Cryptocurrencies are first and foremost money](#). With the exception of a few, ‘crypto-tokens’ are either clearly intended to be money or are intended to be money but are obfuscated by technological jargon. As Bitcoin’s community grew and its prices rose, other cryptocurrencies (often referred to as altcoins) began to hit the market. Many of these cryptocurrencies were built in an attempt to iterate and improve upon Bitcoin’s “fundamental design flaws” and “limited functionality”. In 2018, ten years after Bitcoin’s inception, there are now over [2,000 cryptocurrencies](#).

Contrary to the 20th century’s locally nationalized market for money, the cryptocurrency market much better resembles a competitive private market where no coercive monopolies distort price signals by preventing competitors from entering. Given the open source nature of cryptocurrencies, anyone is free to create their own or modify existing ones, which is as simple as copying the publicly available code of an existing cryptocurrency. This in turn encourages open and inexpensive experimentation.

The open source nature of cryptocurrencies is a promising mechanism to determine what the natural money of society might be. As Jörg Guido Hülsmann highlights in

the [Ethics of Money Production](#), “the only way to find out the natural money of society is to let people freely associate and choose the best means of exchange out of the available alternatives.”

Assuming operation under a free market, the question then becomes to what extent the natural money captures market share. While today’s world has manifested itself differently, a glimpse of a winner take most, if not all, reality was seen with gold. Assuming a long-term time horizon, this same glimpse of reality may play out with cryptocurrencies, this time as more than just a temporary phenomenon.

In Part II, we explore in depth the validity of a winner-takes-all narrative. By defining market size to be the total monetary premium of all cryptocurrencies and deriving what drives a good’s monetary premium, we shed light on the merits of such a narrative.

[1] [Rai stones](#) in Yap and [glass beads](#) in West Africa

[2] Using gold was impractical for daily purchases as it required measuring and dividing it into small quantities.

[3] In 1933, Roosevelt’s Executive Order 6102 forbade the hoarding of gold coin and bullion

Links

- <https://www.goldbroker.com/news/gold-and-silver-correlation-988>
- https://en.wikipedia.org/wiki/Methods_of_coin_debasement
- <https://www.youtube.com/watch?v=EYhEDxFwFRU&t=1230s>
- <https://mises.org/library/free-market-monetary-system>
- <https://bitcoin.org/bitcoin.pdf>
- https://twitter.com/real_vijay?lang=en
- <https://twitter.com/danhedl?lang=en>
- <https://medium.com/@danhedl/planting-bitcoin-56bd1459cb23>
- <https://tokeneconomy.co/cryptocurrencies-are-money-not-equity-30ff8d0491bb>
- <http://coinmarketcap.com/>
- <https://www.google.com/search?q=ethics+of+money+production&oq=ethics+of+money+production&aqs=chrome..69i57j69i65j0.2838j0j7&sourceid=chrome&ie=UTF-8>
- https://en.wikipedia.org/wiki/Rai_stones
- https://en.wikipedia.org/wiki/Trade_beads
- <https://twitter.com/wintonARK?lang=en>
- <https://twitter.com/MustStopMurad?lang=en>

- <https://twitter.com/MartyBent?lang=en>
- <https://twitter.com/saifedean?lang=en>
- <https://docs.google.com/document/d/12pLh5L20ixn7GQR5JtiiTIVYtladf6mE3Wrsd9tgIrc/edit?usp=sharing>

Maker Dai: Stable, but not scalable

A lesson in stablecoin arbitrage

By [Su Zhu](#) and [Hasu](#)

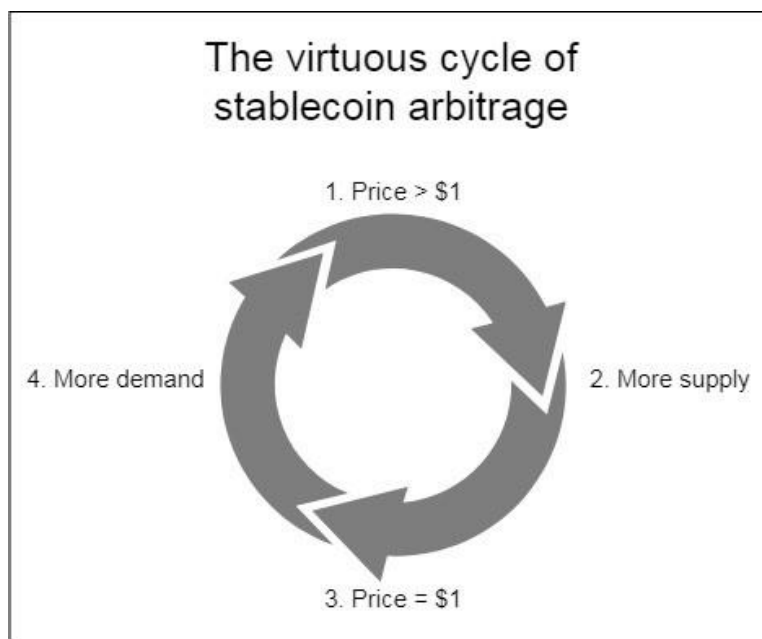
Posted January 7, 2019

The least understood thing about stablecoins is how they come into existence. Who creates the supply of Tether, USDC or Dai that you can buy on your favorite exchange? We will take a look at how professional arbitrageurs expand and contract the supply of a stablecoin based on the current demand of the market, how Dai's model is different and why the lack of a professional arbitrage model makes Dai fundamentally unscalable.

There's a common misconception that Dai can scale to any size, as demand for the stablecoin drives the price over \$1, which leads arbitrageurs to lock up ETH (or other assets) in CDPs and create more Dai. This chain of logic is usually used to support the narrative that higher demand for Dai leads to higher demand for Ether, but both statements are wrong.

How stablecoins scale

Let us define a stablecoin as scalable if its supply can closely track the demand to hold it. To do that, a stablecoin relies on the existence of professional arbitrageurs that react to market signals and keep supply and demand in a constant balance.



Professional arbitrage requires a closed cycle. The faster and more efficient the cycle can be iterated through, the more closely will supply track demand in either direction. For an example, let us look at a collateralized fiatcoin, Tether (USDT).

When market demand pushes the price of USDT against USD to \$1.02, the market signals to the arbitrageur to start working. He sends \$1.00 USD to Tether Inc. and receives 1 USDT in return. Since the market currently values USDT at \$1.02, it buys him \$1.02 worth of USD, for an immediate profit of \$0.02. The same is true in the other direction when the price of USDT falls to \$0.98. Arbitrageurs will buy up USDT for \$0.98 USD, send it to Tether Inc. and redeem it for \$1.00 in USD, again closing the cycle with a profit.

Professional arbitrage is impossible for Dai

There is no way to execute a closed cycle for Dai, so it's much harder to arbitrage. We will demonstrate that by going through a hypothetical arbitrage cycle for Dai.

When market demand pushes the price of Dai to \$1.02, you can again take \$1.00 USD, buy \$1.00 ETH (or any other asset that can be used as collateral) and lock it in a CDP. The problem, however, is that for each \$1.00 ETH locked up, Maker will give you less than \$1 of Dai. That is due to the requirement for over-collateralization. The current collateralization ratio is 150%, so \$1.00 ETH in a CDP can generate up to 0.66 Dai (this ratio could change, but it's never going to be close to 100%).

Now you can certainly sell the 0.66 Dai at the same 2% premium, but you still have the original ETH locked up. The fundamental difference between "arbing" Tether and "arbing" Dai is that with Dai you also need to look for a profitable way to exit the collateralized debt position at a later date. And it's only going to be profitable if you manage to buy back the Dai for less than you sold it for.

While you wait for the price of Dai to drop, you are stuck in an unfortunate position:

1. You don't know when, or if, the price of Dai will fall again
2. Since you cannot complete all the steps of the cycle simultaneously, you are stuck with long exposure to ETH while you wait. You want to sterilize the risk by shorting ETH, but that incurs an additional borrow cost.
3. You have an additional cost of capital for locking up the part of sterilized ETH you didn't borrow Dai against, which is at least 33% (since you can draw \$0.66 Dai for every \$1 ETH). The cost of that is the risk-free rate of USD.
4. There is an additional cost for closing the CDP.

USDT and other collateralized fiatcoins allow for closed arbitrage cycles because the collateralization ratio is 100% and not higher. Arbitrageurs can create \$1 of USDT with \$1 of USD, then sell the USDT and be done with it—they no longer have to worry

about the USD “locked up” in Tether Inc.’s bank account. Those USD are someone else’s problem now. The existence of committed arbitrageurs allows USDT supply to closely track demand.

We established that Dai arbitrage is very costly, but is there a point where it becomes profitable? The collateralization ratio of ETH and Dai is fixed at 1.5:1, so 1 ETH currently creates 0.66 Dai. If the price of Dai were \$1.50 or higher, \$1 ETH would create \$1 Dai. At this point, you can sell the Dai and forget about it your CDP—just as you would with USDT—except that you even have a free option at buying back your ETH later. So deterministically, pure arbitrage is profitable at \$1.50. Probabilistically, it’s going to be profitable below \$1.50, but there is no guarantee to close the cycle within a predictable window of time.

Of course, this is purely hypothetical -people are not going to bid Dai up to \$1.50, or even \$1.10. It’s much cheaper to simply use another stablecoin, or if none existed-say for reasons of regulation—sterilize a volatile asset like ether or bitcoin by shorting it. So the price of Dai, even in a high demand scenario has a relatively low ceiling that will ensure that the professional arb window never opens.

No arbitrage = no scaling

Now one can argue that the same premium will lead to more natural demand for CDPs, resulting in *some* arbitrage, and that is certainly correct. Natural CDP creators will be incentivized to arb the price at the margin, especially those who already have CDPs open and can generate some more Dai at minimal effort. But at every price level, there is still a natural ceiling to the demand for CDPs which doesn’t exist when closed arb cycles are possible.

Why is the natural arbitrage by CDP creators not enough to make Dai scale? Remember, the faster a stablecoin can iterate through this cycle, the more closely will its supply track its demand. **The important part for stability is getting the price of your coin up to \$1. But the important part for scalability is getting the price back down to \$1.** Whenever the price is over \$1, the demand for buying Dai is very low, since a potential buyer has to expect the price to normalize eventually. So the faster arbitrageurs can push the price back down to \$1, the sooner the demand can rise again, leading to further increases in demand (up to a natural ceiling).

A professional arbitrageur is seeking to extract riskfree profits on a limited balance sheet, denominated in USD. Dai does not offer him any opportunities. The difference becomes clear when a buy order for 25M coins at a small premium comes to the market. For Dai, none of these people would open CDPs to create more Dai. In contrast, the same buy order on other stablecoins like USDT would generate an immediate supply increase, and arbers would sell the new supply to the buy order.

Because Dai doesn't allow for professional arbitrage, this cycle will play out very slowly, if at all. While for USDC or USDT new supply generation is triggered whenever a buyer pays more than \$1, the generation of more Dai relies on vague demand for more debt on the CDP side. What does this mean for Maker?

But... Maker is not primarily about the stablecoin

Dai's disability to scale has no impact on Maker because that was never the goal, to begin with. Maker is a decentralized and very efficient version of centralized lending services like BlockFi, the primary use case of which is tax arbitrage:

A loan from BlockFi enables you to use your cryptoassets as collateral and receive USD to your bank account. Borrowing against your cryptoassets enables you to receive liquidity now but does not trigger a capital gains tax event and, depending on the use of funds, the interest may be deductible against capital gains and other investment income. (Source: <https://blockfi.com/faq>)

The two other prominent use cases are long leverage and treasury/payroll management for ICOs. The basic idea is always to generate liquidity *ahead of a future liquidity event*—spending money that you expect to receive later. Either from selling ETH after a tax deadline or from selling it at a higher price at a later time.

We believe Maker is a great service with a distinguished set of features. On the plus side, it offers lower friction, lower fees and less counterparty risk than centralized competitors and on the downside, lower maximum leverage, a lack of standard margin calls, and a steeper auto-liquidation penalty. It is the demand for Maker's core product—lending—that will determine the supply of Dai in existence, not the other way around.

If the price of Dai goes over \$1, that will generally incentivize people to take slightly more debt, especially those who already have CDPs open. But it will not incentivize anyone to make a CDP to arbitrage the difference, not unless he was already indifferent towards taking a debt. Since all money locked in CDPs have to come from a natural demand for debt, there is also a natural ceiling to the amount of debt that people are going to take, and hence for the amount of Dai that will exist.

In our opinion, there are three takeaways. First, because professional arbitrage is unprofitable for Dai, supply will not track demand as it does for other stablecoins. It follows that more demand for Dai will not lead to a meaningful increase in demand for ether as collateral, either. If anything, demand for ether as collateral might go down as Maker starts adding more assets and allows users to borrow against them instead of only against ether.

Second, Maker is often mentioned as a figurehead of Ethereum, usually as a driver for price bullishness. But we believe that Maker's merit is less in "locking supply" and increasing demand for ether, which we showed is incorrect, and more about actual usefulness. Maker is proving that the Ethereum smart contract functionality can be used to create a highly efficient, decentralized version of BlockFi.

Last, it is now clear that too much attention was focussed initially on analyzing if Maker is a house of cards and Dai would hold the peg. The reality is it has survived a 90%+ decline in collateral value. This comes from a misunderstanding of the basic value proposition of Maker and Dai. It is not to create a scalable, censorship-resistant stablecoin. It is to be able to generate censorship resistant stability for anyone holding a volatile censorship resistant asset.

Our special thanks to [Nic Carter](#) and [rae](#) for their feedback and [Richard Brown](#) of Maker for validating our technical references to their system.

Links

<https://blockfi.com/faq>

Unpacking Bitcoin's Assurances

Dis-aggregating the system's guarantees

By [Nic Carter](#)

Posted Jan 13

It has rightfully been pointed out that Bitcoin's decentralization is but a means to an end—censorship resistance. This is in response to the decentralization fetishism that has characterized Bitcoin competitors and the blockchain industry in general. This is an appropriate response: cosmetic network decentralization is probably not sufficient if you plan on breaking any serious rules, and irrelevant if the industry you are seeking to disrupt is dentistry.

Bitcoin's fault-tolerant architecture was designed to survive extreme duress, and its multi-variate decentralization was created (or more accurately: emerged) to promote this. However, censorship resistance—the ability to broadcast information without restriction—does not fully cover the guarantees that Bitcoin provides to users, although it is perhaps the most significant.

In this post I will try and define the various guarantees that Bitcoin users can expect by taking advantage of the system's features over the entire usage lifecycle—from acquisition to exit. Censorship resistance is central to these but not sufficiently comprehensive. I call these 'assurances,' although they aren't perfectly assured, since things go wrong in the real world. (I've been a fan of 'assurances' in this context since reading [this post](#).) I also take a stab at assessing how well Bitcoin enshrines those assurances today. This framework can apply to other cryptocurrencies, but I've tailored the content to Bitcoin specifically as it is the best understood today.

Touted assurance	<i>Open access*</i>	<i>Seizure resistance</i>	<i>Censorship resistance</i>	<i>Counterfeit resistance</i>	<i>Free exit*</i>
Bitcoin user phase	Acquisition	Static state	Broadcast	Receipt	Divestment
Enabling technologies	p2p exchanges, voucher systems, Bitcoin ATMs, conventional exchanges, mobile wallets, bearer wallets, multisig	Elliptic curve cryptography, hardware wallets, multisig, paper wallets, brainwallets	P2p gossip broadcast protocol, Sybil-resistant networking, cheap verification and full node proliferation, redundant broadcast (satellite, SMS, radio, mesh)	Cryptographic auditability guarantees, Proof of Work minting, low bandwidth & storage fully validating nodes, hardware full nodes, node service providers, bandwidth reduction techniques	Tumblers, CoinJoin, other privacy enhancements, p2p exchanges, trust-minimized direct sales intermediation
Threats to those assurances	Exchange concentration, capital controls, extension of US banking rules to cryptocurrency exchanges globally	Hardware wallet supply chain attacks, imprisonment / extortion, bank vault raids, quantum computing (long term)	Costly full nodes (leading to a reduction in node count), network DOS attacks, very high fees (for small transactions), loss of internet connectivity	Concentration in node providers, costly full nodes, complexity in validating transactions, deviations from the PoW minting schedule	Taint analysis, shared user blacklists, chain analysis, collusion among exchanges, regulatory action against unregulated exchanges
Strength of assurance	Weak. Exchanges are tightly regulated and fragile to government action. P2p exchanges not yet widespread	Extraordinarily strong. Bitcoin's property rights are some of the strongest ever conceived, and robust to many forms of attack	Currently strong but at risk. Internet closure is a realistic way to prevent broadcast in authoritarian states	Currently strong but at risk. Large/costly full nodes make trust-minimized validation more difficult	Weak. Chain analysis and risk-averse exchanges degrade the saleability of grey or suspected black market coins

** proposed name*

Bitcoin's assurances by usage phase

Open access

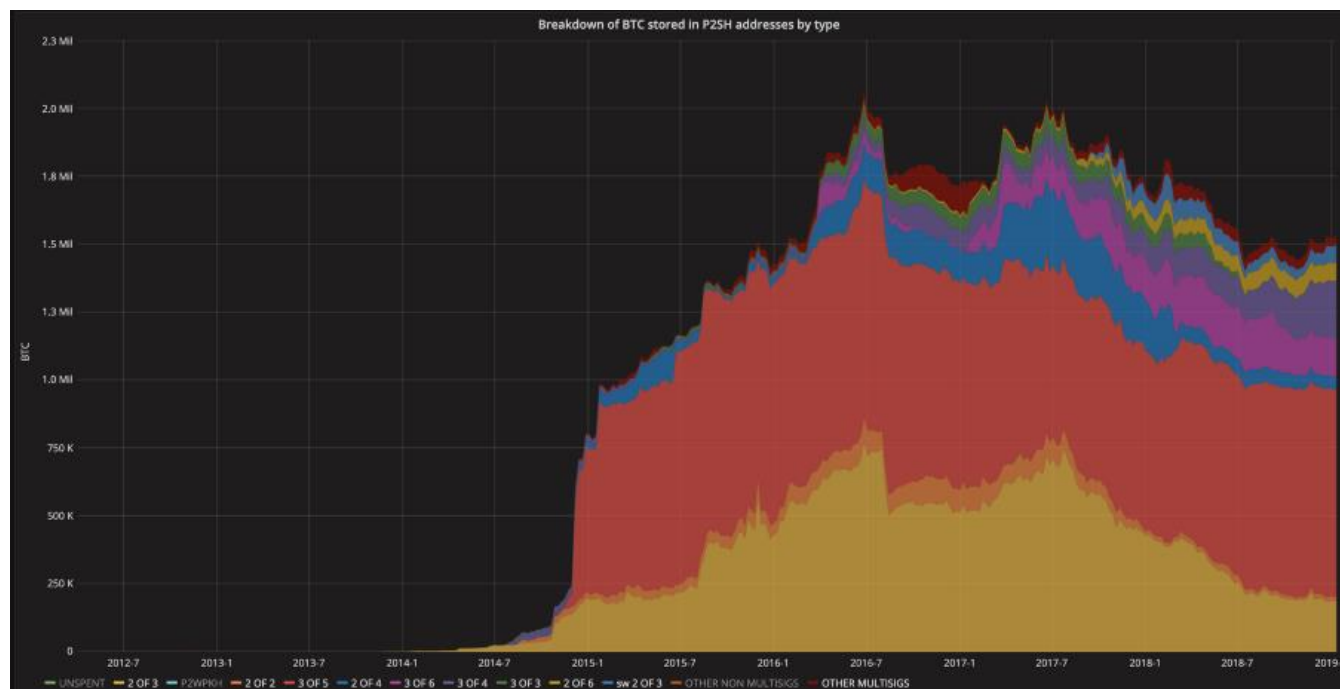
This is the shorthand for “the right to freely acquire Bitcoin.” No amount of decentralization in Bitcoin’s architecture itself can guarantee this. As many Bitcoiners will point out, free access to the asset requires a vibrant and competitive industry of fiat onramps. The existence of quasi monopolists attempting to build regulatory moats in order to raise barriers to entry threatens this. If acquisition of the asset can only occur in a couple large venues, they are not only susceptible to state action, but also liable to collusively deplatform individuals at will. Imagine what happens to the Venezuelan equivalent of Coinbase during a currency crisis: the government trivially shuts it down to preserve its monetary monopoly.

Thus, while large, regulator-friendly, conventional exchanges are good onramps in the developed world, where cryptocurrencies are not (yet) a threat to local sovereign currencies, they aren’t a good fit for states experiencing demonetization or high inflation, which is where access is most impactful. Centralized exchanges must be supplemented by peer to peer exchanges like [LocalBitcoins](#), [Hodl Hodl](#), [Paxful](#)—and indeed, they are the venues where trading seems to occur (Venezuelan traders are doing \$300m annualized on LocalBitcoins, Nigeria ~\$170m, Russia close to a billion USD). Wallets which allow for trust-minimized trading like [Opendimes](#) are vital here—receiving an Opendime where you can be sure your counterparty doesn’t know the private key beats waiting an hour for six confirmations.

Lastly, paper voucher systems enabling users to acquire smaller quantities of Bitcoin at street kiosks or from corner shops are an important piece of the puzzle. Vouchers work by exchanging fiat for a receipt with a code on it; settlement can be done later. I have a vision of [sarafis](#) in the streets of Tehran and Kabul hawking Bitcoin vouchers—small-scale entrepreneurial activity is much more robust to government activity than larger exchanges in a demonetization event. [Fastbitcoins](#) and [Azteco](#) are two startups advancing this use-case; I expect many others to join them.

Peer to peer exchanges like [Hodl Hodl](#) rely on a crucial and unheralded technology: Bitcoin's native multi-signature (multisig) capability. A simple, well-understood, trusted, and widely-used multisig implementation enables massive secondary benefits. In the case of Hodl Hodl, it allows buyers and sellers to transact with a high degree of confidence that they will not be cheated. In 2-of-3 multisig contract, the seller and buyer must both sign the release transaction; and if one disagrees, it is referred to the arbitrator for a decision. In practice, the vast majority of transactions settle without arbitration—the threat of mediation itself enforces good behavior.

Multisig is popular in Bitcoin today: about 1.65m BTC (about \$6b) are held in known multisig wallets. This figure climbs to 3.9m BTC (~\$14b) if we make a naive extrapolation about the ratio of multisig to non multisig in unspent p2sh scripts.



Source: p2sh.info

To sum up, open access to Bitcoin is a core component of the system—what use is the asset if you can't easily obtain it?—yet it is somewhat overlooked. It's important to be realistic about this. Bitcoin suffers from a paradox whereby individuals in

countries with relatively less need for Bitcoin have frictionless access to it, while individuals dealing with hyperinflation have to reckon with a less developed onramp infrastructure. There is much work to be done here.

Seizure resistance

One of the chief motivations for this article was to differentiate the unencumbered broadcast rights that Bitcoin grants users from the strong guarantees it grants to users when it is at rest. As mentioned above, censorship occurs at the time of broadcast, so 'censorship resistance' doesn't quite describe Bitcoin's unique properties when idle.

Thus the inclusion of **seizure resistance** (this is also sometimes referred to as 'tamper resistance' or 'judgment resistance'). By this I mean the ability of users to retain access to their Bitcoin under duress, during times of upheaval or displacement, all in a peaceful and covert way.

As Hasu and Su Zhu have [eloquently written](#), Bitcoin can be understood as an independent institution which provides users property rights which are untethered from the state or the legal system. As virtually all property rights trace back to the state, the legal system, or some local monopoly on violence, Bitcoin's cryptography-based property rights are a genuinely new paradigm.

This has been covered at length, but the fact that individuals can store their wealth in a 12 or 16-word passphrase held in their memory is quite astounding. While that's not the most failure-resistant way to operate, it makes one's wealth extremely portable and concealable.

Multisig also comes into play here. Innovative custody companies like [Casa](#) (disclaimer: Castle Island is an investor) rely on a 3-of-5 multisignature setup whereby the user controls four keys physically dispersed, and Casa holds one for disaster recovery. This makes physical attacks on Bitcoin holders much more difficult and expensive, while preserving convenience and resilience to faults (seedless recovery is possible if a hardware wallet is lost). The secure key sharding that Bitcoin offers fundamentally reinvents what it means to be a custodian, and opens the door for all kinds of innovative hybrid models which offer various resilience/autonomy tradeoffs.

Censorship resistance

This is the most celebrated assurance attributed to Bitcoin, so I'll be brief. At its core, Bitcoin allows permissionless broadcast through the p2p gossip protocol and the miner fee incentive. Anyone can make a transaction, although they have to sufficiently compensate a miner to include it in a block. If there is a lot of traffic, this could entail a delay or a higher fee. The other required component here is a well-

connected network of nodes available to route transactions. If full nodes were to become very expensive and difficult to run, full node counts might decline, making broadcast more difficult. That said, node counts would have to drop precipitously to impair network performance, so this isn't an immediate concern.

One realistic impairment to censorship resistance is the simple approach of simply shutting off local access to the internet. While Bitcoin's global infrastructure cannot be realistically held back by even by the most motivated state actor, a state under severe monetary duress—experiencing a demonetization event, for instance—might take the extreme step of temporarily restricting access to Bitcoin by shutting off the internet. In recent memory, governments in [Iran](#), [Turkey](#), and [Russia](#) have shown themselves willing to exert massive collateral damage on local internet access to target services like Telegram and Wikipedia. Places like China where the internet and Bitcoin usage are already [tightly regulated](#) would be well-positioned to impose such restrictions. It's not inconceivable that a state could attempt to target Bitcoin in such a manner.

Touted mitigations to state censorship of Bitcoin's broadcast layer include Nick Szabo's [long-range radio proposal](#) as well as [Samourai/Gotenna's](#) SMS and short-range radio mesh proofs of concept. These initiatives, however, are still either in the R&D phase or the very earliest phases of deployment. At present, individuals in internet-restricted locations have little recourse when faced with such an attack, aside from physically getting their funds out of the country in a hardware or paper wallet. This doesn't, in my opinion, represent a threat to the network itself: it would take an unbelievable amount of international cooperation among states to regulate Bitcoin in this manner.

Network DOS attacks through fee spam are also an effective if costly way to make it more difficult for everyday users to broadcast transactions. There are few mitigations for this aside from waiting out the attacker or outbidding them.

Counterfeit resistance

This is a crucial quality of the system, and yet it doesn't get quite the rhetorical exposure that censorship resistance does. **Counterfeit resistance** is simply the idea that individuals who use Bitcoin have very cheap access to the tools required to verify that payments they are receiving are legitimate, that their savings have not been debased through inflation, and that their counterparties aren't cheating them in some way.

Comparing Bitcoin to gold, the ability to run a full node is akin to owning a professional-grade XRF spectrometer to check the integrity of your bullion. Compared to the expensive and tricky tests to verify gold's authenticity, verifying the integrity of one's Bitcoin is a breeze. Running a node costs a few dollars a year and

can be done on consumer hardware and bandwidth with little difficulty. This very accessible counterfeit resistance only persists as long as running a node is relatively cheap—a significant increase in the bandwidth, computation, or memory required to run a fully validating node would hinder it significantly. Right now, Bitcoin is growing at a stable rate, and physical plug-n-play node hardware has made full nodes more accessible than ever, so this assurance seems safe for now. For individuals and enterprises that don't want to run nodes directly, a good diversity of managed node software exists.

The other side of counterfeit resistance is the ability to determine that all units that exist were created according to a predefined, predictable schedule. The proof of work minting function, plus the difficulty adjustment, takes care of this. Well—close enough. Naively assuming that blocks were meant to arrive every 10 minutes on average, Bitcoin is actually slightly ahead of schedule by 30,000 blocks or so. This is because hash power has generally increased over time, and this caused block arrival to outpace the defined schedule due the coarse granularity in the difficulty adjustment. Aside from this interesting emergent property, Bitcoin's PoW has never been compromised, nor has the hash function been broken (and this doesn't seem eminently likely in the foreseeable future). Verifying that the correct number of units exist is as simple as running the `gettxoutsetinfo` command in your Bitcoin Core node. The inherent auditability of Bitcoin and all of its derivatives is what makes deceptions like the [Bitcoin Private](#) covert inflation scandal easy to spot.

At present, Bitcoin's counterfeit resistance is made possible by a deliberate design philosophy from the core developers that prides accessibility and user self-sovereignty at all costs. It is augmented by a network of Bitcoin businesses that provide hardware nodes or managed access to node software. However, if the chain's growth were to radically accelerate, consumer-grade counterfeit resistance would be significantly impaired.

Free exit

Free exit—the ability to sell Bitcoin unencumbered—is another aspect of the system that is sometimes overlooked. It's not strictly a Bitcoin guarantee, but Bitcoin's usefulness is significantly downgraded in its absence. The real world consequences of overzealous chain analysis companies (whose heuristics implicate innocent users through false positives) make themselves felt when those users attempt to sell their Bitcoin for fiat. Since fiat offramps are the most easily regulated and are run by risk-averse institutions, they are a natural target for entities that create blacklists and ascribe taint to individual UTXOs.

There are a few strategies to reckon with this. One is to obfuscate the origin of funds through collaborative tumblers like the [Wasabi wallet](#). Another approach is to reverse-engineer the heuristics that chain analysis firms use and develop mixing

strategies that implicate everyone in taint (thus rendering those heuristics incoherent) or that avoid detection altogether through specialized transaction types. This is the general approach of the folks behind the [Samourai](#) wallet. Routing around the centralized, highly-regulated exchanges is another option, either on the p2p marketplaces or by exchanging BTC for goods and services, rather than fiat.

Ultimately, I expect that a tranche of grey or black-market Bitcoins will emerge, with coins available at a discount in exchange for their reduced access to capital markets. This will not be a death knell—there will likely be more than enough demand globally for slightly cheaper Bitcoins, even if they cannot be traded on Coinbase. The world is a big place, with a variety of regulatory regimes, and individuals fleeing hyperinflation may not be too bothered by the fact that the Bitcoins they acquired cannot be deposited on US-regulated exchanges.

The objective for this piece was to present a framework of the major assurances that Bitcoin provides to users, and make it clear that censorship resistance is only one of them. Additionally, I wanted to make the point that Bitcoin the software is only one part of a much vaster system—a collaborative social and industrial project aiming to provide unencumbered financial tools to individuals the world over. Entrepreneurs that have created hardware wallets, merchant services, novel exchanges, voucher systems, Bitcoin contract structuring, and hybrid custody models have all done their bit to advance user sovereignty and discretion when it comes to their personal wealth. They deserve to be recognized, as does the broader struggle to make these touted assurances a reality.

Links

- https://medium.com/@nic_carter?source=post_header_lockup
- https://medium.com/@nic_carter
- <https://blog.goodaudience.com/1-assurances-in-crypto-14c55a1fd616>
- <https://localbitcoins.com/>
- <https://hodlhodl.com/>
- <https://paxful.com/>
- <https://opendime.com/>
- <https://hackernoon.com/the-key-to-bitcoin-adoption-in-developing-countries-60edfbe60786>
- <https://fastbitcoins.com/>
- <https://azte.co/>
- https://en.bitcoinwiki.org/wiki/Hodl_Hodl#How_does_Hodl_Hodl_work.3F
- <https://p2sh.info/dashboard/db/p2sh-repartition-by-type?orgId=1>
- <https://medium.com/@hasufly/bitcoin-and-the-promise-of-independent-property-rights-8f10e5c7efa8?sk=226124e0ff272801b8a9e49ce3403ac7>
- <https://keys.casa/>

- <https://www.wired.com/story/iran-telegram-ban/>
- https://en.wikipedia.org/wiki/Block_of_Wikipedia_in_Turkey
- <https://www.theverge.com/2018/4/17/17246150/telegram-russia-ban>
- <https://bitcoinist.com/bitcoin-node-illegal-china/>
- <https://scalingbitcoin.org/stanford2017/Day2/Weak-Signal-Radio-Communications-for-Bitcoin-Network-Resilience.pdf>
- <https://github.com/MuleTools/PonyDirect>
- <https://bitcoinmagazine.com/articles/samourai-and-gotenna-enable-bitcoin-transactions-without-internet-access/>
- <https://coinmetrics.io/bitcoin-private/>
- <https://www.wasabiwallet.io/>
- <https://samouraiwallet.com/features>

96 Theses for Crypto in 2019

By [Ryan Selkis](#)

Posted January 14, 2019

Often imitated. Never replicated. I call your predictions post, and raise you.

There have been a few good predictions pieces so far this year. This one is [my encore from last year](#), with a little help from my colleagues at Messari, who are building the industry's best market intelligence platform.

Without further adieu...

Top General Trends

1. Our top 2019 bets:
 - Lightning Network growth will blow up (50x YoY in USD growth = \$100mm channel capacity) and have its “irrational exuberance” moment.
 - Ethereum will face legitimate smart contract platform competition (EOS, Dfinity), AND “parachains” (Cosmos, Polkadot) will chip away at ETH's dominance.
 - ICO's are dead (for now). It's all about security tokens...at least that's the narrative. New synthetic securities will be really exciting, the tokenized real estate assets we see in 2019 betas...marginally exciting, but not more than that.
 - Privacy upgrades will cause headaches and pushback from regulated exchanges and wallets. Some of the new tech is so good it might hurt compliance efforts.
2. On Lightning Network, it's our theme of the year. We could see network growth get crazy and hit \$100mm (50X 2018). It will continue to get easier to spin up nodes with out of the box solutions (e.g. [Casa](#)), and there will be numerous technical improvements (e.g. dual-funded channels), and perhaps major exchange buy-in. Arjun Balaji covered a bunch of these in [his post](#), which I'll reference throughout this piece. (Want more plain English details on the state of Lightning? [Andreas](#) also walks through some [Lightning Network misconceptions](#) in this 20 minute video.)
3. Although we won't see a serious proposal this year to re-appropriate Satoshi's bitcoin or add perpetual low inflation to bitcoin in lieu of transaction fees, it does make sense to begin to explore. I wrote about this [back in 2015](#).
Eventually this issue will come to a head: when bitcoin inflation dips below 1-2% (a few years), miner's incentives will skew to “attack” vs. “secure” the blockchain.
4. Serenity NOW! Ultimately, the transition from PoW to PoS is shaping up to be as messy and unpredictable as we should have expected. I'm excited about

Ethereum 1.x (state pruning, Ewasm, transaction parallelization) because 2.0 won't ship before 2020 (earliest). I liked (Ethereum core developer) [Lane Rettig's](#) breakdown, and CoinDesk also has a [good backgrounder](#).

5. Top 20 coin hot takes:
BTC: Digital Gold | ETH: ICO Reserve | XRP: Too-Big-to-Jail-Coin | BCH (ABC): Bitmain Casino Chip | EOS: Wait, It's Legit? | XLM: Cool, Enigmatic | LTC: Now Useless | USDT: Surprise! They're Solvent. | TRON: omg, these guys own BitTorrent | BSV: Faketoshi Coin | ADA: DO YOU KNOW WHAT IT IS? | IOTA: Ass hole founders | XMR: Fluffy Pony Reserve | BNB: exciting unregistered security | DASH: airplane promos | NEO: "Chinese ETH" | XEM: wtf is NEM? | ETC: [redacted]'s shitcoin | MKR: #DeFi Reserve | ZEC: Winning Privacy Coin
6. Top 10 people to keep an eye on in 2019:
CZ (Binance), Vitalik (Ethereum), Elizabeth Stark (Lightning Labs), Jae Kwon/Jutta Steiner (Cosmos/Polkadot), Zooko (ZCash), Rune Christensen (MakerDAO), Bram Cohen (Chia), Robert Leshner (Compound)/Nadav Hollander (Dharma), Will Warren (Ox), Joe Lubin (ConsenSys), Arthur Hayes (BitMEX).
7. I know. Many of those are obvious, but they continue to be the ones to pay closest attention to. If I had to pick 5 more under-followed folks (sub-15k), I'd go with: Hasu (researcher), Mason Borda (TokenSoft), Yaniv Tal (TheGraph), Demi Brener / Manuel Araoz (Zeppelin) (both had great [year-end pieces](#), too), and Spencer Noon (investor).
8. Biggest rebounds? I'll be fascinated to see what happens with both Bitmain and ConsenSys, two of the world's largest crypto companies that got burned by concentrated crypto positions. I think Bitmain's IPO is in trouble, but rumors of ConsenSys's death have been greatly exaggerated.
9. Taxes will get more nightmarish. You thought thinking through ERC-20 like kind transactions and scraping Poloniex trade histories was bad? Try trading from a self-custodied wallet using a non-custodial exchange where your keys never move.
And what do you do about "interest" on staked tokens, or dapp usage where you leverage multiple tokens? It's near impossible to proactively report on these, so imagine the helluva time the IRS will have tracking all this down. Worse still, complexity means that audit victims are going to have a bad time explaining the esoterica to the men in suits.
10. Security tokens will fall flat. a) nobody actually cares about hard assets on the blockchain (beyond some initial hype and novelty), b) none of the assets / cashflows getting tokenized are interesting to crypto geeks. The "killer app" for STOs are DAOs, but don't expect those in 2019 because the infrastructure isn't there. Yet. (h/t [Ben](#)) AGREED

DeFi / Open Finance

1. "Open finance" (lending, derivatives) will become the primary use case for Ethereum. Most other dApps (gaming, distributed storage, attention markets)

will move to competing blockchains that are optimized for single uses. (h/t [Eric](#)) AGREED

2. The Gemini Dollar, Paxos, TrueUSD, or USDC will overtake Tether as the largest fiat-backed stablecoin. Three of the top ten assets by market cap will be fiat-denominated stablecoins by year-end. You can track the action [here](#). (h/t [Eric](#)) BOLD
3. A legitimate game development team will build an NFT app that gets more DAUs than any other dapp. Everyone is talking about Ethereum NFTs, but the Ethereum blockchain's performance is lagging its less decentralized competitors. Meanwhile, something viral will get built on EOS. (h/t [Ben](#))
4. It's getting less sexy, but I still believe in digital resource tokens for storage, computing, etc. Its importance isn't obvious to many (yet) and it's a five year vs. 2019 trend, but these tokens will be critical to fueling Web 3.0's growth. I've gotten more bullish on them recently as a) speech censorship globally is ramping up, b) the "Airbnb" model for of excess file storage / compute / cellular data seems intuitive, c) AWS margins are insane, and ripe for the "your margin is my opportunity" treatment...this time by disruptive distributed protocols. Filecoin is the one to keep the closest eye on. They'll launch by Q3. (Ok, maybe Q4).
5. I still believe in governance tokens with **serious** caveats. Most of these tokens were wildly overvalued last year, but many have crashed so viciously, they make more sense today. The litmus test? Is the governance token in question securing a valuable code base upon which a good deal of economic activity relies?
If so, you can value them sort of like insurance premiums. Ones you pay to guarantee the underlying code's reliability. I buy that narrative for Zeppelin (reusable smart contracts), Ox (reliable DEX logic), and Aragon (DAO governance). In those protocols, if the majority of "governors" abuse their power in any of these systems, the disenfranchised still retain the right to fork / exit.
6. Speaking of Ox, if you're them, you have to be thinking of how to share your token reserves with top relayers more efficiently. The previous top relayer by volume, DDEX, [forked away](#) in order to build on a \$3 million market cap protocol token (Hydro) in which it had a stake. I wonder if these defections could be avoided with more generous token treasury distributions. Slippery slope, maybe.
7. Ox is making baby steps in that direction by rolling out incentive plans for market makers ([announced yesterday, actually](#)). This seems like a critical initiative as the DEX ecosystem has no small task in bootstrapping liquidity to become competitive with larger, faster, better custodial exchanges. Which leads to...
8. If any DEX captures significant market share, it'll be one built by a company with a centralized exchange (e.g. Bitfinex, Binance). The giants already own the user relationship, have the liquidity and market making capabilities to make spreads competitive, and UI to abstract away the actual DEX. (h/t [Qiao](#))

9. After [regulatory action against EtherDelta](#) chilled DEX developers' willingness to push the envelope, and neutered perceived advantages of decentralized trading, we'll see a DEX launch with completely anonymous founders (a la Grin), with code similar to Bittorrent's. (h/t [Eric](#))
10. That anonymity might be a critical missing piece of the DeFi movement in general. Here's my five variable formula to create unstoppable commerce: *secure wallet hardware + DEX + stablecoins + zk-SNARKs + high-throughput smart contract platform = Web 3.0.*
If you can store value, exchange freely, self-custody, and program scalable contracts, you can conduct any type of transaction.
11. Over time, DEX will be an indispensable abstraction for machine to machine smart payments, and application interoperability. Today, however, the killer app for DEX may be tax evasion (see #9). DEX power traders will be tough to trace, and you'd be willing to pay a 2% spread if it meant 20% in capital gains evasion. (NOT A RECOMMENDATION. I use TokenTax.co)
12. DEX skeptics underestimate the hassle of global asset onboarding to centralized exchanges. DEX protocols can support new tokens instantly, so in a future with thousands (or millions) of tokens, "listings fees" will be obsolete, and liquidity pools will aggregate globally.
13. Are DeFi spreads silly? Of course! That's how this starts, not how it ends. We work our way from the most chronically underserved retail user to enterprise adopters, not the other way around. BitMEX is a \$10 billion company because it helped bootstrap a global margin trading market for ["degenerate gamblers."](#)
14. I'm extremely excited about [Ripio's collaboration with MakerDAO](#). Bringing dollar-pegged lending products to customers in an economy experiencing 40% annual inflation is massive. I'm sure the compliance teams are buttoned up, but even if these initiatives aren't explicitly blessed by regulators, they're worth pursuing aggressively. I view stablecoin fueled cross-border credit as a killer app for crypto.
15. Speaking of MakerDAO (track it [here](#)—graphic below), it's today's most systemically important crypto dapp. \$Dai should power all sorts of DeFi applications, while centralized stablecoins end up getting relegated to a primary use case of facilitating inter-exchange liquidity. Fully reserved regulated stablecoins are less "crypto," more just simply "finance."
16. Dai also survived one of its most significant tests in 2018. "Can Dai survive a market crash?" Asked and answered. Dai survived the 94% drawdown in ETH, and the move from a single-collateral to multi-collateral model should accelerate its adoption in 2019. (Now if we can [just scale it safely](#)...no one yet knows whether Dai works without significant over-collateralization. Big TBD.)
17. Dollar-backed stablecoins will catapult "open finance" into mainstream adoption. The idea of dollar backed stablecoins will be generalized to other asset classes, i.e. a token that tracks S&P 500. New crypto indices that mirror traditional asset performance (synthetic crypto securities) are a massive

untapped (and probably illegal) market that could pick up steam in 2019. (h/t [Qiao](#))

Other Killer Dapps

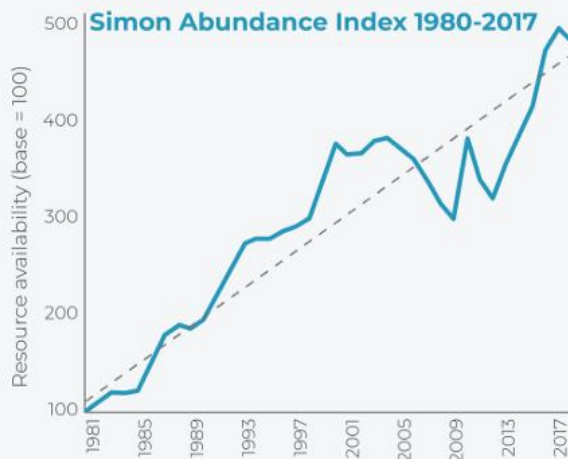
1. The top dapp markets at the end of this year will prove to be the ones already running experiments, although the market leaders may (will?) change. I'm more bullish than ever on prediction markets (Augur), lending products (Compound), and digital gaming assets (Decentraland).
2. Re current Dapp usage being slow / non-existent: a) it's expected (we're in the "toy" stage), b) we should compare Dapp stats to 2019's most hyped project, Lightning (e.g. \$2M \$REP staked = current \$2M LN capacity), c) Dapps with a stablecoin are far more usable than Dapps with ETH. Usage will come slowly, but surely. Until then, usage charts will look ugly.
3. Speaking of Augur's \$REP, prediction markets may eke out steady growth this year, but it won't be explosive because market making is still so risky (potentially illegal gambling or unregistered futures trading) for such a small payout. The CFTC's "[developer liability](#)" assertion was chilling, there is no major catalyst for volumes until the 2020 election, and the top prediction market may be highly centralized. Good teams will figure out how to better abstract away the tech. One of my top companies to watch in 2019 will be [Veil \(funding announcement\)](#).

Macro/Politics/Taxes

1. I like Fred Wilson's [President Pence by EoY prediction](#). Part of me hopes it's so. Especially after last night. But Trump is more likely to get reelected than he is to resign. How do most people still underestimate how little he gives AF? The Democrats will blink over "the wall" before the gov't reopens. (And I doubt they blink anytime soon. Did you watch the addresses last week???)
2. Why bring this up in a crypto post? Well, Trump wreaking havoc on the government (shutdowns, scandals, god help us if a national security crisis emerges), impacts the crypto markets insofar that crypto is still a highly correlated "risk" asset that will crater further in a macro recession. Generally, political dysfunction slowly advances the move from USD as reserve currency to something new, and that could greatly benefit bitcoin. So long as the dysfunction isn't severe.
3. The shutdown will impact bodies that still need to provide better clarity on crypto tax rules (IRS) and the bitcoin ETF (SEC—next deadline is in Feb). It will also delay the 60+ crypto companies (word of mouth) that have filed for a Reg A+ offering, which allows companies to offer shares to the general public. Without approval, a lot of those tokens cannot be legally distributed. ([KWu](#))
4. The two greatest American lies: "Rising debt isn't a big deal because the dollar is a reserve" (we'll lose reserve status by 2030); "If you don't like things, vote!"

(voting for big gov't right (R) and big gov't left (D) isn't a choice if you're in the small gov't party. "Exit" is a choice. Long live bitcoin!)

5. Speaking of losing reserve currency status... Given Brexit, the Chinese economic slowdown, the rise of global populism, etc. 2019 will be the year a top 50 central bank starts purchasing crypto as a speculative bet on a new type of disaster hedge. Look to mid-inflation developing economy banks in particular. What is there to lose? It's an asymmetric bet.
6. Things aren't all doom and gloom. It doesn't take magic mushrooms to appreciate we live in an era of abundance. The average time an average human needs to work to purchase a given commodity **has fallen 65%**. As that falls, we get further from a Mad Max-level dystopia. My favorite 2019 prediction: things will continue to get better! So stay rationally optimistic.



"The Earth was
**379.6 percent
more abundant in 2017**
than it was in 1980."

The Simon Abundance Index
HumanProgress

Image: HumanProgress.org

Information overload:

1. The bad news is that along with our commodity abundance, we also have information abundance, yet finite attention. We tend to get more of our information based on its memetic value these days (see #41), and what is "popular" vs. what is mentally nutritious, which is one reason the web is such a wasteland of messy, unstructured, and unreliable information. Curation markets will be massive for solving some of our attention and information problems even if early concepts have struggled.
2. Yes, token curated registries launched to date have been disastrous, ineffective, and offered questionable incentives. ConsenSys has a few interesting

experiments to keep an eye on though ([TruSet](#), [TCR.Party](#)), and I'm watching developments from Slava ([Relevant](#)) and Thibault ([Continuous Organizations](#)) closely as we think about how to roll out Messari's token registry.

This primitive is young. There are solutions to all the critiques...

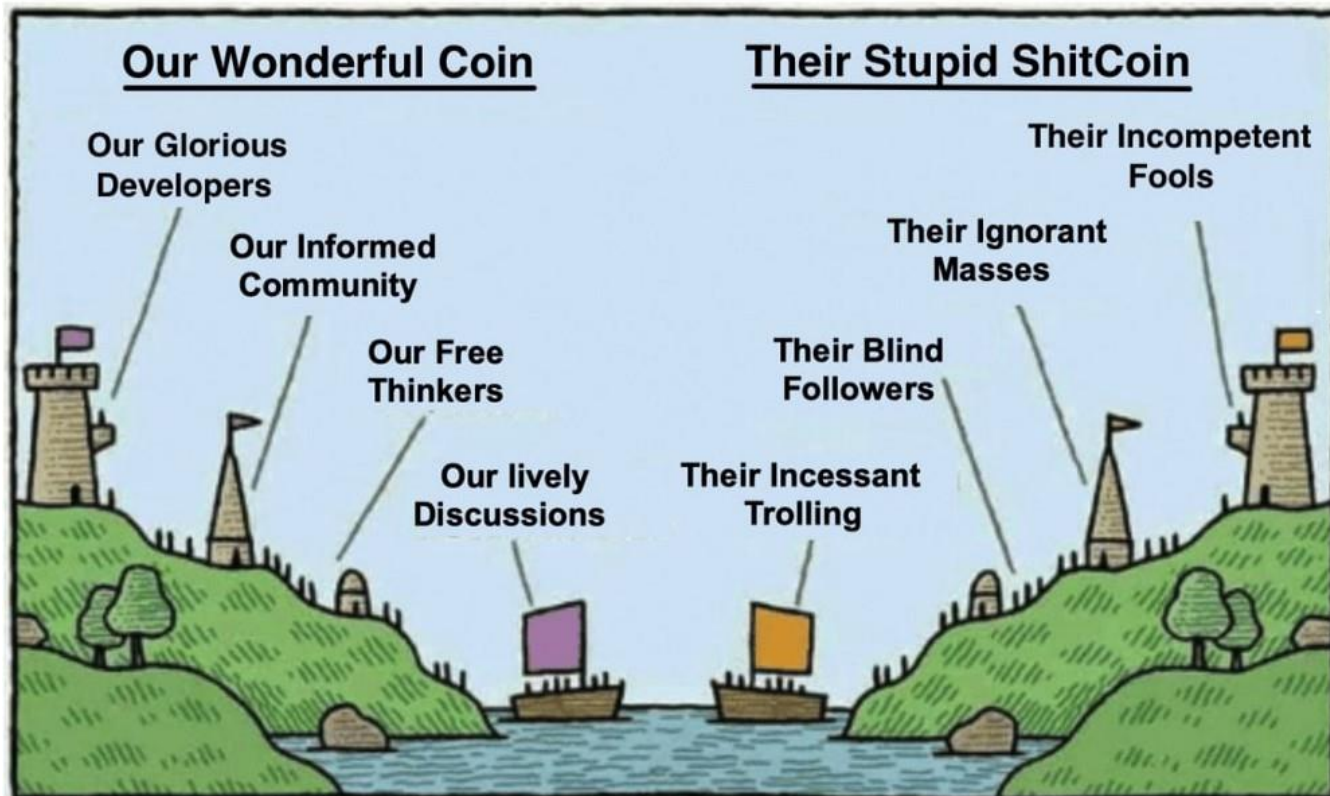
+ popularity contest! -> well, design TCRs for popularity contests, then! + easy to corrupt at launch! -> well, distribute the registry tokens slowly to strategic parties and incorporate lock-ups / illiquidity by design!

+ who's actually going to vote on this?! -> make sure you include delegated voting logic so token-holders can vote by proxy!

3. Lots of good niche data services. No great information aggregators and curators. Messari is going to win this market. (Or I'm going to be eating ramen until the Citadels pop up.) Stay tuned.
4. People will finally realize valuation metrics like NVT have no predictive power because you can game them. We'll also get much [better measures of token size and importance](#) than market cap, likely a liquidity adjusted market cap.
5. Technical analysis on BTC and other liquid cryptoassets will become much less effective as real prop shops begin operating with meaningful capital. Crypto economic data will become more valuable as people bargain shop, and that will coincide with a decline in CoinMarketCap's dominance.

Memes and Meanies:

1. Success in crypto community building hinges on memes:
Pomp: "The Virus is Spreading." "Long Bitcoin, Short the Bankers."
Blockstream: "Make bitcoin great again." "Don't trust, verify."
Neeraj: Take the least sexy crypto role (policy), and win w/ 24/7 memes.
2. When you're behind in the polls, go negative. Or troll your way to the top.
Vitalik coined the term bitcoin maximalism in 2014 to combat critics.
Gemini's "Crypto Needs Rules" campaign is BRILLIANT.
Mike Dudas / TheBlock started with obnoxious as a strategy. It's working.
3. One of my favorite lines from 2018 came from Ameen Soleimani, who told me BTC vs. ETH communities were like Spartans vs. Athenians [in this scene](#) from 300. 2019 will show which ETH Athenians earn their warrior stripes and which jump ship to other protocols. Many Ethereum folks have never been through a crypto bear market. Many will run out of money. How religious will they be once the dry powder runs out?
4. #XRPthestandard is a top all time astroturfing campaign from the Ripplecoin aficionados. These folks have reinvented truth, attacked and pissed off everyone else in crypto, and still get to delude themselves into [thinking a former President is a fan](#) of the project. "I'm not even mad. That's amazing."
5. You look like this when you get all tribal about your favorite crypto. But you'll never admit it. (h/t [Roger Ver](#))



All time favorite cartoon. Gets better with age.

#Influencers

1. [The 1 million bitcoin lawsuit against Craig Wright](#) will prove once and for all that he is, in fact, not Satoshi, but he will continue pandering to the less sophisticated masses about his early involvement to shill shitforks and obvious scams until he has no more ammunition (social, crypto, or otherwise) left. (h/t [Ben](#))
2. (47a, for those wondering the count.) Actually, Ben's wrong. I continue to believe Craig was at least part of whoever created Satoshi Nakamoto, and he's been hiding in plain sight. [This lawsuit](#) IS the most interesting thing to watch this year in the search for Satoshi.
3. CoinDesk, Breaker, TheBlock are all tracking the movements of execs in the industry well and killing it on the research and content. But if CoinDesk doesn't fix its site performance and cut down on the dogshit adware, TheBlock will eclipse them by year-end. CoinDesk has great content, but is totally unreadable. It's Forbes-level terribleness on Chrome.
4. I'm intrigued by efforts I've seen to score crypto twitter using a "people rank" algo that monitors strength of following. Heavy bias for tenure in crypto, but the work [Iconomist](#) & [Hive.one](#) have done is interesting. These will end up

being incredible tools to leverage in curation markets.
(Bonus points, I'm in a fun sandwich between two former masters:)

# 19	 barrysilbert  180 690 followers	VC	467 POINTS
# 20	 twobitidiot  85 690 followers	BUILDERS	459 POINTS
# 21	 ethereumJoseph  99 592 followers	BUILDERS	456 POINTS

I'm so popular. When will you realize I'm a fraud?

Markets & Price

1. A portfolio consisting of 50% Tron + 50% XRP will outperform a portfolio consisting of 50% LTC + 50% ETC. (Centralized marketing and execution definitely helps.) The S&P 500 will outperform HOLD10 on a risk-adjusted basis. (h/t [Qiao](#)) BOLD
2. Look to developing markets for salvation: If there's a bull market in 2019, it'll be driven by Europe, South America, or Africa. If anyone builds an open finance killer app on Ethereum, it will be a team based in a developing country. (h/t [Qiao](#))
3. Bitcoin isn't dead. Ethereum isn't dead. But the "great cleansing" of top 100 cryptos on CMC won't happen overnight. It takes time to flush out crap. We only get "decoupling" of quality and crap during bear markets, *not* vertical bull runs. Look at the [Dec 2013 top 20](#) assets, they're almost all long gone.
4. Returns in crypto will be captured by money/store of value like assets vs startup equity. BTC will outperform equity in Coinbase, Binance, BitMEX, and all of today's other crypto unicorns over the next five years. If this doesn't prove true, it's because BTC somehow lost its lead.
5. BTC and ETH have bottomed. (Maybe wishful thinking, but the November crash sure felt like January 2015.)
6. Filecoin, Telegram, and Cosmos will launch within the next 12 months and catapult to the top 10 crypto assets by market cap. (That's a lot of top 10 turnover in a less liquid market if I'm right.)

Privacy

1. Lightning will start to be used as a privacy layer for BTC transactions. There will be a lot more talk of privacy solutions for later-1 on bitcoin, but no progress that impacts end users. (h/t [Dan](#))
2. Arjun [outlined](#) the monster year in Bitcoin privacy research. But I'm skeptical hosted wallets and exchanges will make speedy upgrades when these features are rolled out due to regulatory concerns. The race is on between Chainalysis + Elliptic (the two largest on-chain data forensics companies) and crypto privacy engineers to unshield, obfuscate, unshield transactions (ad infinitum). Monero, ZCash, Bitcoin, Grin, BEAM...there's so much to look forward to if you're a hardcore privacy advocate...or a technical sleuth. Cops and robbers for Web 3.0.
3. Privacy tech's success also means we'll eventually we'll have to move to an opt-in disclosures system, where most economic actors provide their business partners or regulators/authorities with view keys to key accounts and transactions. The powers that be won't let a multi-trillion dollar shadow financial system emerge with no surveillance capacity. Entrepreneurs know this, so will ultimately be more proactive about this.
4. No one really understands privacy solutions. Few actually use the tools that **do** exist. If privacy upgrades aren't abstracted away by developers, or there aren't real economic incentives to adopt them, no one will push for them. This is a pithy take, but it's worth reiterating over and over and over again because zk-SNARKS, zk-STARKs, Confidential Transactions, etc. aren't worth anything if they aren't actually embedded in useable products.
5. Great take from researcher [Hasu](#) (h/t Token Daily): *"Bitcoin will continue to get more private: LN and sidechains offer full fungibility if you accept certain tradeoffs of trust and security. Dandelion will add more privacy on the p2p network layer (harder to do UTXO forensics). My fingers are crossed for Schnorr signatures in 2019 (these hide multi-signature transactions — that would be a huge deal in combination with Coinjoin). Private transactions by default would be encouraged, because it's cheaper to share a signature (the biggest/costliest part of a bitcoin transaction) with others."*

Top-Down Regulation—Boo.

1. The SEC's mandates are to facilitate responsible capital formation, promote fair and efficient markets, and protect investors. But their slowness, vagueness, and demonstrated enforcement-first mindset will lead to more market opacity, and offshoring. U.S. teams are getting frustrated that all conversations with regulators are one-way streets.
2. A large, offshore exchange will face serious legal action from a U.S. regulator (even if the exchange blocks IPs or restricts U.S. user access via its terms of service). It will set up an epic legal showdown, as \$10 billion companies usually don't roll over without a fight. (h/t [Eric](#))
3. Ripple will get away with murder. Too well capitalized (~\$500M in 2018 \$XRP sales), too well connected (ex-regulators Mary Jo White, Ben Lawsky, Gene

Sperling are advisors or directors) to face trouble for their private money sales to retail. Negligible, if any, fine, showcasing the ineffectiveness of relying on the state.

4. Thanks to SEC/CFTC hostility and uncertainty, we'll see more anonymously deployed token projects and sales. Some will be legit like [MimbleWimble](#). Others will be epic scams made possible only because SEC regs drove people to this behavior. (#self-regulation) (h/t [Dan](#))
5. Token ratings and research shops in the U.S. are going to flirt with the SEC as well. Rating tokens "BB" based on your interpretation of the NVT ratio, a TradingView chart, and a witty telegram post is going to lead to some questions about how and who you're marketing those scores to, anyway.
6. The SEC will do nothing of real import aside from impede the progress of good teams, pick easy cases, make scammers harder to identify, and block the actually useful bitcoin ETF. Elon spoke for [crypto twitter](#) when he said: "I want to be clear. I do not respect the SEC."
7. This was a [good take from Arjun](#) that I pretty much agreed with wholeheartedly: *"Some of the US-based teams working on the DeFi stack are taking on material risk and will face regulatory scrutiny in the US (70% confidence) given their move into structured products. This will test the runaway killer app of Ethereum: regulatory arbitrage (first with the offering of unregistered securities offerings and now with quasi-legal structured derivatives), as teams "move fast and break [the law](#)." While engineers are discussing "compounding financial primitives," I'm worried about compounding technical (or legal) risk."*

Market / Self-Regulation – Yay!

1. There will be a ton of asset delistings this year. For many exchanges, trading certain cryptos is too much of a headache for little to no return. I'm talking about the absolute *gems* like Clams, PascalCoin, Viacoin, and Primecoin. (All still on Polo. All sub 50k in daily trading volume and single digit millions float. There will be blood...)
2. There will be voluntary and involuntary conversions of ICOs to security tokens. [ICONOMI](#) did it the "voluntary"(?) way. Others will do it the involuntary way either via [SEC enforcement](#) (Airfox, Paragon) as teams are forced to brush up on investor rescission rights. We also have a new brand of [activist investor](#) who's entering the fray, something I'm especially excited to watch unfold with respect to converting tokens to equity, or other protocol tokens.
3. Messari will onboard 100+ projects to our crypto registry. (We're closing in on 20. If you're interested in staking / sponsoring your favorite token team, [hit us up!](#)) Binance, Coinbase Pro, Polo, and others will require basic disclosures + add them to their sites.
4. I'm really hoping GDF, the Blockchain Association, Coin Center, the VCA, ADAM and others [play nicely together](#). Crypto self-regulatory groups seem like

they're going to almost inevitably compete and talk past each other. I hope I'm wrong, but standards setting in 2019 will look like this:

Opinionated people tilting against windmills wrt standards setting.

Life hacks

1. For those who swear to make new years resolutions, but have a tough time keeping them, this is an awesome [habits tracker](#), you can use. I recommend also reading the [original thread](#) on forming new habits from Ali at a16z.
2. This [multiple inbox custom gmail implementation](#) changed everything for me a few years ago. I actually keep up with email now, and regularly hit inbox 0. (*Update: Jinx. I'm now at 50 again.*) It's tough to get shit done with a messy desk or desktop or inbox. I promise you, it's worth the 30 minutes to set this up. It will pay dividends for years.
3. Don't worry if you're not waking up at 4am, meditating, working out for three hours, eating keto, and journaling. Self-improvement is great, but this is how Ali's boss claims to start his day:

Tim Ferriss: Do you have any particular morning rituals that are important to you?

Marc Andreessen: Sleep in as long as possible.

Tim Ferriss: Sleep in as long as possible? When do you usually wake up?

Marc Andreessen: Try not to blow through any red lights on the way to work.

Tim Ferriss: When do you usually wake up?

Marc Andreessen: So 45 minutes before I have my first meeting. I do what they call the hot docking. It's like the controlled crash into the office. It's the whole 14 things to be successful people do in the morning. I can't even imagine.

Tim Ferriss: Do you drink coffee?

Marc Andreessen: Yes.

Tim Ferriss: You do?

Marc Andreessen: Yes.

Tim Ferriss: That was an emphatic yes.

Marc Andreessen: If it has caffeine in it, I drink it. The perfect day is caffeine for 10 hours, alcohol for 4. It balances everything out really well.

Tim Ferriss: It sounds a lot like my day.

Marc Andreessen: I'm not shy for a second about that.

Tim Ferriss: The Silicon Valley speedball.

Marc Andreessen: That's right.

pmarca knows what's up

Protocol Wars

1. For the die hards trying to keep up with the various ETH scaling proposals, Arjun did a nice job aggregating them all. If this looks complex, it's because it is. Now try to imagine Ethereum 2.0 actually coming to market successfully in the next 18 months herding all of these cats:

7) 2018 was a big year for proof of stake research with [June's deprecation](#) of [EIP 1011](#) (Hybrid Casper FFG), scrapping the hybrid PoW/PoS step in favor of moving to pure PoS. The next phase for Ethereum—first termed *Shasper* (Casper + Sharding), now called *Serenity* (Ethereum 2.0)—has [six distinct phases](#), which stretch over several years. There are 8+ dev teams working on independent implementations including:

- ChainSafe Systems, building a [JS implementation](#) called Lodestar
- 50-person ConsenSys-backed PegaSys, building an [enterprise-grade implementation](#) in Java
- An independent group called Harmony, building a [Java implementation](#) based on the original EthereumJ client
- Parity Technologies, building an [Ethereum 2.0 client](#) in Rust
- Prysmatic Labs, building a [Go client](#) (recently, Raul Jordan [announced](#) the team had full test coverage with the latest spec)
- Sigma Prime, building a [2.0 client](#) in Rust
- Status, makers of the Ethereum-based [messaging app](#), building the first [mobile-native client](#) in the language Nim
- Trinity, a team predominantly backed by the Ethereum Foundation, building a [client](#) in Python

Despite seeing major setbacks and changes to the Ethereum 2.0 roadmap, I think the first phase will ship some time in Q4 2019 (*70% confidence*), albeit with friction.

yikes.

1. EOS will surpass ETH. EOS could surpass ETH in dapp activity; as serenity delays continue, developer mindshare will wander; EOS smart contracts use C++ and compile into WebAssembly (better dev experience); on-chain governance works in EOS, isn't close in ETH. (h/t [Jane](#))
2. Various ETH competitors with seasoned executives, top VC backers, and technically superior platforms will run aggressive marketing campaigns, but stall as ETH's culture, grassroots mindshare, and developer network-effect lead prove too strong to overcome. (h/t [Dan](#))
3. This month could be a messy one in Ethereum. We'll see major pushback from disenfranchised ETH miners around the Constantinople upgrade (which, among other changes is going to crush ETH miner margins further by reducing block rewards 33%). [We'll find out tomorrow.]
4. Protocol M&A! In this bear market, consolidation is inevitable at the company level. But it will make more sense for many teams to merge together than fork away from each other. The TRON and Stellar acquisitions of BitTorrent and

Chain were the biggest M&A eye-openers in 2018 (even moreso than Polo to Circle and Earn to Coinbase). This year, the question isn't about companies that will get acquired, but how many low market cap crypto tokens will "merge" with larger competitors?

5. We'll see more tokens [buy back portions of their supply](#) like ICON did. Here's a few token projects trading well below their estimated [balance sheet ETH coffers](#):
Aragon: Market Cap \$14MM | Balance Sheet \$26MM
DigixDAO: Market Cap \$42MM Balance \$58MM
Gnosis: Market Cap \$13MM,117 Balance \$28MM
6. Could we see more tokens proactively burn some of their undistributed treasury tokens to ensure the majority of their supplies are decentralized [like Numerai did](#)? If a token project: a) issued 100% of its supply at inception, b) currently holds more tokens in treasury than is circulating, c) doesn't have a pre-defined secondary sales process, then the entity should burn a significant portion of its treasury tokens! That would look like a share repurchase in equities, but with no capital outlay required or board approval. Just a snap of the fingers.
7. While it would be great to continue to see new crypto VC blood enter the fray to take advantage of bear market prices, the universe of crypto fund managers is unlikely to see many new entrants until the next hype cycle. The ones that closed their funds know they are now in position to "[Raise during bubbles, deploy during busts.](#)"
8. We'll continue to see an explosion of [ecosystem development funds](#), but for smaller projects. Metaverse was an [interesting early example](#). Multicoin capital frames it well: *"Just as a traditional VC firm would set aside capital for follow on rounds, we believe that crypto investors who typically invest in protocols will find it's a best practice to also set aside capital for supporting the network."*
9. Bitcoin benefits from its static nature. There's just one problem: bitcoin will have more contentious hard forks in the future. A big one will be around changing the hard cap as the fee market compresses, another will be—you guessed it—around the block size. We know forks are risky and dilutive, but the next one will be a real threat, because it will likely incorporate significant privacy upgrades that governments will not like and block at all costs.

Then They Join You

1. I'm bearish on Facebook's stablecoin in the short-term. The WhatsApp Indian remittance target use case is not compelling, and crypto regulation in India is notoriously tough to navigate. USD works fine as a parallel currency most places, and competitive services are entrenched. The Indian government won't look kindly upon a private company undermining its monetary sovereignty. (h/t [KWu](#))

2. Very few blockchains that raised mega pre-launch rounds will find product-market fit. One that will actually launch, and have wild success, will be Telegram. Top team, massive user base, crypto ethos, and they'll fork whichever relevant crypto protocols work for their own purposes. Good artists copy. Great artists steal. (h/t [Eric](#))
3. As global macro fears return, talk of central bank digital currencies—and their Orwellian surveillance and control—will excite Big Brothers globally. BTC will remain an antidote to financial totalitarianism. CBDCs “replacing bitcoin” will become this cycle’s “blockchain not bitcoin” stupid establishment meme. (h/t [Dan](#))
4. China will be the first to issue a sovereign-backed digital currency that **actually** sees widespread adoption. China’s economy is already highly digitized, and this could be a way for the Yuan to replace (or seriously threaten) USD as the dominant reserve currency. (h/t [KWu](#))

Great Artists Steal

Throwback to a few October 2017 forward-looking predictions from Daniel Jeffries that I really liked, and am going to steal for 2019. Full post is [here](#).

1. *“Many governments will not sit by and lose control of the money supply without a vicious fight. Anyone working on a project right now should be anticipating protocol level assaults on decentralized cryptos and designing defenses against them.”* China is still a major threat to bitcoin. The U.S. less so, because the government is so slow and dysfunctional.
2. *“The same factors that make it hard to form consensus across a blockchain, make it hard for all the world’s governments to agree on anything. They won’t be able to do it. Some governments will love decentralization and others will hate it.”* Smaller governments (e.g. Malta, Singapore, Estonia) can make asymmetric bets on crypto and potentially catapult their economies forward. This trend will continue to accelerate as PBOC crackdowns continue and as the SEC pursues more frequent enforcement actions.
3. *“We will have four dominant meta coins, plus fifty to one hundred minor coins, and infinite virtual variations of these coins, plus state coins. At this point I can only see four types of coins needed, with a blockchain of blockchains (or post-blockchain tech) seamlessly swapping them as needed to consume services: Deflationary Saver Coin — hoarding and investing, these rise over time like a “digital gold” — it’s the reason Bitcoin started in the first place; Inflationary Spender Coin — inflationary coin mirrors the dollar today, these are the stablecoin experiments; Action Token — actions on the network that should always be free (i.e. voting); Reward Token — designed to flow around the system as a digital representation of karma, incentivizing good behavior and punishing bad behavior; You could literally*

build the ultimate universal system with just these four coins. Every other coin could simply act as a subcomponent with different metadata."

And my favorite three from the ~40 I read on Token Daily's curated 2019 prediction piece. (Curate the curators!)

1. Alex Pack (co-founder, Dragonfly Capital) *"The largest crypto businesses in the world are already in Asia — of the top 20 exchanges by volume no more than a handful are based outside of Asia, as are the largest mining companies. In 2019, we will start to see these exchanges and mining companies act as distribution channels, offering new financial products and smart contract-based applications to their users."*
2. Benny Giang (co-founder of Cryptokitties) *"Korean market will have consolidation amongst technology and crypto businesses next year. There will be a huge effort amongst some of the top gaming companies to break into this space. What this means as a whole, is that Korea will be leading the way for consumer adoption early next year. We'll see lots of questions about decentralized systems being slow vs semi-centralized systems with mass adoption. (The Multicoins Capital debate on platform-grade vs. sovereign-grade censorship resistance)"*
3. Benny again *"Japan's largest tech companies have secretive R&D teams. From my perspective, I don't think a lot of the efforts will translate into new business lines in 2019. However, there is a handful of experienced veteran game producers who have formed their own blockchain gaming studios. A lot of high-quality blockchain games will be released in Japan late Spring to Summer of next year. This will set a new standard for hybrid on/off chain blockchain games."*

Us and Me

1. I've always been the best at shameless self-promotion. My thought leadership, influencer status, pioneer pedigree, plus general authenticity and good humor is why Unqualified Opinions will be a top 50 crypto newsletter and podcast by 2020. Share with your friends, and show some bear market love. [Give a gift subscription](#). Or contact us about corporate subscription rates. No one ever got fired for paying an idiot with the corporate Amex. (At least no one I'd tell you about.)
2. But actually, I'm terrified UO is going to suck, and it's going to be all my fault and CT and the subscribers alike will finally tell me what a fraud I am. If our new podcast underperforms, remember this interview [instead](#), which captures my thoughts on the year ahead. It's me being my best self.

Hope y'all are your best selves in 2019 as well.

Keep building. Beat the bear.

-TBI

Links

- <https://medium.com/tbis-weekly-bits/95-crypto-theses-for-2018-ca7b74f8abcf>
- <https://store.casa/lightning-node/>
- <https://medium.com/@arjunblj/crypto-theses-for-2019-dd20cb7f9895>
- <https://twitter.com/aantonop>
- <https://www.youtube.com/watch?v=c4TjfaLgzj4>
- <https://medium.com/@twobitidiot/the-21mm-btc-soft-cap-71e14cd09946>
- <https://medium.com/@lrettig/how-open-is-too-open-bfc412cf0d24>
- <https://www.coindesk.com/developers-rally-around-ethereum-1x-a-new-roadmap-for-faster-scaling>
- <https://medium.com/@demibrener/state-of-crypto-2018-market-trends-7066f5484217>
- <https://twitter.com/benhoneill>
- <https://twitter.com/ericturnr>
- <https://stablecoinindex.com/>
- <https://messari.io/blog/96-theses>
- <https://blog.0xproject.com/ecosystem-update-ddex-and-the-0x-roadmap-5d201cafa133>
- <https://blog.0xproject.com/introducing-the-0x-market-maker-program-42edc902b1f0>
- <https://twitter.com/QWQiao>
- <https://www.sec.gov/news/press-release/2018-258>
- <https://www.theblockcrypto.com/2018/12/07/bitmex-lets-you-bet-big-on-bitcoin-for-a-price/>
- <https://medium.com/makerdao/makerdao-partners-with-ripio-to-bring-dai-to-south-america-via-fiat-on-off-ramp-e22ac71a210d?source=rss-----blockchain-5%C2%A0>
- <https://mkr.tools/>
- <https://medium.com/@hasufly/maker-dai-stable-but-not-scalable-3107ba730484>
- <https://messari.substack.com/p/code-will-be-law-unqualified-opinions>
- <https://veil.co/>
- <https://medium.com/veil-blog/introducing-veil-649036f9d492>
- <https://avc.com/2019/01/what-is-going-to-happen-in-2019/>
- <https://twitter.com/katherineykwu>
- <https://humanprogress.org/article.php?p=1603>

- <https://www.truset.com/>
- <https://www.tcr.party/>
- <https://relevant.community/>
- <https://hackernoon.com/introducing-continuous-organizations-22ad9d1f63b7?gi=f4d0f574fe7a>
- <https://blog.nomics.com/essays/crypto-market-cap-review-emerging-alternatives/>
- <https://www.youtube.com/watch?v=gl6sARmxEuc>
- <https://ripple.com/insights/president-bill-clinton-keynotes-swell-2018/>
- <https://twitter.com/rogerkver/status/1081541185921941509>
- <https://messari.io/article/u-s-court-denies-craig-wright-motion-to-dismiss-1-1-million-btc-lawsuit>
- <https://economist.com/>
- <https://hive.one/>
- <https://coinmarketcap.com/historical/20140112/>
- <https://twitter.com/robustus>
- <https://twitter.com/hasufl>
- <https://www.theblockcrypto.com/2019/01/08/mimblewimble-history-technology-and-the-mining-industry/>
- <https://www.youtube.com/watch?v=cRNypdYQoWk>
- <https://medium.com/iconominet/a-new-chapter-for-iconomi-transformation-of-corporate-governance-and-issuance-of-equity-tokens-dc603df2272b>
- <https://www.sec.gov/news/press-release/2018-264%C2%A0>
- <https://www.businesswire.com/news/home/20181219005016/en/Peter-Thiel-Digital-Currency-Group-Invest-Crypto>
- <https://messari.io/registry>
- <https://messari.substack.com/p/sympathy-for-the-sec-unqualified>
- <https://threadreaderapp.com/thread/1079768556882092032.html>
- <https://twitter.com/ali01/status/1078647576201703427>
- <http://klinger.io/post/71640845938/dont-drown-in-email-how-to-use-gmail-more>
- <http://janeylwang/>
- <https://sludgefeed.com/icon-surges-after-announcing-token-buyback-program/>
- <https://projecttransparency.org/>
- <https://www.coindesk.com/numerai-to-cut-token-supply-by-10-million-to-become-decentralized-as-fck>
- <https://twitter.com/cburniske/status/1082148158602240000>
- <https://multico.in.capital/2018/10/23/the-evolving-role-of-crypto-investors/>
- <https://insights.dcg.co/introducing-metaverse-ventures-f82fc09a5f83>

- <https://hackernoon.com/what-will-bitcoin-look-like-in-twenty-years-7e75481a798c>
- <https://messari.substack.com/subscribe?&gift=true>
- <https://www.youtube.com/watch?v=ik83dXsbAls>

Tweetstorm: Bitcoin as SoV

By [Dan Held](#)

Posted January 14, 2019

1. Satoshi's Vision™ is a silly endeavor, as it doesn't matter what it was, we are where we are now. However, those pushing the "Bitcoin was first made for payments" narrative insist on cherry-picking sentences from the white paper and forum posts to champion their perspective.
2. The following tweetstorm is a categorical repudiation of this tired narrative. Bitcoin was purpose-built to first be a Store of Value (SoV), a thread:
3. How do we determine Satoshi's intention? We need to look at his ideology, description of functionality/architecture, timing, and audience. Let's start with how Satoshi describes the problem Bitcoin solves. In his first public comms after the whitepaper, in the first paragraph:
4. "The root problem with conventional currency is all the trust that's required to make it work. The central bank must be trusted not to debase the currency, but the history of fiat currencies is full of breaches of that trust." - Satoshi
5. He later expands on that Libertarian thought in his other writings:
"[with Bitcoin] we can win a major battle in the arms race and gain a new territory of freedom for several years." — Satoshi Nakamoto
6. How does Satoshi describe Bitcoin? His forum posts provide insight through his consistent gold/metal analogy:
"Bitcoin [is] more like a collectible or commodity." - Satoshi
7. *"In this sense, it's more typical of a precious metal. Instead of the supply changing to keep the value the same, the supply is predetermined and the value changes. As the number of users grows, the value per coin increases" - Satoshi*
8. *"As a thought experiment, imagine there was a base metal as scarce as gold but with the following properties: [not useful/no utility]. And one special, magical property: can be transported over a communications channel" - Satoshi*
9. *"If there were nothing in the world with intrinsic value that could be used as money, only scarce but no intrinsic value, I think people would still take up something. (I'm using the word scarce here to only mean limited potential supply)" - Satoshi*
10. *"It might make sense just to get some in case it catches on. If enough people think the same way, that becomes a self fulfilling prophecy." - Satoshi*

Satoshi here clearly highlights that Bitcoin's scarcity gives it value... as a SoV.
Limited supply is meaningless for VISA

11. So we now have an idea of Satoshi's motivations, and how he describes Bitcoin, but what does his timing tell us?
Bitcoin's launch during the 08' financial crisis was not coincidental. Satoshi had been coding Bitcoin for the last 2 years. Let's look at the sequence of events
12. Jan - July: Fed tries to stop the housing bust: Fed bails out Bear Sterns. Paulson explains the need to bail out Fannie Mae, Freddie Mac the two agencies that held or guarantee 50% of the \$12T in US mortgages.
13. Aug 18: Satoshi registers [Bitcoin.org](https://bitcoin.org)
Sept 15: Lehman Brothers files for bankruptcy, the largest in U.S. history (\$600B)
Sept 17: Investors withdrew a record \$144B from their money market accounts. During a typical week, only about \$7B is withdrawn
14. Oct 3: Bitcoin whitepaper PDF likely created
Oct 13: Treasury Secretary Paulson talks with 9 major bank CEOs. The total bailout package ~\$2.25T
Oct 21: Fed lends \$540B to bail out money market funds
Oct 31: Satoshi publishes the Bitcoin whitepaper
15. With the 2008 financial crisis, trust had been lost in a world that ran on trust. Bitcoin was launched in a time of absolute necessity, Satoshi planted the seed at precisely the right moment. The world didn't need a new VISA, they needed an alternative to banks.
16. So we now have an idea of Satoshi's motivations, how he describes Bitcoin, and his timing, what about this initial audience for the whitepaper? How did he market his message?
17. Satoshi crafted the whitepaper as a call to arms for his target audience: the Cypherpunks on the cryptography mailing list. Key components of their ideology are privacy and finality. His message needed to resonate with them as they would have to help him build it.
18. "Therefore, privacy in an open society requires anonymous transaction systems. An anonymous system empowers individuals to reveal their identity when desired and only when desired; this is the essence of privacy." - A Cypherpunk's Manifesto
19. Many point to this in the whitepaper "peer-to-peer version of electronic cash would allow online payments" as proof that Satoshi meant for Bitcoin's main purpose is to disrupt VISA. However, "cash" represents a pseudonymous push payment in contrast to a credit-based system
20. Cash is a bearer asset. Let's look at the whitepaper with that in mind:
"A purely peer-to-peer version of electronic [bearer assets] that would allow

online payments to be sent directly from one party to another without going through a financial institution."

21. Note that the origin of the word "cash" is "caisse" (French) meaning money-box. So cash is by definition store-of-value. Other Cypherpunks had used the word cash in their whitepapers to reflect that functionality, like "HashCASH", "eCASH", etc"
22. In the other part of the whitepaper sentence the phrase "peer-to-peer" has been used as well against the SoV narrative. Charlie Lee has a great tweet storm that addresses this point of contention:
23. *"Bitcoin isn't "peer-to-peer." Payments are sent from sender to miners, who record it on a distributed ledger. The recipient receives the payment when it's recorded. BUT, this is facilitated by a p2p network where transactions are broadcasted."* [@SatoshiLite](#)
24. *"Lightning network payments, on the other hand, are p2p payments. They are sometimes direct p2p, sometimes indirect p2p. LN payments have to be sent from p2p to get from the sender to the recipient. Both have to be online, just like other p2p networks like BitTorrent"*
25. *"Bitcoin with Lightning Network more closely fits the Bitcoin whitepaper's title: "A Peer-to-Peer Electronic Cash System." This is Satoshi's Vision."* - [@SatoshiLite](#)
26. He wrote the paper to fit his target audience, but the source code implementation were his product specs. "If the Bitcoin Whitepaper is the Declaration of Independence, the Source Code is the Constitution" - [@pierre_rochard](#)
27. *"The functional details are not covered in the paper, but the sourcecode is coming soon."* — Satoshi Nakamoto
Aka the whitepaper was marketing, the important details are coming.
28. In true Cypherpunk fashion, Satoshi's whitepaper was quickly followed by code release in January 2009. The notion that good ideas need to be implemented, not just discussed, is very much part of the culture of the mailing list.
29. Just focusing on the whitepaper is a gross misinterpretation, here are the things not described in the whitepaper, but included in the source code or later defined by Satoshi: 21M hard cap, 10 minute blocks, 1 mb block caps.
30. If Satoshi wanted Bitcoin to first be used as a medium of exchange to purchase goods and services, he would have made it inflationary. People don't spend deflationary currencies when they can make the same purchase in infl. curr. There's even a name for It, Gresham's Law
31. Which is entirely intuitive. Why would any average consumer spend their Bitcoin with the perception that it will be worth more in the future when they can spend their fiat that they KNOW will be worth less?

32. So far that doesn't sound like he's trying to disrupt VISA now does it? And if that wasn't made perfectly clear, he permanently etched this message into the Genesis Block:

"The Times 03/Jan/2009 Chancellor on brink of second bailout for banks"

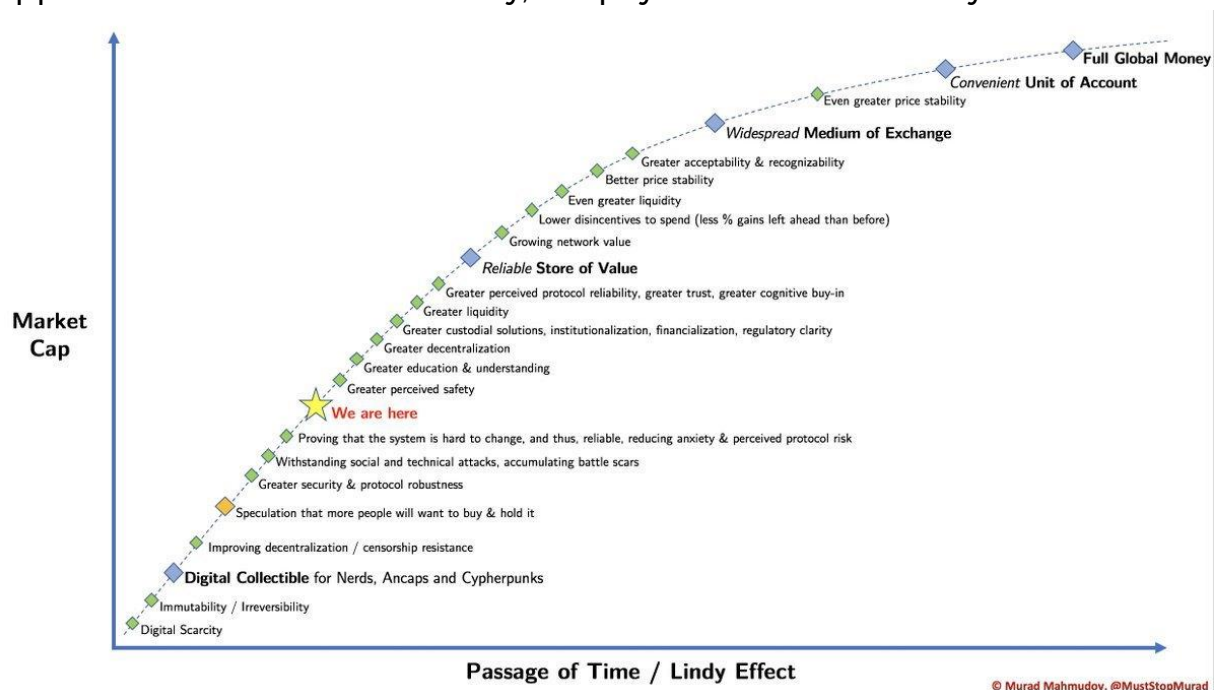
33. To take it a step further, as a subtle jab to central banks, he chose his birthday as the date the US made gold ownership illegal through EO 6102 April 5th. He chose 1975 as his year of birth which is the year when the US citizens were allowed to own gold again

34. And finally, why did Satoshi choose to be anonymous if he were just disrupting payments?

What he was trying to accomplish was clear, he wanted to build a new backbone for the financial system. Bitcoin isn't merely digital cash, but an alternative to banks.

35. And how does a new money get created? A new money comes into existence through stages: Collectible, SoV, MoE, and UoA.

SoV and MoE aren't mutually exclusive. It's about where in the cycle of appreciation we're in. At maturity, the payment use case finally makes sense.



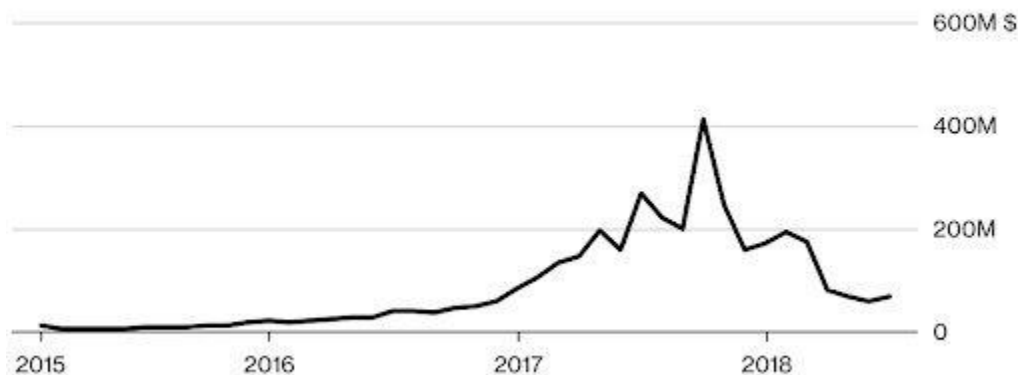
36. Some may balk at the SoV terminology for Bitcoin since the price fluctuates. However, nothing in this life has a "stable" value, the longest running fiat currency, GBP, has lost 99% of its value since inception. Bitcoin has all the traits of a good SoV

37. Bitcoin is stable. The protocol has a 99.99989% uptime which is higher than USD. The "fluctuation" you see is the volatility of the world flowing into the stability of Bitcoin in ebbs and flows.

38. When applying "The Szaboian Theory of Money Origins" to Bitcoin, it is reasonable to conclude we just barely left the "collectible phase" and are now witnessing its first steps into "Proto-money" [@Willem_VdBergh](#) [@NickSzabo4](#)
39. This phase, which is characterized by its primordial exploration of the SoV properties of the commodity, can easily take a decades to properly mature. Volatility is part of this maturing process.
40. People pushing the MoE narrative at this moment in time are counterproductive to adoption. By creating these expectations, which are unattainable at the moment, many people will get burned or disillusioned. This is a big loss for adoption and for the affected individuals

Amount of Bitcoin Received by Top Merchant Processors

In millions of U.S. dollars



Source: Chainalysis Inc.

41. *"Only by informing people correctly about the use case Bitcoin has *at this moment* can we maximize its adoption and prevent a lot of people from making the biggest financial mistake of their life."* [@Willem_VdBergh](#)
42. So how did the payments narrative become a thing?
A/ Satoshi used it to attract the cypherpunks
B/ HODLing isn't good for business. In order to command higher valuations, startups latched onto narratives that VCs would fund. And in 2013-2016 that was "merchant processing."
43. Background on me: I was the first PM [@Blockchain](#) and [@ChangeTip](#), both attempted to get people to use Bitcoin for payments. Consumers couldn't care less, which is entirely intuitive: right now it's not faster, cheaper, or easier to use for 99.99% of use cases.
44. After all of this do you really think Bitcoin was primarily built for payments at this stage in its lifecycle?
45. If you enjoyed this tweet storm, please sign up for an e-mail newsletter which will include more of my thoughts like these. (at a date far in the future when I have time)

46. Special thanks for the insight and inspiration:

[@real_vijay](#) [@nwoodfine](#) [@saifedean](#) [@NickSzabo4](#) [@MustStopMurad](#)
[@pierre_rochard](#) [@nic__carter](#) [@hugohanoi](#) [@MartyBent](#) [@francispouliot](#)
[@TuurDemeester](#) [@arjunblj](#) [@jimmysong](#) [@hasufl](#) [@_prestwich](#)
[@CremeDeLaCrypto](#) [@SatoshiLite](#) [@MrHodl](#)

Are Crypto Lending And Institutional Custody Good For Crypto?

First Principles

By [Caitlin Long](#)

Posted January 21, 2019

One of the network effects necessary for Bitcoin & other crypto assets to become widely adopted—including by institutional investors—is financialization, as noted by early Bitcoin owner [Trace Mayer](#). I agree with his assessment and believe all crypto assets need financialization in order to succeed, because financialization—if done properly—enables the efficient allocation of resources.

But there's a big problem. Financialization requires the development of markets for lending, and the Bitcoin protocol was not designed to allow bitcoin lending transactions on the Bitcoin blockchain. At present, bitcoin lending cannot be done in a trustless manner. The same is true for many crypto assets, but I'll focus on bitcoin in this post because financialization of bitcoin is most advanced relative to other crypto assets.

Development of lending markets is necessary and beneficial, if done right. Despite the lack of trustless lending for bitcoin at present, I'll lay out how financialization of bitcoin can be done responsibly. Building the infrastructure for responsible financialization of bitcoin is a prerequisite to attracting major fiduciary institutional investors, all of whom are held to very high fiduciary standards. Based on my past experience as a fiduciary of pensions, 401(k) plans and a university endowment, the crypto industry needs to up its game before it can become an asset class investable by the big leagues. Thankfully, some key achievements are likely to happen in 2019.

First Principles: Is Bitcoin Lending Good or Bad?

“Financialization” means the development of markets through which entrepreneurs can borrow money to finance investment in business enterprises. Notice the word *borrow*. Yes, financialization involves *borrowing money*. To understand whether debt is good or bad, let's start with first principles.

Money is a good that provides a basic service: a ledger. When you produce something of value and sell it for value, you earn one of the spots on that ledger by receiving money. You want that ledger to have a finite number of spots—in other words, you want that ledger to be *honest*. History has repeatedly proven that, over time, the most honest ledger will become the most commonly used ledger, which we call money.

Money can be exchanged for goods and services that are consumed (medium of exchange), or it can be saved (store of value)—both of these are *uses* of money, but neither is inherent to money itself. Money is simply a *good* that serves as a ledger—a way to keep score.

By definition, goods that aren't immediately consumed are saved. Saving, which means foregoing the consumption of goods that were previously produced, makes those resources available for investing ("capital goods"). People invest capital goods in order to produce even more goods or services in the future. If we don't invest those capital goods directly ourselves (e.g., a farmer planting seed corn), we can *lend* them to someone else who will. The price of borrowing these resources—the interest rate—coordinates the optimal investment of these saved resources across people, places and time.

Borrowing money facilitates the optimal investment of society's saved resources. Markets for borrowing money enable the calculation of implied interest rates for different time periods (the "spot" yield curve). And from that yield curve, parties can calculate an implied forward curve for interest rates beginning on future dates instead of today. And from that forward curve, parties can calculate the price of trade credit and financial hedges. Such financial products are *necessary* for commerce to happen in the real world. All this is good for society, if done right.

Yet, a pre-requisite to achieving these benefits is that money must first be *borrowable*. If it's not borrowable, financialization cannot occur.

So, for bitcoin & other crypto assets to become financialized, they must be borrowable.

History has proven that markets for borrowing money can become unanchored from the money itself and end up corrupting the money—first by creating substitutes for the real money, which are accepted as if they're real, and then later by creating insidious mechanisms to inflate the quantity of those money substitutes so that some players gain something for nothing. I call this "bad financialization." The temptation to corrupt money through bad financialization is strong—especially if the process is insidious and difficult to police.

Hence, owners of money must take great care to protect money against the tremendous incentive that exists to corrupt it by creating more claims to money than the quantity of money that exists.

Hence, owners of bitcoin must take great care to protect bitcoin against the tremendous incentive that exists to corrupt it by creating more claims to bitcoin than the quantity of bitcoin that exists.

Financialization is, therefore, a dicey process. But it is absolutely necessary. Without it, society cannot optimize the investment of saved resources across people, places and time. Consequently, for Bitcoin, responsible financialization will involve finding ways to lend bitcoin without corrupting it by creating more claims to bitcoin than there are bitcoins.

Here's a basic technological framework for distinguishing the good from the bad types of bitcoin financialization:

- all bitcoin lending/financial products that transact on the Bitcoin blockchain will, by definition, be the good type of financialization.
- all bitcoin lending/financial products that do NOT transact on the Bitcoin blockchain should be presumed to be the bad type of financialization—albeit rebuttable if the issuers of such products prove they are 100% collateralized at all times and that they never artificially inflate bitcoin's supply, even momentarily.

Category 1 doesn't exist yet, unfortunately. Currently there's no trustless way to settle the fiat-currency leg of a bitcoin loan, which must settle in traditional banking infrastructure (off the Bitcoin blockchain).

Category 2 includes all custodial crypto exchanges, coin lending businesses, crypto custodians, and issuers of Wall Street products that “physically” settle in bitcoin (futures, ETFs, depositary receipts, etc). These businesses actually settle most of their transaction volume off the Bitcoin blockchain. It may be possible for them to provide cryptographic [proof of reserves](#), but that's exceedingly rare. The issuers of financial products that settle transactions using traditional Wall Street infrastructure will find it nearly impossible to prove that they're 100% collateralized all the time—if they even wanted to prove it—simply because Wall Street's ledgers are never 100% in sync, and its infrastructure inherently creates more claims to assets than there are underlying assets (see [here](#), [here](#), [here](#) and [here](#) for more explanation).

To summarize thus far, please ponder this: Is debt inherently bad? No, not always. The lending of saved resources is fundamentally good because it enables the optimal investment of those saved resources.

Some types of debt are, however, quite bad. Any form of debt that creates multiple claims to the very same asset is quite bad. Why? Because these forms of debt create more claims to an asset than there are assets, thereby suppressing the asset's price. Why? All else equal, increasing the supply of something drives its price down. That's simple supply/demand dynamics.

So, applying these first-principles to bitcoin, we can draw two conclusions:

- **Bitcoin lending is fundamentally good—but only if the same bitcoin is lent exactly once.** If the same bitcoin is lent *and then re-lent* (rehypothecated), that's bad because it creates more claims to bitcoin than there are bitcoins.
- **Markets that enable the shorting of bitcoin are also fundamentally good—but only if the short seller actually borrows bitcoin *before* selling it short.** If the short seller shorts bitcoin before borrowing it, that's bad because it creates more claims to bitcoin than there are bitcoins.

In the absence of protocol-level mechanisms supporting peer-to-peer coin lending, how can bitcoin lending markets develop responsibly? The only option is to establish legal structures that clearly define and protect property rights. Even the purists would likely appreciate this, since property rights stem from natural law.

Until Trustless Bitcoin Lending Comes Along, Here's How to Prevent Bad Financialization

Property rights in the U.S. are protected by state law, not federal law, and state law also governs the creation of liens on assets pledged as collateral for loans.

But there's a big problem. No state has yet clarified the precise legal status of crypto assets or clearly defined the process for a lender to place a legally-enforceable lien on a lent crypto asset. Coin lending and coin custody businesses already exist, of course, but **every U.S. party involved in coin lending and coin custody is taking some degree of legal risk because the law is simply not clear.** In the absence of clear law, it's not predictable how judges will rule in litigation or bankruptcy.

The fiduciaries of what I call “fiduciary institutional investors”—mutual funds, pension funds, 401(k) plans, endowments, foundations and insurance companies—simply cannot take such open-ended legal risk (in the way that a hedge fund or venture capital fund can, since hedge funds & VC funds are expected to have higher risk/reward relative to “fiduciary institutional investors”). Speaking as a former fiduciary of multiple pensions, 401(k)s and an endowment, legal clarity is an absolute prerequisite.

[Wyoming is endeavoring to solve this problem—and solve it in a way that preserves the peer-to-peer nature of blockchain protocols.](#) Disclosure—Wyoming is my native state, and I've been volunteering over the past year to advance this and other legislation that attracts the blockchain industry to Wyoming by providing an enabling legal framework.

[Forbes](#) has already written a story about Wyoming's proposed bill to solve these problems, [SF 125](#), and here are the key points. If the bill becomes law, it would:

- For everyone: Provide basic legal clarity for crypto assets (“digital assets”). This isn’t rocket science, and I’m amazed no US state has done this yet. Such clarity would enable coin lending markets in the US to develop free of the legal uncertainty hanging over them today. Consequently, financialization can begin to flourish.
- For everyone: Cleanse digital assets of stale liens after two years, as long as the coins are stored in a Wyoming custodian. This solves a [problem](#) many legal scholars have identified for the sector, which is that stale liens can pop up years later—a nasty surprise for coin owners who might otherwise discover they never legally owned their coins.
- For digital asset custodians: Create a superior regulatory path for digital asset custodians to achieve the big prize, which is “qualified custodian” status pursuant to the SEC’s custody rule. Since 1940 that rule has required US investment companies (such as mutual fund managers) and large US investment advisers to store the assets they manage at an unaffiliated custodian. Until the SEC clarifies that a blockchain itself can be a custodian (which it should), investment managers will need to engage digital asset custodians. Many firms are currently building institutional-quality custody platforms, but all of them currently suffer from the lack of an ideal regulatory path—they’re pursuing a state-by-state licensing strategy. Well, Wyoming’s bill would solve that. Banks can do business in all 50 states and have other advantages as well.
- For investors: Provide an opt-in regime for enhanced supervision, which means Wyoming’s digital asset custodians can choose to opt-into a higher standard that would provide some very basic investor protections that don’t really exist in the industry (including custody as bailment rather than as an IOU). Other investor protections include the 3 D’s—define, disclose, delegate. Custodians must *define* which version of source code they’re running (“bitcoin is a digital asset” won’t cut it as a contractual definition for big institutional investors). All gains from client assets belong to the client, unless expressly *disclosed* otherwise and the client agreed. Customers must *delegate* authority to custodians before custodians can take action on anything. Most exchanges/custodians today aren’t set up to comply with the 3 D’s but will need to be ready to before providing services to the “fiduciary investment manager” market segment.
- For Wyoming: bring JOBS and REVENUE to the State.
- For everyone: Enable the peer-to-peer nature of the technology. As one example, the bill enables a smart contract to take custody of a digital asset—smoothing the legal path to responsible financialization of Ethereum and—as soon as trustless lending becomes possible—Bitcoin too.

I’ll close with my favorite reaction to the Wyoming news, posted by Donald McIntyre on Twitter. If SF 125 and the other proposed bills—including a special-purpose financial institution, a fintech sandbox, Wyoming’s Secretary of State integrating with

a blockchain, recognition of tokenized securities and a chancery court to litigate business disputes—all become law, I believe the answer to Donald's question will become obvious. Stay tuned—the news should be out by late February!



Donald McIntyre ⚡
@TokenHash

Following

Replying to @CaitlinLong_ @Tyler_Lindholm and 3 others

Is Wyoming to crypto what Delaware is to corporate law?

Links

- <https://twitter.com/tracemayer/status/934672438385954818?lang=en>
- <https://blog.kraken.com/post/300/kraken-passes-worlds-first-cryptographic-proof-of/>
- <https://www.forbes.com/sites/caitlinlong/2018/07/31/is-financialization-a-double-edged-sword-for-bitcoin-and-cryptocurrencies/#3flcefd2a20>
- <https://www.forbes.com/sites/caitlinlong/2018/08/03/ice-creating-new-cryptocurrency-market-a-double-edged-sword/#3fdd63d61015>
- <https://www.forbes.com/sites/caitlinlong/2018/08/07/racing-to-fix-wall-street-ice-cryptocurrencies-and-enterprise-blockchain/#698e1e7d215e>
- <https://www.forbes.com/sites/caitlinlong/2018/08/13/the-r-and-c-words-enter-the-vocabulary-of-bitcoin-enthusiasts/#650ea60368f3>
- https://www.forbes.com/sites/darrynpollock/2019/01/18/wyoming-introduces-bill-offering-cryptocurrencies-legal-clarity-to-attract-blockchain-business/?ss=crypto-blockchain&utm_source=TWITTER&utm_medium=social&utm_content=2087367833&utm_campaign=sprinklrForbesCrypto#1d2d4ef746d5
- <https://www.wyoleg.gov/Legislation/2019/SF0125>
- <https://www.usv.com/post/531eec41c4072a1e3a04f7cc/is-the-ucc-the-achilles-heel-of-bitcoin>

Quantum Narratives

The rise and fall of crypto narratives

By [Dan Held](#)

Posted January 22, 2019

Quantum Superposition

If you like audiobooks, I've done a voiceover of this article which is available to listen to on [Soundcloud](#) and [YouTube](#).

In 1935, scientists wrote an article called “The [EPR](#) Paradox” which described the strange situation of quantum superpositions, in which systems can exist in multiple states corresponding to different outcomes simultaneously. In effect, the paper argued that there wasn’t only one but in fact multiple “true” realities. Each of these realities would remain valid until they were interacted with or observed by the external world. At that time, the superposition collapses into one of the possible states.

To better visualize this idea, Austrian physicist Erwin Schrödinger proposed a [thought experiment](#) that would eventually become ingrained in our culture. Imagine a cat in a box with a flask of poison, a radioactive material, and a monitor that will smash the flask and release the poison if a single atom decays. After a while, quantum theory dictates that the cat is simultaneously dead and alive at the same time. It is only once we open the box to observe the cat to be either dead or alive that the multiple states cease to be simultaneously true. It is our actions that determine, ultimately, which reality prevails.

(The above and below section was largely borrowed from @nlw’s [article](#) titled “Schrödinger’s Securities: Regulation & The Quantum State Of Crypto”)

Narratives

Nobody can know everything. [The complexity of society is irreducible](#). We cling to [mental models](#) that satisfy our thirst for understanding a given phenomenon, and stick to groups who identify with similar narratives.

Beliefs are not only shaped by reality; narratives define it. In any social arena, there’s a never-ending battle to tell what’s happening, why is it happening, and what is happening next. Controlling narratives is particularly powerful. These narratives constitute the fabric of the world around us: government, religion, culture, and

finance all exist simply because we believe in it (and provides value for those who believe in it).

Investors invest in or against narratives; builders build directionally towards narratives; commentators race to associate themselves with the dominant narratives or, alternatively, to be the contrarian positioning against the conventional wisdom.

Market narratives are marketing. The incentives to push a narrative can be financial, like an investor sharing a view of the world that would just so happen to benefit them if more people were to agree with them and invest accordingly. In this way, narratives are attempts at self-fulfilling prophecy. Incentives can also be even simpler, however, such as the desire for status and community relevance.

The fact that narratives are marketing is not a bad or malicious thing. Indeed, there is value in an emerging industry enabling a space where people can discuss narratives they see trending.

This is especially true in the crypto space, in which content from investors and builders today has an [outsized](#) influence on market sentiment relative to neutral third-party research firms or data-driven journalism. Again, this is not in and of itself a problem. It is a good thing to get live insights into how operators see things. Moreover, the independent, data-driven research/journalist side of the market is catching up quickly which is accelerating the critical analysis of these narratives.

Cambrian Explosion of Crypto Narratives

During the Cambrian explosion more than half a billion years ago, the variety of life on Earth burgeoned dramatically. While most species that came about eventually went extinct in a series of mass extinction events, we still have this relatively short period of profligate experimentation to thank for the variety of life we experience around us now. In other words, the [truly bizarre](#) creatures that roamed the planet then were side-effects of Nature showing off its capacity for variegated expression of lifeforms, before settling into a somewhat more sensible pattern.

In an [analogous](#) vein, the dotcom bubble was an extinction event that wiped out exuberant companies, but fundamentally sound ideas survived, a large variety of which are to be found today (ex: Amazon).

In the crypto world, we have WhopperCoins, Putincoins, Bitcoin Cash, Bitconnect, and a string of other tokens/cryptocurrencies that were created during the last bubble. In the long-run, many shall die out—much like the numerous [species](#) that kicked the bucket at the end of the Cambrian explosion. Only the fittest shall survive.

“Jostling for narratives can be seen as an evolutionary battle to compose the doctrines most likely to attract the next wave of adherents. Coin prices amplify this mess. Market cycles—especially up-cycles—appear to pick winning narratives, leading to sudden increases in [evangelism](#) and waves of new adherents. And when the market swings the other way, a new narrative gains steam and steals adherents.” — [Tony Sheng](#)

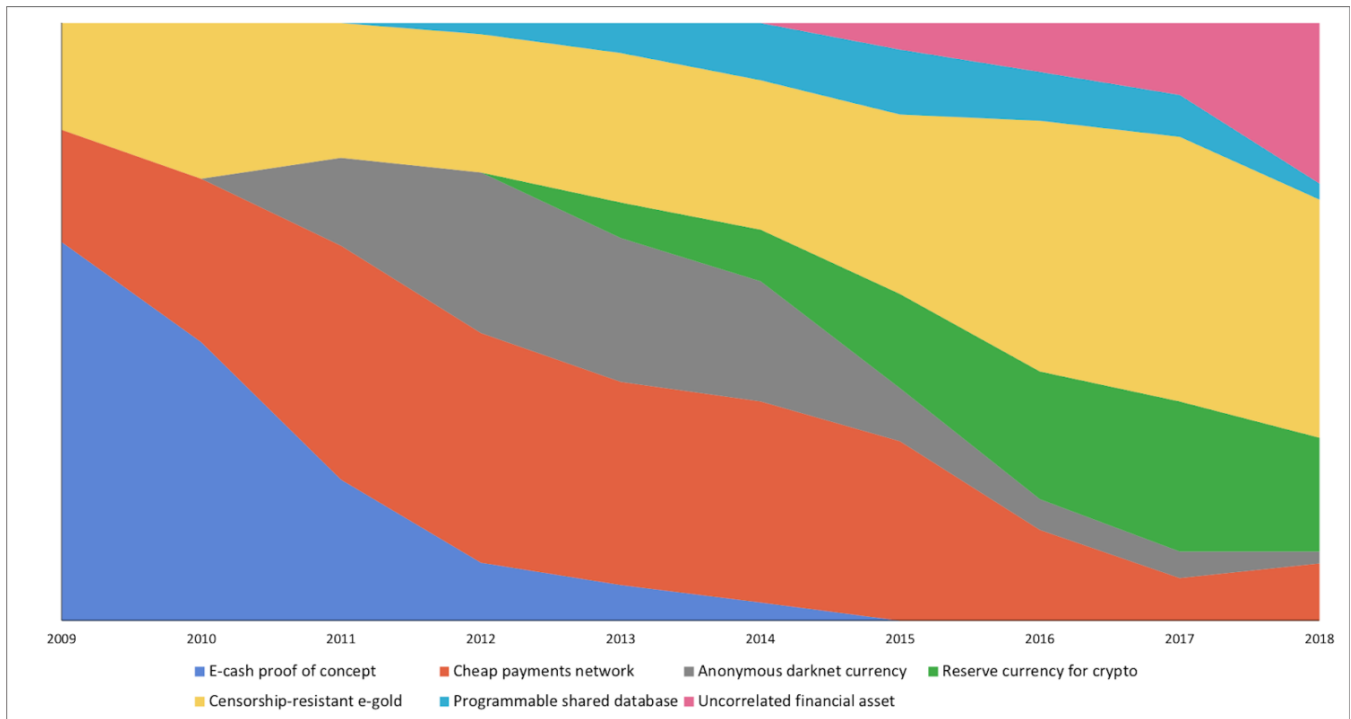
Which crypto narratives are gaining steam tomorrow? How will that change next month or year (or 10)? What are prospective catalysts that could change the dominant narratives of today? How does this differ globally?

Bitcoin and Ethereum, the two most popular cryptocurrencies, have had many narratives fade in and out of popularity over the years. In the below sections are two charts which visualize the ebb and flow of these different narratives for both cryptocurrencies.

Before you read further, I must note an important differentiation. Bitcoin’s narrative of SoV/Gold 2.0 was [present](#) from day one, has Protocol Market Fit (PMF), has held off competing narratives, has been delivered on, and remains the dominant narrative today. There is persistence of the original intent.

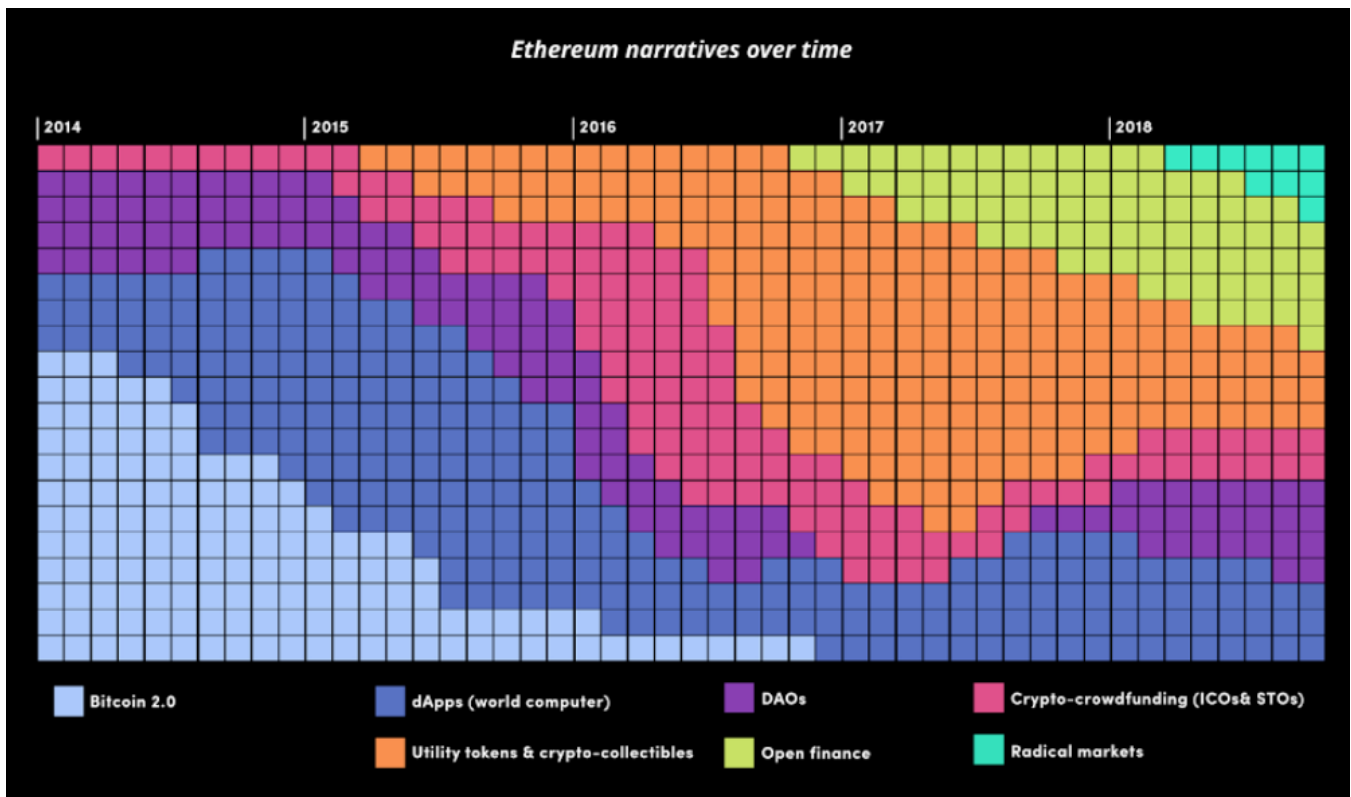
While the Ethereum community has endorsed radical changes/pivots, trying to find narrative fit (PMF), even so far as to recently [claim](#) a SoV narrative. The Ethereum leadership team is more willing to embrace alternations to the core objective of the protocol in their search for PMF (world computer, dapps, crowdfunding, nonfungibles, open finance, radical markets).

Bitcoin Narratives



https://medium.com/@nic_carter/visions-of-bitcoin-4b7b7cbcd24c

Ethereum Narratives



<https://tokeneconomy.co/visions-of-ether-590858bf848e>

Only the antifragile narratives will survive

When something is “antifragile” it gains strength as a result of volatility, stressors, or shocks (originally coined by [Nassim Nicholas Taleb](#))

“Every criticism Bitcoin survives makes it stronger.”—[Jimmy Song](#)

Crypto-communities seek for newish narratives or adapt current ones as an exercise of collective strengthening. They also do so to combat critique by isolating some of its premises. **Since there is no objectively correct monetary premium, promoting the superior attributes of a monetary good is more effective than for regular goods, whose value is ultimately anchored to cash flow or use-demand.** The religious fervor of participants in the Bitcoin market can be observed in various online forums where owners actively promote the benefits of Bitcoin and the wealth that can be made by investing in it. In observing the Bitcoin market, [Leigh Drogen](#) [comments](#):

“You recognize this as a religion—a story we all tell each other and agree upon. Religion is the adoption curve we ought to be thinking about. It’s almost perfect—as soon as someone gets in, they tell everyone and go out evangelizing. Then their friends get in and they start evangelizing.

While the comparison to religion may give Bitcoin an aura of irrational faith, **it is entirely rational for the individual owner to evangelize for a superior monetary good and for society as a whole to standardize on it.** Money acts as the foundation for all trade and savings, so the adoption of a superior form of money has **tremendous multiplicative benefits to wealth creation for all members of a society.**”

Fiat currency, similarly, is faith based. Per wikipedia:

“Fiat money is a currency **without intrinsic value** that has been established as money, often by government regulation. Fiat money does not have use value, and has value only because a government maintains its value, or **because parties engaging in exchange agree on its value.**”

US dollars reinforce the faith with “In God We Trust”

“Gold’s simplicity is a great feature. But Bitcoin is likewise the simplest cryptocurrency. You can [explain the intuitions behind Bitcoin](#) to any captive high schooler who has a basic grasp of probability and a moderate attention span. To the digital native of the future, Bitcoin wallets will probably seem more natural than vaults full of useless metals painstakingly drilled out of the earth.”—[Haseeb Qureshi](#)

“Stable ideologies allow communities to thrive. A simple example in religion is the Christian tenet that “there is one true god”. This belief strengthens the religion because it weakens membership in competing religions. Communities with unstable ideologies will eventually collapse. **The very ideology that justifies the existence of Bitcoin Cash, also justifies the use of chain splits to settle any disagreements within the community. It’s easy to see that this ideology, that a hard forked minority chain can be a legitimate successor to the original chain, is completely unstable.** It is thus reasonable to conclude that Bitcoin Cash will face a never-ending threat where its community members threaten to split off permanently from the main chain.” — [Kay Kurokawa](#)

This was prophetic. Due to fragmented ideology, Bitcoin Cash (also known as the altcoin “bcash”) ultimately split into two chains late last year and the price collapsed.

Wave Function Collapse

In quantum mechanics, “wave function collapse” occurs when the superposition of several states appears to reduce to a single state due to interaction with the external world; this is called an “observation.” Narratives can persist in the multiple states for quite some time, until the moment when it comes under critical observation.

Narrative wave function collapses only when we believe that everyone else believes the critical observation (common knowledge). That’s what changes behavior. And when that transition to common knowledge happens, behavior changes fast.

The classic example of this is the fable of The Emperor’s New Clothes. Two weavers who promise an [emperor](#) a new suit of clothes that they say is invisible to those who are unfit for their positions, stupid, or incompetent—while in reality, they make no clothes at all, making everyone believe the clothes are invisible to them. When the emperor parades before his subjects in his new “clothes”, no one dares to say that they do not see any suit of clothes on him for fear that they will be seen as stupid. The only thing that changes behavior is when the little girl announces the Emperor’s nudity loudly enough so that the entire crowd believes that everyone else in the crowd heard the news. That’s when behavior changes. There’s a lot of ubiquitous

private information about powerful ideas trapped in the crowd today, just waiting for a someone to release it as [common knowledge](#).—Ben Hunt

What we are observing now in the crypto bear market is the collapse of the narrative wave function from critical observations making knowledge common, ultimately manifested as price.

Some narratives are unraveling. Narratives that conflict will reconcile (ex: utility vs SoV theory of money). Which ones will remain? Which ones will survive? As we've seen in previous crypto market cycles, only the most antifragile will endure.

Links

- https://en.wikipedia.org/wiki/EPR_paradox
- https://en.wikipedia.org/wiki/Schr%C3%B6dinger%27s_cat
- <https://hackernoon.com/schr%C3%B6dingers-securities-regulation-the-quantum-state-of-crypto-ffb4e5b7446>
- <https://www.econlib.org/library/Essays/hykKnw.html>
- <https://fs.blog/mental-models/>
- <https://tokeneconomy.co/market-narratives-are-marketing-introducing-the-crypto-narrative-index-deeeb49bc909>
- <https://www.nationalgeographic.com/science/phenomena/2013/02/18/weird-youth-animal-kingdom/>
- <https://blog.goodaudience.com/bitcoin-as-exit-bitcoin-as-voice-c3d4520e201e>
- <https://www.danheld.com/blog/2019/1/6/planting-bitcoinspecies-14>
- <https://www.tonysheng.com/mass-movement>
- <https://medium.com/u/be4506861043>
- <https://twitter.com/danheld/status/1084848063947071488>
- <https://github.com/ethereum/EIPs/issues/960>
- https://medium.com/@nic_carter/visions-of-bitcoin-4b7b7cbcd24c
- <https://tokeneconomy.co/visions-of-ether-590858bf848e>
- <https://medium.com/u/f138bf5466fe>
- <https://medium.com/u/4acb12744ff8>
- <https://www.cnbc.com/2017/10/19/josh-brown-goes-down-the-bitcoin-rabbit-hole-commentary.html>
- <https://www.youtube.com/watch?v=bBC-nXj3Ng4>
- <https://medium.com/u/8bc4e5f8b505>
- <https://medium.com/u/731e1423e587>
- <https://en.wikipedia.org/wiki/Emperor>
- <https://www.epsilontheory.com/harvey-weinstein-common-knowledge-game/>

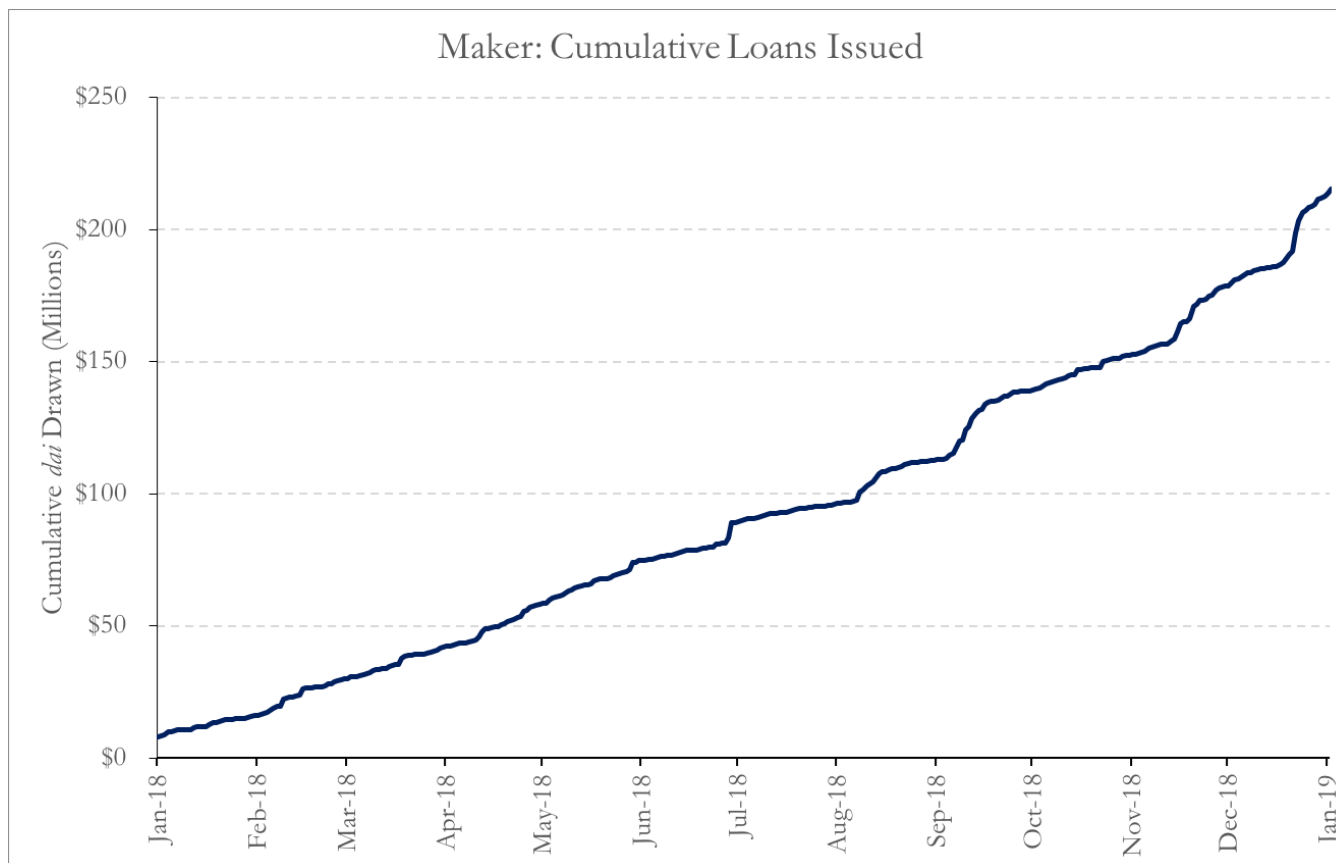
Maker Investment Thesis

By [Chris Burniske](#) and [Joel Monegro](#)

Posted January 23, 2019

Credit has greased economic wheels for millennia, and [Maker](#) is the world's first 100% software-based, community owned and operated credit facility. As a family of smart contracts operating on Ethereum, the system offers secured loans of equal cost to anyone in the world. The by-product of loan generation is *dai*, a stablecoin collateralized using on-chain rules and assets.

In its first year, Maker issued roughly \$200 million in loans, with [over \\$70 million](#) currently outstanding (Figure 1). For some perspective, it took Lending Club five years to originate \$250 million in loans [1].



Data from [Digital Asset Research \(DAR\)](#)

To get a loan, borrowers first lock ETH through an Ethereum transaction [2], creating a *collateralized debt position* (CDP). They are then able to issue themselves a dai-denominated loan against the posted collateral. The maximum amount of dai that

users can issue themselves depends on the loan parameters set by [MKR](#) holders. Currently, the loan must remain under 2/3 the value of the locked collateral (i.e., \$3 of collateral allows for \$2 of dai to be issued to the borrower). The newly-created dai can then be exchanged for any of the assets [it trades against](#) (including BTC, ETH, USDC and USDT), which can be used to purchase other goods and services.

If the borrower's collateral drops in value such that the loan outstanding becomes greater than 2/3 the value of the collateral (that is, if the loan becomes less than 150% collateralized [3]), then some of the borrower's collateral is automatically sold to repurchase dai and partially pay down the loan. Self-interested agents called *keepers* do the work of enforcing this [liquidation ratio](#), and in some months have made [\\$200-300K](#) in nearly risk-free profit from their efforts. The supply of dai expands as users create loans, and contracts as loans are paid down or liquidated.

Having principal at risk incentivizes borrowers to be responsible about their debts. Proper risk management combined with a lean protocol as the facilitator, instead of a profit-seeking company, leads to a lower cost of credit for all. The cost of a loan has ranged from 0.5% - 2.5% per year (called a *stability fee*), placing Maker's credit facility at [1/10th](#) the cost of secured loans offered by traditional financial institutions [4].

The stability fee must be paid with the second cryptoasset of the system, MKR, which is subsequently destroyed, making it a deflationary asset from its starting supply of 1,000,000 units. The more loans that are created and redeemed, the more MKR's supply will deflate. This burning mechanism helps create token value similar to how equity buy-back programs can drive share prices in traditional companies.

But MKR holders don't get something for nothing: they must govern the system by [voting](#) for the parameters around loans, such as collateralization ratios, types, and fees. While they stand to benefit from a MKR supply that deflates as loans are redeemed, they also stand to lose if any loan becomes undercollateralized. Should collateral values fall such that not enough value is left to cover the loan (i.e., the loan is less than 103% collateralized), then new MKR would automatically be created and sold in order to buy back dai and pay down the toxic loan. MKR holders would then be diluted for having set parameters that allowed for such an event to occur.

The permissionless creation and circulation of dai positions it as an important unit of account within other decentralized finance applications. It is already being used by a rich ecosystem of centralized and decentralized applications, such as [Ripio](#), [Wyre](#), [Compound](#) and [Nexo](#), with many more integrations in the works.

While there are valid concerns about the dangers of "permissionless credit creation," MakerDAO's *auditable code & collateral* and *direct consequences for operators* solves two [principal-agent problems](#) that have historically plagued the behavior of credit facilities.

First, credit facilities consistently run into trust issues due to the (relative) opacity of their operations and centrally held collateral. By contrast, if anyone is suspicious of Maker's integrity, they can inspect all code (operations) and collateral of the system, anytime, anywhere. Transparency enables remediation before a crisis in confidence, making for a more resilient system.

Second, direct consequences for operators and holders of MKR disincentivize risky management. As we witnessed in the 2008 Financial Crisis, many of the actors that enabled an over-extension of credit were not directly punished for their actions, and many were even able to extract [billions in bonuses](#) from the government bailouts. In Maker, if the system fails, all capital holders are diluted equally, with no room to walk away enriched.

Maker's open, low-fee service provides fair access to credit for everyone. Today, such access is only available to those already in the best financial position, while the rest are subject to wealth-eroding, high fee loans. Maker's solution serves crypto-geeks and investors right now, but we believe is a critical step towards a more equal economic opportunity future.

Footnotes:

1. In a future report, we'll share a full set of stats on Maker adoption. Some may object to the LendingClub comparison, which we agree is not apples to apples, but we provide it for perspective nonetheless.
2. While ETH is currently the only collateral accepted, Maker is moving to a [multi-collateral](#) model soon.
3. Some will complain that a 150% collateralization requirement is capital inefficient and will impede Maker's broader adoption. As the volatility of cryptoassets drop, and more kinds of collateral can be used, the volatility of the value securing the loans will drop as well, allowing more capital efficient parameters to be set. Beyond these simple mechanics, the Maker team has a variety of other ideas for how to make the system more capital efficient over time. Right now, as one of the few venues where cryptoassets can be used as collateral for loans, Maker is not focused on optimizing, but instead enabling.
4. As mentioned in Footnote 3, Maker loans are currently over-collateralized, which is a cost due to the time value of money. The other cost to keep in mind is if a loan becomes under-collateralized, the liquidation process incurs a 13% liquidation penalty.

Links

- <https://makerdao.com/en/>
- <https://coinmarketcap.com/currencies/dai/>
- <https://www.digitalassetresearch.com/>

- <https://coinmarketcap.com/currencies/maker/>
- <https://coinmarketcap.com/currencies/dai/#markets>
- https://www.reddit.com/r/MakerDAO/comments/8efk5q/faq_possibly_everything_you_ever_wanted_to_know/
- <https://medium.com/@mikeraymcdonald/single-collateral-dai-9-months-in-review-b9d9fbe45ab>
- <https://www.nerdwallet.com/blog/loans/secured-personal-loans-lenders/>
- <https://vote.makerdao.com/>
- <https://medium.com/makerdao/makerdao-partners-with-ripio-to-bring-dai-to-south-america-via-fiat-on-off-ramp-e22ac71a210d>
- <https://medium.com/makerdao/makerdao-and-wyre-give-businesses-immediate-access-to-dai-stablecoin-in-over-thirty-countries-4fe94957c730>
- <https://app.compound.finance/?fbclid=IwAR1yBqcpanBEP58-ZR-XVCw7Amp7W4oxYfQSDB7lbldRpCZBLNQba9xvdOs#Markets>
- <https://medium.com/nexo/earn-interest-and-protect-your-stablecoins-with-nexos-1-to-1-conversion-guarantee-dbdefa8a8152>
- <https://www.investopedia.com/terms/p/principal-agent-problem.asp>
- <https://www.nytimes.com/2009/07/31/business/31pay.html>
- <https://medium.com/makerdao/the-road-to-mainnet-release-21931d47f857>

Grin and the Mythical Fair Launch

By [Arjun Balaji](#) and [Hasu](#)

Posted January 25, 2019

Grading Grin among a sea of cryptocurrency distribution models

When Grin launched in early January after years of anticipation, it faced material pushback from prominent Bitcoiners who labeled it a “VC coin” and compared it to offerings from the 2016/18 ICO era. We think that criticism is unjustified as Grin’s launch was one of the fairest launches ever, if not the fairest.

What constitutes a fair launch?

Philosophers have debated questions of fairness for thousands of years, so we won’t pretend to have any new insight there. Instead, we will focus our analysis on what criteria for a fair launch have emerged over the short history of private currency markets.

The foundational principle we observe is that a fair launch offers equal opportunity—not equal outcome—to acquire a coin 1) over a long period of time 2) at a relatively equal price. This can be broken down across two dimensions: length of issuance and price equality.

1 - Length of Issuance

A lengthy issuance schedule is important to give the market ample time to become aware of the project and discover a fair price. When 100% of the token supply is sold in a single 1-month time span, did the market really have a chance for proper price discovery for each of the tokens? On the other end of the spectrum, we find issuance schedules that are stretched out over decades. Here, the market has a good chance to absorb the supply and discover a fair price.

2 - Price equality

The second dimension, price equality, proposes that there is no group or person that can acquire the token at a sizable discount to the market price. Zcash and Beam both have a timelocked pre-mine (the founder’s reward), that was partially sold to accredited venture investors. With Dfinity (and many other ICOs), early investors paid 1/100 or less than later investors in the public offering. It can be argued that these discounts are justified because these investors lend needed credibility to projects and accept longer lockup/illiquidity periods than public investors. Whether the market agrees with this argument remains to be seen.

Our aim isn't to provide a normative view of what projects should or shouldn't do, it is simply to describe market realities around perceptions of fairness. The argument that venture investors take on material risk, including whether or not the project will launch, is trivially true. In our view, the longer a project remains illiquid to pre-sale backers, the more any discount offered is "earned", as this can be thought of as the investors' own proof of work.

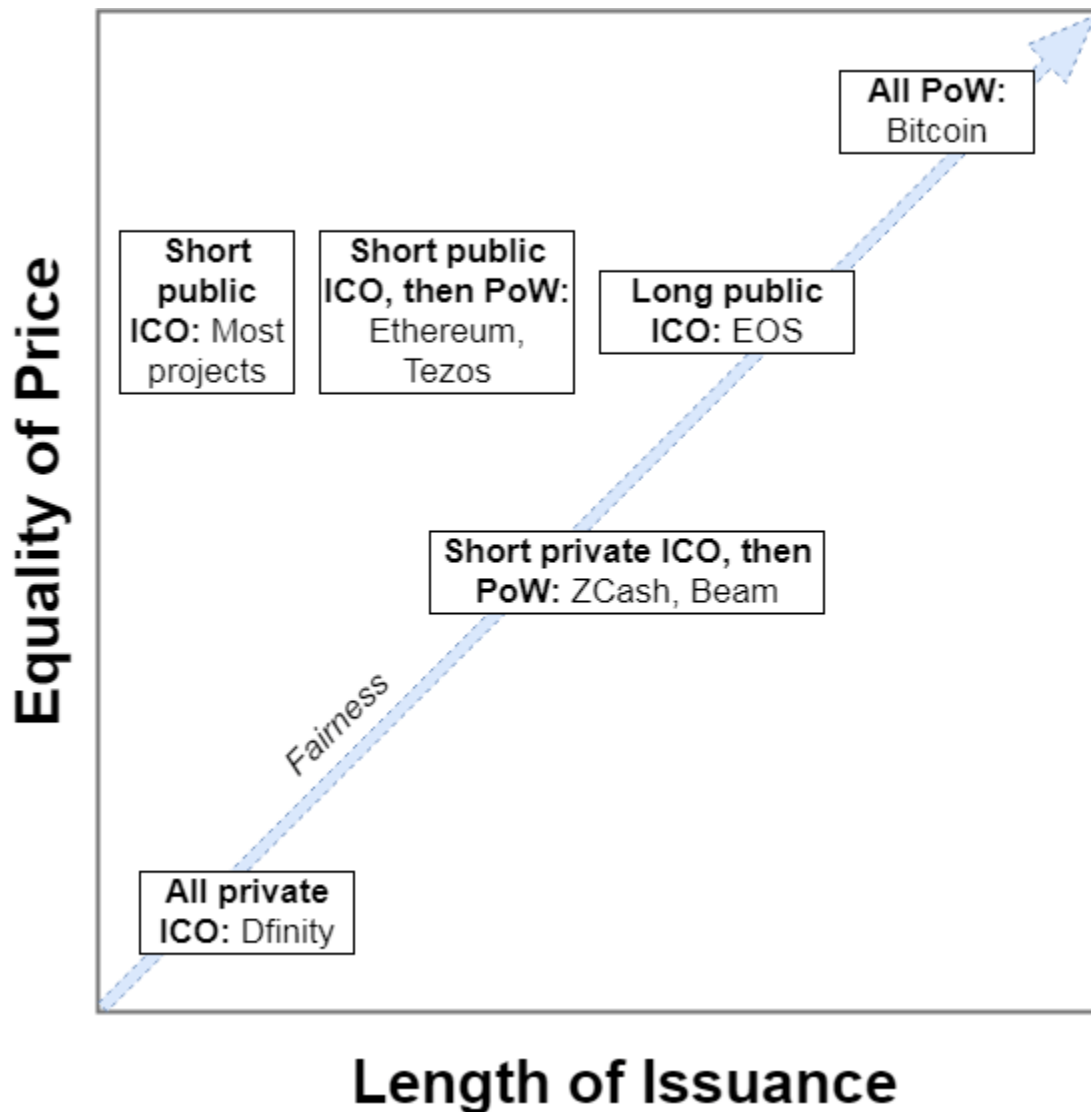
Venture investors accessing a pre-sale is distinct from the notion of pre-mines or allocated coins. While we believe pre-mined coins suffer from issues of price discovery, they are not inherently bad for price equality.

Comparing ICOs and PoW

ICOs are generally fairer the longer they are open. The EOS ICO, although unjustly criticized by the market, was the fairest to date because it took over a year. This continuous ICO functioned similarly to proof of work, auctioning coins to the market on a daily basis, giving the market ample time to become aware of the offering and its details and allowed finely grained price discovery to happen in secondary markets.

Expanding on this idea, proof of work can be seen as a perpetual ICO where every day, a fixed number of coins are auctioned on the market and the proceeds are burned. When discussing fairness, proof of work is sometimes criticized due to the power law winners that emerge via economies of scale, but this argument is easily debunked. Large-scale mining operations operate in a highly competitive environment that ensures that coins are immediately delivered to the secondary market as they become available, as miners need to sell to replenish their liquidity. There, millions of participants have the opportunity to purchase these coins while miners are left with a small margin (or even without a margin at all in many cases). **The more competitive mining is, the more it feels like coins are directly issued to the secondary market itself.**

Across these two dimensions, time and price, we can graph different distribution models that we have seen so far.



As ICOs and pre-mined coins often sell a large portion of their token supply in a short time window (unequal opportunity to buy across time) and are known to give some investors large discounts over others (unequal price) they are deemed more unfair by the market on both dimensions. Projects that bootstrap initial financing entirely in private and maintain a large ownership stake in the project, [such as Dfinity](#), are on the extreme end of the “unfairness” scale.

Grading Grin’s launch

So where does Grin rank? Let’s look at the properties of their launch:

- The project was highly transparent. The specs of the project, including its technical features, monetary policy, etc. were all known well in advance, giving the market ample time to become aware of them.

- The hashing algorithm(s) used in Grin's PoW were also known and discourse around this crucial decision happened in [the project's public forums](#). In order to ensure that the offering was open to as many participants as possible, [the community converged](#) on offering a dual-PoW system over the first 2y, with one hashing algorithm targeting generalized hardware and the other allowing for specialized optimizations (via ASIC). This was a pragmatic choice, the development of ASICs on the Grin network was seen as inevitable. However, rather than privilege vertically integrated miners who can develop ASICs prior to launch, the team chose to gradually scale up the portion of coins allocated to the ASIC-friendly hashing algorithm over 2y, allowing small-scale hobbyist miners to participate.
- The total supply is auctioned over a long period of time, which ensures proper price discovery across the full issuance schedule. Grin's tail issuance, while not as strict as Bitcoin's hard cap, allows for continual participation forever.

Arguments against Grin

There are primarily two arguments made against the Grin launch by Bitcoiners.

The first argument is that much of the initial hash rate was provided by mining operations which were predominantly funded by venture capital dollars and that this is somehow indistinguishable from a pre-mined offering. This argument is a red herring—our previous explorations have shown that the **more** competitive a mining market is, the fairer the distribution will be perceived, as competition guarantees that coins are delivered to the market at the smallest possible margin. Venture investors are speculators like any other and when investing in miners, they're rewarded proportionally for the risk they take on around operational execution and market reception.

The second argument is that there was a lot of attention on the Grin launch, while Bitcoin's launch happened with few eyeballs. We think this argument, that a launch can no longer be fair because more people are interested in it, is irreconcilable with a free market view. In fact, we argue the opposite: **a launch is fairer the more potential buyers are aware that a project exists.** This cannot be held against Bitcoin as the number of people interested in non-sovereign money at the time was admittedly limited to a small group of participants on a cypherpunk mailing list. However, if you launch a project silently today, many would see it as an act of deception no different than giving some set of investors unequal opportunity (access) over others.

Conclusion

In the spirit of free-market competition between monies, we believe all distribution models are generally fine. A distribution model's theoretical "fairness" is divorced from questions about whether the project works as advertised. All cryptocurrency

projects are nascent experiments with varying degrees of success. Assuming a reasonable level of market efficiency, full access to transparent information—allowing market participants to discern between reality and fiction—matters even more than the perceived accuracy of a project’s claims. Discerning whether an ambitious project’s vision is misleading or naive is a problem better left to the market and is orthogonal to the fairness of the distribution model.

In conclusion, we argue that fairness of launch or distribution is evaluated by the market on two dimensions: **a lengthy issuance—so the market can discover a fair price for each token—and price equality, so no one can buy a token below this fair market price.** Grin’s launch excels in both dimensions. While the concept of “fairness” is ultimately subjective and a “perfectly fair” launch a pipe dream, these are the factors the market currently considers most relevant.

Links

- <https://uncommoncore.co/>
- <https://twitter.com/arjunblj>
- <https://twitter.com/hasufl>
- <https://medium.com/r/?url=https%3A%2F%2Ftwitter.com%2FICODrops%2Fstatus%2F976104225796214786>
- <https://medium.com/r/?url=https%3A%2F%2Fwww.grin-forum.org%2Fc%2Fmining>
- <https://medium.com/r/?url=https%3A%2F%2Fwww.grin-forum.org%2Ft%2Fchoice-of-asic-resistant-pow-for-gpu-miners%2F1017>

Money, Bitcoin and Time: Part 1 of 3

By [Robert Breedlove](#)

Posted January 20, 2019

A synthesis of perspectives from many prolific thinkers, this 3-part essay will cover the following topics in sequence:

- *Money — its properties, story and evolutionary history*
- *Bitcoin — its nature and significance in the story of money (see [PART 2](#))*
- *Time — perspectives on its value and how the story of money might play out (see [PART 3](#))*

This essay is guided, inspired and adapted from the literary works of many. Each section header will include a number [n] referencing relevant synthesized works at the end of each part. For those seeking further elucidation on any of the topics discussed herein, I highly encourage you to read these original works.

This essay is also available in .pdf form at:

<https://www.parallaxdigital.io/blog>

Please feel free to send any questions or feedback to

info@parallaxdigital.io

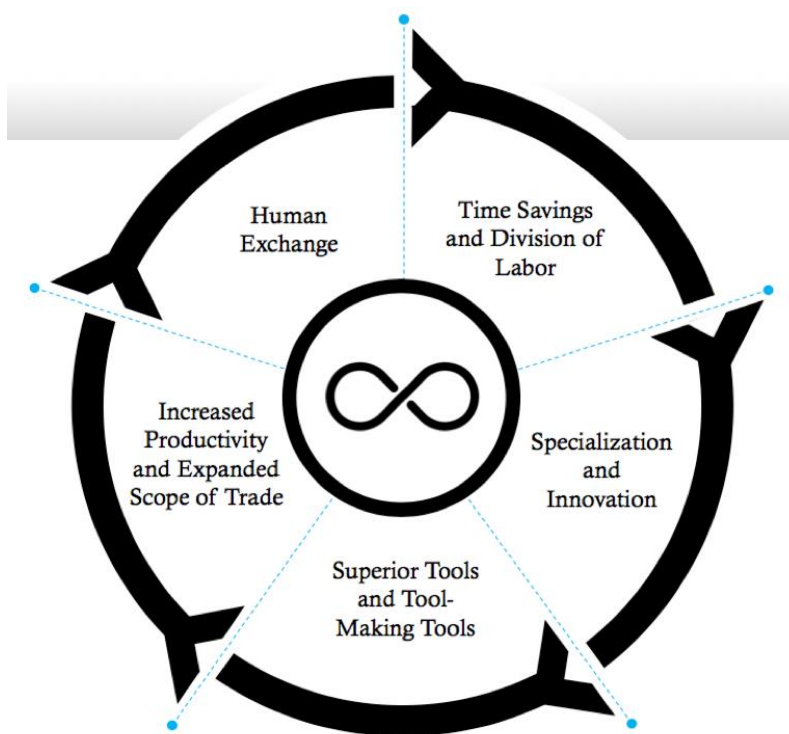
The Simple Truth about Money: Money is the most successful story ever told by humans. It is a reflexive narrative: meaning it has value only because everyone believes it, and everyone believes it because it has value. Money is a story that continues to be written...

Human Exchange [2,6]

Human beings are the networked species. Initially, these were small bands of hunters and gatherers numbering no more than 150 persons strong (Dunbar's number). When humans began to exchange with one another, they intuitively discovered the *division of labor* which allows people to focus on their relative advantages and concentrate on their chosen craft. The division of labor enables the *specialization* of productive efforts for mutual gain. If John makes axes faster than Steve, and Steve makes bows faster than John, then they both are better off by specializing and

trading. Interestingly, this holds true even if John is faster than Steve at making axes and bows (up to a point) and, amazingly, this effect compounds.

Tools, or technologies, are mechanisms that increase *productivity* by amplifying the returns on human time directed at production. You can chop more wood per man hour using an axe than you can with your bare hands. As people made and exchanged more tools, time savings increased and specialization deepened. Specialization sparked innovation, because it encouraged the investment of time in tool-making tools, such as whetstones used for making sharper axes. This enabled people to create superior tools, which increased productivity even further. That saved more time, which people used to specialize even further and expand their *scope of trade* by exchanging with an even greater number and variety of people, which increased the division of labor even further, and so on. This recursive dynamic persists to this day as a virtuous cycle with no known natural limit—modern markets in goods, services and ideas allow human beings to exchange and specialize honestly for the betterment of all. In this way, the act of exchange is the incipient force driving all human progress and *prosperity*. Prosperity is simply time saved, which is proportional to the division of labor:



Human exchange is the incipient force driving all human progress and prosperity. Prosperity is simply time saved, which is proportional to the division of labor. This recursive dynamic persists to this day as a virtuous cycle with no known natural limit — modern markets in

goods, services and ideas allow human beings to exchange and specialize honestly for the betterment of all.

Human exchange is to cultural evolution what sex is to biological evolution. By exchanging and specializing, innovations come into existence and spread. At some point, human intelligence became collective and cumulative in a way that happened to no other animal. Language, and later writing, allowed us to pass our collective learnings to each successive generation. Written language allowed us to manifest and share our belief systems. As the only animal that can tell and believe stories, we learned to organize ourselves using abstractions such as money, mathematics, nations and corporations. Our unique ability to tell and believe stories—as free market capitalists, human rights activists, national citizens or whatever story we accord with—enables us to cooperate flexibly in large numbers and across genetic boundaries. This scale of collaboration, never attained by any other animal before or since, is the reason mankind came to dominate the Earth. We are the networked species, fully interconnected by our acts of exchange. A spontaneous emergent property of these complex human interactions is money, which solved problems inherent to trade and accelerated the rate of human exchange and the division of labor. Money, as the vital lubricant for human exchange, was among the first stories we used to collectively organize ourselves.

Story of Money [1]

Let's begin with first principles and follow logic from there. The simplest form of human exchange is the direct trading of actual goods, say guns for boats, in a process known as *direct exchange* or barter. Direct exchange is only practical when few people are trading few goods. In larger groups of people, there are more opportunities for individuals to specialize in production and trade with more people, which increases the aggregate wealth for everyone. This simple fact, that exchange enables us to produce more goods per hour of human effort is the foundation of economics itself:

Economics is the social science of increasing production per unit of contribution.

Larger groups of people exchanging goods mean larger markets, but also creates a problem of *non-coincidence of wants* — what you are seeking to acquire by trade is produced by someone who doesn't want what you have to offer. This problem has three distinct dimensions:

- Non-coincidence in Scales—imagine trying to trade pencils for a house, you cannot acquire fractions of a house and the owner of the house may not need such a large amount of pencils
- Non-coincidence of Locations—imagine trying to trade a coal mine in one place for a factory in another location, unless by coincidence you are

- seeking a factory in that exact location and the counterparty you are dealing with is seeking a coal mine in that precise place, the deal will not be completed since factories and coal mines are not movable
- Non-coincidence in Time Frames—imagine trying to accumulate enough oranges to trade for a truck, since the oranges are perishable they would likely rot before the deal could be completed

The only way to resolve this three-dimensional problem is with *indirect exchange*, where you seek to find another person with a good desired by the counterparty and exchange your good for theirs only to, in turn, exchange it for the counterparty's good to complete the deal. The intermediary good used to complete the deal with the counterparty is called a *medium of exchange* – the first function of money. Over time, people tend to gradually converge on a single medium of exchange (or, at most, a few media of exchange) as it simplifies trade. A good that becomes widely accepted as a medium of exchange is commonly called money.

Money offers its users pure optionality, as it can be readily exchanged for any good available in the marketplace. In other words, money is the most liquid asset within a trade network. In this sense, money is said to have the highest *salability*, meaning the ease with which it can be sold on the market at any time with the least loss in price. Salability of a good is relatively determinable by how well it addresses the three dimensions of the non-coincidence of wants problem:

- Salability across Scales—a good that is easily subdivided into smaller units or grouped together in larger units, which allows the user to trade it in whatever quantity desired
- Salability across Space—a good that is easily transported or transmitted over distances
- Salability across Time—a good that can reliably hold its value into the future by being resistant to rot, corrosion, counterfeit, unpredictable increases in supply and other debasements of value

It is the third element, salability across time, that determines a good's utility as a *store of value*—the second function of money. Since the production of each new unit of a monetary good makes every other unit relatively less scarce, it dilutes the value of the existing units in a process known as *inflation*. Protecting value from confiscation via inflation is a critical feature of money, and money is critical to the existence of flourishing trade networks.

Hard Money [1]

Hard money is more trustworthy as a store of value precisely because it resists intentional debasements of its value by others and therefore maintains salability across time. The hardness of a monetary good, also known as its soundness, is

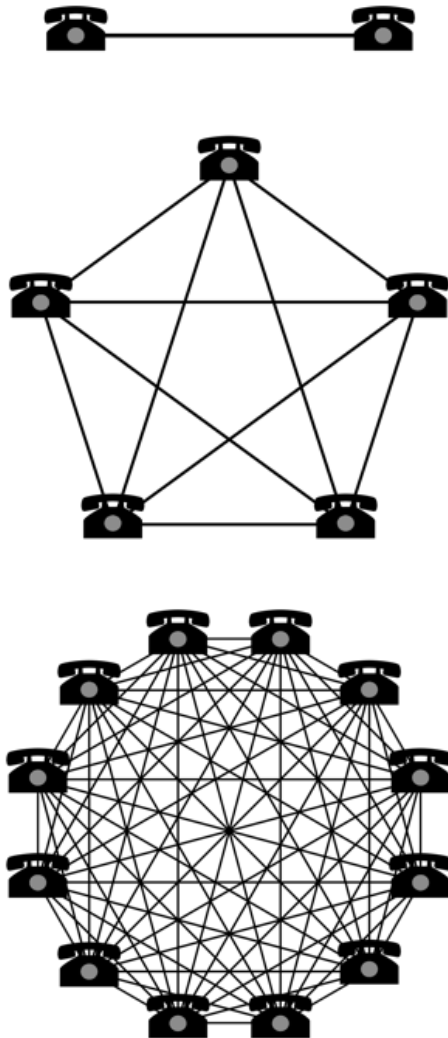
determined by the stock of its existing supply and the flow of its new supply. The ratio which quantifies the hardness of money is called the *stock-to-flow* ratio:

- 'Stock' is the existing supply of monetary units
- 'Flow' is the newly created supply over a specified time period, usually one year
- Dividing the stock of a monetary good by its flow equals its stock-to-flow ratio
- The higher the stock-to-flow ratio, the greater the hardness (or soundness) of money

The higher the stock-to-flow ratio, the more resistant the money is to having its value compromised by inflation. There are no correct choices as to forms of money, however there are consequences to what form a market naturally selects. If people choose to store their wealth in a monetary good which exhibits less hardness, then the producers of this monetary good are incentivized to produce more monetary units, which expropriates the wealth of existing unit holders and destroys the monetary good's salability across time. This is the fatal flaw of *soft money*: anything used as a store of value that can have its supply increased will have its supply increased, as producers seek to steal the value stored within the soft monetary units and store it in a harder form of money. As many historical examples in this essay will demonstrate, any monetary good which can have its supply cheaply and easily increased will rapidly destroy the wealth of those using it as a store of value.

For a good to assume a dominant monetary role within an economy, it must exhibit superior hardness with a higher stock-to-flow ratio than competing monetary goods. Otherwise, excessive unit production will destroy the wealth of savers and the incentives to use it as a store of value. Particular goods achieve monetary roles based on the interplay of people's decisions. It is from the chaos of complex human interactions that monetary orders emerge. Therefore, it is important to consider the social aspects of the spontaneous emergence of monetary orders.

Money is a Social Network [1,4]



Money, as a value system which connects people across space and time, is the original and largest social network. The value of a network is a reflection of the total number of possible connections it allows. Similar to the telephone and modern social media platforms, a monetary network becomes exponentially more valuable as more people join it because the number of possible connections it allows is proportional to the square of the number of its total network participants, a relationship defined by *Metcalf's Law*:

Network values are based on the number of possible connections they allow. Such values grow exponentially with the addition of each new constituent — a property commonly known as network effects.

In a monetary network, more possible connections mean more salability and a broader scope of trade. Participants in a monetary network are connected by their use of a common form of money to express and store value. *Network effects*, defined as the incremental benefit attained by adding a new member to a network for all existing members in that same network, encourage people to adopt a single form of money. Intuitively, a monetary good that

holds value across time (hard money) is always preferable to one that loses value (soft money). This causes people to naturally gravitate to the hardest form of money available to them. Further, since human exchange is a singular communal phenomenon suffering from a three-dimensional non-coincidence of wants problem, any monetary good that can solve all three dimensions of this problem will win the entire (or vast majority) of the market. For these reasons, a free market for money exhibits a *winner take all* (or, at least, a winner take most) *dynamic*. Network effects accelerate people's natural coalescence around a single monetary technology since larger monetary networks support higher salability of the monetary good involved. However, the selection of a monetary good is limited by the technological realities of the markets selecting. This can impede the winner take all dynamic, since particular monetary goods each satisfy the desirable traits of money to greater or lesser extents.

Monetary Traits [1,4]

As we will see, markets have naturally and spontaneously selected for the monetary good which best satisfies a variety of desirable traits that determine how useful a particular monetary good is as a form of money:

- Hardness—resistance to unpredictable supply increases and debasements of value
- Fungibility—units are interchangeable and indistinguishable from one another
- Portability—ease of transporting or transmitting monetary units across distances
- Durability—resistance of monetary units to rot, corrosion or deterioration of value
- Divisibility—ease of subdividing or grouping monetary units
- Security—resistance to counterfeiting or forgery
- Sovereignty—the source of its value, trust factors and permissions necessary to transact with it (natural social consensus or artificial government decree)
- Government Issued—authorized as legal tender by a government

As discussed, hardness is the singular trait that takes primacy over all others in determining a good's suitability for playing a monetary role. Money, as an expression of value, has remained conceptually constant but has evolved to inhabit many different goods over time. Like language, which was first spoken, then written and now typed, the meaning expressed by money remains the same while its modality continually evolves. As the monetary technologies we use to express value change, so too do our preferences.

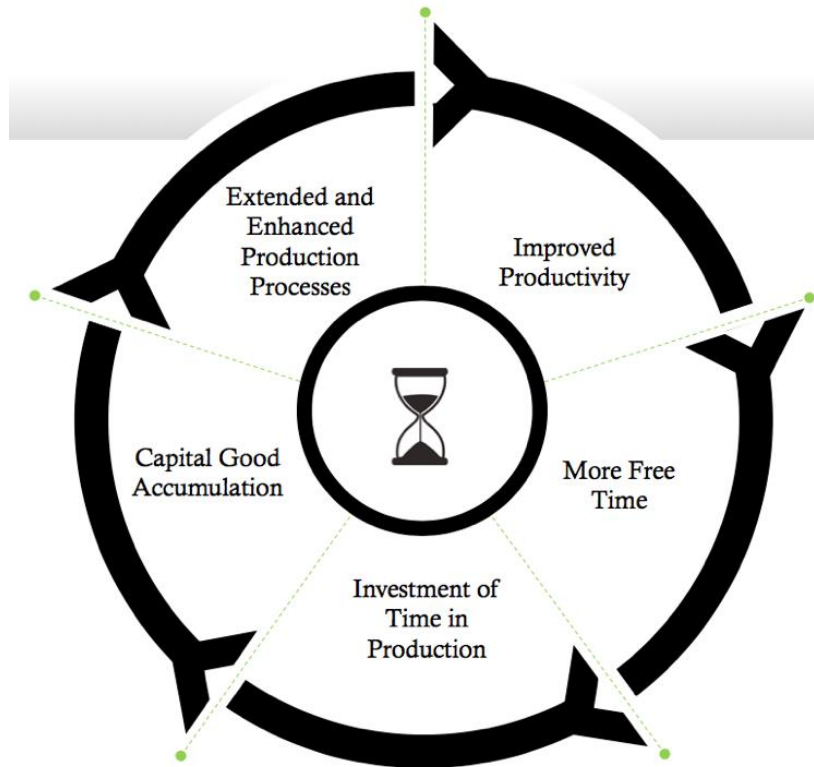
Prospects of Prosperity [1]

In economics, a critical aspect of human decision making is called *time preference*, which refers to the ratio at which an individual values the present relative to the future. Time preference is positive for all humans, as the future is uncertain, and the end could always be near. Therefore, all else being equal, we naturally prefer to receive value sooner rather than later. People who prefer to defer current consumption and instead invest for the future are said to have a lower time preference. The lowering of time preference is closely related to the hardness of money and is also exactly what enables human civilization to advance and become more prosperous. In regard to time preference, hard money is important in three critical aspects:

- By providing a reliable way to protect value across time, hard money incentivizes people to think longer term and thus lowers their time preferences
- As a stable unit of measurement, hard money enables markets to grow ever-larger by reducing the costs and risks of free trade, which increases the incentives for long-term cooperation and lowers time preferences
- Self-sovereign money (like gold and Bitcoin) that cannot be manipulated by any single party reduces governmental intervention which encourages the growth of free markets, which increases their long-term stability and lowers time preferences

A lower time preference is an important part of what separates humans from other animals. By considering what is better for the future, we can curb our animalistic impulses and choose to act rationally and cooperate for the betterment of everyone involved. As humans lower their time preference, they develop a scope for carrying out tasks over longer time horizons. Instead of spending all our time producing goods for immediate consumption, we can choose to spend time creating superior goods that take longer to complete but benefit us more in the long run. Only by lowering time preference can humans produce goods that are not meant to be consumed themselves but are instead used in the production of other goods. Goods used exclusively for the production of other goods are called *capital goods*.

Only humans with a lower time preference can decide to forgo a few hours of fishing and opt to build a superior fishing pole, which cannot be eaten itself, but in the future will enable better results per hour of human effort spent fishing. This is the essence of *investment*: humans defer immediate gratification and invest their time producing capital goods which will, in turn, make the production process itself more sophisticated, extend it over a longer time horizon and yield superior results per hour of human effort. In this way, investment increases capital good stocks which increases productivity. Amazingly, this effect also transforms into a *positive feedback loop*. Also known as a virtuous cycle or the flywheel effect, a positive feedback loop is a process that is recursively energized (its outputs also serve as its inputs) and therefore creates compounding effects. Positive feedback loops play an important role in biology, chemistry, psychology, sociology, economics and cybernetics. In respect to investment, as more capital goods are accumulated, levels of productivity are increased even more and the time horizon of production is extended even further:



As people exhibit lower time preferences and spend their time wisely, they increase their capacity for investment and create more free time for themselves.

To understand this preference clearly, let's consider two hypothetical fishermen, Harold and Louis, who start out with nothing other than their bare hands. Harold has a higher time preference than Louis and chooses to spend his time catching fish with using just his bare hands. Using this approach, Harold spends about 8 hours per day to catch enough fish to feed himself for one day. Louis, on the other hand, spends just 6 hours per day catching fish, makes do with the smaller amount of fish and chooses to spend the other 2 hours building a fishing pole. Two weeks later, Louis has succeeded in building a fishing pole, which he can now use to catch twice as many fish per hour as Harold. Louis's investment in the fishing pole could allow him to only fish for 4 hours each day, eat the same amount of fish as Harold and spend his other 4 hours in leisure. However, since Louis has a lower time preference, he instead chooses to fish for 4 hours per day and spend the other 4 hours building a fishing boat.

One month later, Louis has succeeded in building a fishing boat, which he can now use to go further out to sea and catch fish that Harold has never even seen. Not only has Louis increased his productivity (fish caught per man hour) but he has also increased the quality of his production (a greater variety of fish from the deep sea). By using his fishing pole and boat, Louis now needs only 1 hour per day to catch a day's

worth of food and spends his other 7 hours engaged in further capital accumulation—building better fishing poles, boats, nets, lures, etc.—which, in turn, further increases his productivity and quality of life.

Should Louis and his descendants continue to exhibit a lower time preference, the results will compound over time and across generations. As they accumulate more capital, their work efforts will be ever-further amplified by productivity gains and enable them to engage in ever-larger projects that take ever-longer to complete. These gains are amplified even further when Louis and his descendants begin trading with others that specialize in crafts in which they themselves do not—such as housing, wine making or farming. Successive layers of learning, productivity gains and flourishing trade networks are the foundational sediment upon which all human advancement in terms of knowledge, technology and culture is built. Human advancement is noticeable in the tools we make and the way we relate with one another.

From this perspective, it becomes clear that the most important economic decisions any individual faces are related to the trade-offs they face with their future self. Eat less fish today, build a fishing boat tomorrow. Eat clean today, be healthy tomorrow. Exercise today, be fit tomorrow. Read books today, be knowledgeable tomorrow. Invest money today, be wealthy tomorrow. We can all take solace that this compounding force of nature is always available to each and every one of us. No matter how bad the circumstances are for a man with a low time preference, he will likely find a way to keep compounding his present efforts and prioritizing his future self until he achieves his objectives. Contrarily, no matter how much fortune and wealth favors the man with a high time preference, he will likely find a way to continue squandering his wealth and shortchanging his future self. These individual relationships with our future selves is the microcosm of the societal macrocosm. As society develops a lower time preference, its prospects of prosperity improve in tandem.

Foundation of Economic Growth [1,4]

There are many factors beyond the scope of this essay which influence time preference. Most relevant to our discussion is the expected future value of money. As we have seen, hard money is superior at holding its value across time. Since its purchasing power tends to remain constant or grow over time, hard money incentivizes people to delay consumption and invest for the future, thereby lowering their time preference. On the other hand, soft money is subject to having its supply increased unexpectedly. Increasing the money supply is the same as lowering the *interest rate*, which is effectively the price of borrowing money and the incentive to save. By reducing the interest rate, the incentive to save and invest is diminished whereas the incentive to borrow is increased. So, soft money disincentivizes a favorable orientation towards the future. In other words, soft money systems raise

society's time preference. For this reason, soft money, once it is sufficiently debased, tends to precede societal collapse (more on this later).

An ideal hard money would be one whose supply is absolutely scarce, meaning no one could produce more of it. The only noncriminal way to acquire money in such a society would be to produce something of value and exchange it for money. As everyone seeks to acquire more money, everyone would become ever-more productive which would encourage capital accumulation, productivity gains and a lowering of time preference. Since the money supply is fixed, economic growth would cause the prices of real goods and services to drop over time, as a fixed quantity of monetary units chases an increasing quantity of goods. Since people could expect to be able to purchase more with the same amount of money in the future, such a world would discourage immediate consumption and encourage saving and investment for the future. Paradoxically, a world that consistently defers consumption will actually end up consuming more in the long run as its increased savings would increase investment and productivity, thus making its citizens wealthier in the future. This dynamic would spark a positive feedback loop—with present needs met and an ever-greater focus on the future, people naturally begin concentrating other aspects of life such as social, cultural and spiritual endeavors. This is the essence of free market capitalism: people choosing to lower their time preference, defer immediate gratification and invest in the future.

The foundation of all economic growth is delayed gratification, which leads to savings, which leads to investment, which extends the duration of the production cycle and increases productivity in a self-sustaining, virtuous cycle with no known natural limit.

Debt is the opposite of saving. As saving creates the possibility for capital accumulation and its associated benefits, debt is what can reverse it by reducing capital stocks, productivity and living standards across generations. As we will show later, when the gold standard was forcibly ended by governments, money not only became much softer, but it also fell under the command of politicians who are incentivized to operate with high time preferences as they strive for reelection every few years. This explains why politicians continue to mandate the use of soft government money, despite the long-term harm it causes to an economy, ensuring that it remains the dominant form of money in the world (we will cover soft government money's unnatural ascent to world domination later).

When a form of money becomes globally dominant, it finally serves the third function of money—*unit of account*. History shows us that this function is the final evolutionary stage in the natural ascendancy of monetary goods that achieve a dominant role—which are first a store of value, then a medium of exchange and finally a unit of account. As economist William Stanley Jevons explained:

“Historically speaking, gold seems to have served, firstly, as a commodity valuable for ornamental purposes; secondly, as stored wealth; thirdly, as a medium of exchange; and, lastly, as a measure of value.”

Today, the US Dollar is dominant and serves as the global unit of account as prices are most commonly expressed in its terms. This consistency of expression simplifies trade and enables a (somewhat) stable pricing structure for the global economy.

The Economic Nervous System [1]

Market prices are an essential communicative force in economics. As economic production moves from a primitive scale, it becomes harder for individuals to make production, consumption and trade decisions without having a fixed frame of reference (unit of account) which to compare the value of different objects to one another.

In his paper ‘The Use of Knowledge in Society’ Friedrich Hayek elucidated the economic problem as not merely a matter of allocating human effort. More accurately, the economic problem is one of allocating human effort according to knowledge that is distributed in the minds of people that are each primarily concerned with their respective area in the broader economy. This distributed knowledge includes the:

- Conditions of production
- Availability of the factors of production
- Preferences of individuals

Knowledge, due to its dynamic and fluid nature, cannot be fully known by a single entity as it is constantly in flux and widely distributed within many minds. In a free market economic system prices capture this distributed knowledge, convert it into impartial information and disseminate it widely. *Price signals* are the coordinating force of free market systems. Each individual decision maker can faithfully rely on the prices of goods relevant to their production process, as the prices themselves are a distillation of all known market realities into a single, actionable variable. Each individual’s buy and sell decisions, in turn, further shape prices which carry this altered information back out into the market. Price signals are to market participants what light is to the eye.

To understand this point, consider the 2010 earthquake which badly damaged an area in Chile responsible for a great deal of the world’s copper production. This earthquake severely damaged copper mines and export infrastructure, which immediately reduced the flow of new supply to the world copper market and resulted in a 6.2% increase in its price. Anyone in the world whose business interfaces

with the copper market will be affected by this, but they do not need any specific knowledge about the earthquake in Chile or market conditions to decide how to respond. All the relevant information they need to make effective decisions is contained within the price of copper itself. Immediately, all firms that demand copper are incentivized to demand less, delay purchases or find substitutes. On the other side of the market, all firms that produce copper are incentivized to produce more of it. With a natural shift in price, everyone in the world involved in the copper industry is incentivized to act in a way that alleviates the negative consequences of the earthquake. This is the power of a free market with accurate price signals.

The wisdom of the crowd is always superior to the wisdom of the board room. There is simply no way to recreate the adaptivity and collective intelligence of markets by installing a centralized planning authority. How would they decide who should increase production and by how much? How would they decide who should reduce consumption and by how much? How would they coordinate and enforce their decisions in real time on a global scale? In this sense, prices are the economic nervous system that disseminate knowledge across the world and help coordinate complex production processes by:

- Incentivizing supply and demand changes to match economic reality and restore market equilibriums quickly
- Efficiently matching buyers and sellers in the marketplace
- Compensating producers for their work efforts

Without accurate price signals, humans could not benefit from the division of labor and specialization beyond a small scale. Trade allows producers of goods to mutually increase their living standards by specializing in goods in which they have a relative or *comparative advantage*—goods they can produce relatively faster, cheaper or better. Accurate prices expressed in a common, stable medium of exchange help people identify their comparative advantage and specialize in it. Specialization, guided by reliable price signals, enables producers to improve their efficiency of production and accumulate capital specific to their craft. This is why the most productive allocation of human efforts is only determinable by an accurate pricing system within a free market. Also (as we will see later), this is exactly why capitalism prevailed over socialism, because socialism lacked an economic nervous system. But before diving into the economic aspects which underpinned this historic ideological struggle and seeing how it is still relevant today, we first need to understand the evolutionary forces that have shaped money throughout history.

Monetary Evolution [1]

Throughout history, money has taken many forms—seashells, salt, cattle, beads, stones, precious metals and government paper have all functioned as money at one or more points in history. Monetary roles are naturally determined by the

technological realities of the societies shaping the salability of goods. Even today, forms of money still spontaneously emerge with things like prepaid mobile phone minutes in Africa or cigarettes in prisons being used as localized currencies. Different monetary technologies are in constant competition, like animals competing within an ecosystem. Although instead of competing for food and mates like animals, monetary goods compete for the belief and trust of people. Believability and trustworthiness form the basis of *social consensus*—the source of a particular monetary good's sovereignty from which it derives its market value along with the trust factors and permissions necessary to transact with it.

As these competitions continue to unfold in a free market, goods attain and lose monetary roles according to the traits which determine how believable or trustworthy they are and are expected to remain over time. As we will show, free market competition is ruthlessly effective at promulgating hard money as it only allows those who choose the hardest form available to maintain wealth over time. This *market-driven natural selection* causes new forms of money to come into existence and older forms to fade into extinction. Like biologically-driven natural selection, in which nature continuously favors the organisms which are best suited for success in their respective ecologies, this market-driven natural selection is a process in which people naturally and rationally favor the most believable and trustworthy monetary technologies available in their respective trade networks. Unlike ecological competition which can favor many dominant organisms, the marketplace for money is driven by network effects and favors a winner take all (or, at least, a winner take most) dynamic as the non-coincidence of wants problem is universal and if a single hard money is capable of solving all three of its dimensions than it will become dominant (as discussed earlier in the social network aspects of money).

An example of this market-driven natural selection of money comes from the ancient Rai Stones system of Yap Island, located in what is today Micronesia. Rai Stones were large disks of various sizes with a hole in the middle that weighed up to eight thousand pounds each. These stones were mined in neighboring Palau or Guam and were not native to Yap. Acquiring these stones involved a labor-intensive process of quarrying and shipping. Procuring the largest Rai Stones required workforces numbering in the hundreds. Once the stones arrived in Yap, they were placed in a prominent location where everyone could see them. Owners of the stones could then use them as payment by announcing to the townsfolk the transfer of ownership to a new recipient. Everybody in the town would then record the transaction in their individual ledger, noting the new owner of the stone. There was no way to steal the stone because its ownership was recorded by everyone. In this way, the Rai Stones solved the three dimensions of the non-coincidence of wants problem for the Yapese by providing:

- Salability across scales as the stones were various in size and payments could be made in fractions of a stone
- Salability across space as the stones were accepted for payment everywhere on the island and did not have to be moved physically, just recorded by the townsfolk's individual ledgers (remarkably similar to Bitcoin's distributed ledger model, as we will see later)
- Salability across time due to the durability of stones and the difficulty of procuring new stones which meant that the existing supply of stones was always large relative to any new supply that could be created within a given time period (a high stock-to-flow ratio)

This monetary system worked well until 1871, when an Irish-American captain named David O'Keefe was found shipwrecked on the shores of Yap by the local islanders. Soon, O'Keefe identified a profit opportunity in buying coconuts from the Yapese and selling them to coconut oil producers. However, he could not transact with the locals because he was not a Rai Stone owner and the locals had no use for his foreign forms of money. Undeterred, O'Keefe sailed to Hong Kong and acquired some tools, a large boat and explosives to procure Rai Stones from neighboring Palau. Although he met resistance from them initially, he was eventually able to use his Rai Stones to purchase coconuts from the Yapese. Other opportunists followed O'Keefe's lead and soon the flow of Rai Stones increased dramatically. This sparked conflict on the island and disrupted economic activity. By using modern technologies to acquire Rai Stones more cheaply, foreigners were able to compromise the hardness of this ancient monetary good. The market naturally selected against Rai Stones because, as their stock-to-flow ratio declined, they became less reliable as a store of value and thus lost their salability across time, which ultimately led to the extinction of this ancient monetary system.

A similar story played out in western Africa which for centuries used aggrary beads as money. These small glass beads were used in a region where glassmaking was an expensive craft, which gave them a high stock-to-flow ratio and made them salable across time. Since aggrary beads were small and light they could easily be combined into necklaces or bracelets and transported easily, thus giving them salability across scales and space. In the 16th century, European explorers discovered the high value ascribed to these beads by the west Africans and began importing them in mass quantities; as European glassmaking technology made them extremely cheap to produce. Slowly but surely, the Europeans used these cheaply produced beads to acquire most of the precious resources of Africa. The net effect of this incursion into Africa was the transference of its vast natural resource wealth to Europeans and the conversion of aggrary beads from hard money to soft money. Again, the market naturally selected against a monetary good once its stock-to-flow ratio began to decline, as its store of value functionality and, therefore, its salability across time were compromised as a result. Although the details vary, this underlying dynamic of a declining stock-to-flow ratio presaging a good's loss of its monetary role has been the

same for every form of money throughout history. Today, we are seeing a similar pattern cause the collapse of the Venezuelan bolivar, (where some Venezuelans are using Bitcoin to protect their wealth as the currency collapses).

As societies continued to evolve, they began to move away from artifact money like stones and glass beads and towards monetary metals. It was initially difficult to produce most metals which kept their supply flows low, thus giving them good salability across time. Gold in particular, with its extreme rarity in the Earth's crust and its virtual indestructibility, made it an extremely hard monetary technology. Gold mining was difficult, limiting supply increases relative to its existing supply, which itself could not be destroyed. Gold gave humans a way to store value across generations and develop a longer-term perspective on their actions (a lower time preference), which led to the proliferation of ancient civilizations:



The earliest coins are found mainly in the parts of modern Turkey that formed the ancient kingdom of Lydia. They are made from a naturally occurring mixture of gold and silver called electrum.

Monetary Metals [1]

The last dictator of the Roman Republic, Julius Caesar, issued a gold coin called the aureus coin which contained a standard 8 grams of gold. The aureus was traded widely across Europe and the Mediterranean, alongside a silver coin called the denarius, which was used for its superior salability across scales. Used together, these coins provided a hard money system that increased the scope of trade and specialization in the Old World. The republic became more economically stable and integrated for 75 years until the infamous emperor Nero came into power.

Nero was the first to engage in the act of *coin clipping* in which he would periodically collect the coins of his citizenry, melt them down and mint them into newer versions with the same face value but less precious metal content, keeping the residual content to enrich himself. Similar to modern day inflation, this was a way of surreptitiously taxing the population by debasing its currency. Nero and successive emperors would continue the practice of coin clipping for several hundred years to finance government expenditures:



Isaac Newton is attributed with adding the small stripes along the edges of coins as a security measure against coin clipping. These stripes are still present on most coins today.

Citizens gradually wised up to this deceit and began hoarding the coins with higher precious metal content and spending the debased coins, as they were legally required to be accepted at face value in settlement of debts, one of the earliest instances of *legal tender* laws being implemented. This had the effect of driving up the price of coins with higher precious metal content and driving down the price of those with less—a dynamic that came to be known as *Gresham's Law*: bad money (soft money) drives good money (hard money) out of circulation. This is an important law to recall when we look at how modern-day hoarding of Bitcoin impacts its price.

Eventually, a new coin called the solidus was introduced which contained only 4.5 grams of gold, almost half the content of the original aureus coin. Pursuant to this decline in monetary value, a cycle familiar to many modern economies running on government money began to take hold—coin clipping reduced the money's real value, increased the money supply, gave the emperor the means to continue imprudent spending and eventually ended with rampant inflation and economic crisis. Analogous to central bank practices today, Swiss banker Ferdinand Lips summarized this era well:

"Although the emperors of Rome frantically tried to 'manage' their economies, they only succeeded in making matters worse. Price and wage controls and legal tender laws were passed, but it was like trying to hold back the tides. Rioting, corruption, lawlessness and a mindless mania for speculation and gambling engulfed the empire like a plague."

Amid the chaos of the crumbling Roman Republic, Constantine the Great took power. Intent on restoring the once great empire, Constantine began adopting responsible economic policies. He first committed to maintaining the solidus at 4.5 grams of gold, ended the practice of coin clipping and began minting massive quantities of these standardized gold coins. Constantine then moved east and

established Constantinople in modern day Istanbul. This became the birthplace of the Eastern Roman Empire, which adopted the solidus as its monetary system.

Rome continued its soft money-induced cultural deterioration until it finally collapsed in 476 AD. Meanwhile, Constantinople flourished. The solidus, which eventually became known as the bezant, provided a hard money system with which Constantinople would remain prosperous and free for centuries to come. As with Rome before it, the fall of Constantinople happened only when its rulers began the debasing its currency around 1050 AD. As with Rome before it, the move away from hard money led to the fiscal and cultural decline of the Eastern Roman Empire. After suffering many successive crises, Constantinople was ultimately overtaken by the Ottomans in 1453. However, the bezant inspired another form of hard money that still circulates to this day, the Islamic dinar. People all over the world have used this coin for over seventeen centuries—which began as the solidus before changing its name to the bezant and finally becoming the Islamic dinar—for transactions, thus highlighting the superior salability of a hard money such as gold across time.

Following the collapse of the Roman Empire, Europe fell into the dark ages. It was the rise of the city-state (a new story mankind would begin organizing itself around) and its use of hard money systems that would pull Europe out of the Dark Ages and into the Renaissance. Beginning in Florence in 1252, the city minted the florin which was the first major European coinage issued since Julius Caesar's aureus. By the end of the 14th century more than 150 European cities and states had minted coins to the same specifications as the florin. By giving its citizenry the ability to accumulate wealth in a reliable store of value which could be traded freely across scales, space and time, this hard money system unlocked scientific, intellectual and cultural capital within the Italian city-states and eventually spread to the rest of Europe. Of course, the situation was far from perfect, as there were still many periods marked by various rulers choosing to debase their currencies to finance war or lavish expenditure.

Global Gold Standard [1,4]

When they were being used as physical means of settlement, gold and silver coins served complementary roles. Silver, having a stock-to-flow ratio second only to that of gold, had the advantage of being a more salable metal across scales, since its lower value per weight than gold made it ideal as a medium of exchange for smaller transactions. In this way, gold and silver were complementary as gold could be used for large settlements and silver could be used for smaller payments. However, by the 19th century, with the development of modern custodial banking and advanced telecommunications, people were increasingly able to transact seamlessly across scales using bank notes or checks backed by gold:



The US Dollar was once redeemable for gold on demand.

With all of the critical salability characteristics gathered under a gold standard monetary system facilitated by paper bank notes, the superior salability across scales of physical silver lost relevance, setting it up to become demonetized (due to the winner take all dynamic discussed earlier). Ironically, the same banking industry that enabled a global gold standard would in later years see to its elimination (more on this later).

A brief aside on silver: This demonetization dynamic also explains why the silver bubble popped many times throughout history when facing off with gold and will pop again if it ever reflate. Since silver is not the hardest form of monetary good available, should any significant investment flow into silver, its producers will be incentivized to increase the flow of silver, and store any value expropriated from its increased production in the hardest form of money available to them (which, before Bitcoin, was only gold). This, of course, will bring the price of silver crashing back down, taking the wealth from the investment inflows with it. As a more recent historical example of this dynamic in action: In the 1970s, the affluent Hunt brothers attempted to remonetize silver by buying vast quantities of it in the market. This drove up the price initially, and the Hunt brothers believed they could continue driving up its price until they cornered the market. Their intent was to induce others to chase its appreciation and recreate a monetary demand for silver. As they kept buying and the price kept rising, silver holders and producers kept selling into the market. No matter how much the Hunt brothers purchased, the selling and flow of silver continued to outpace their buying, which decreased its stock-to-flow ratio and eventually led to a dramatic crash in the price of silver. The Hunt brothers lost over \$1B (due to rampant inflation of government money since then, their losses equal \$6.5B in 2019 dollars) in the ordeal, which is likely the highest price ever paid for learning the importance of hard money and its defining metric, the stock-to-flow ratio.

Driven by expanding telecommunication and trade networks, and with custodial banks enhancing its salability across scales by issuing gold-backed bank notes and checks, the gold standard spread quickly. More nations began switching to paper

based monetary systems fully backed by and redeemable in gold. Network effects took hold as more nations moved onto the gold standard, giving gold deeper liquidity, more marketability and creating larger incentives for other nations to join.

Those nations which remained on a silver standard the longest before converting, like China and India, witnessed tremendous devaluations of their currencies in the intervening period. The demonetization of silver for China and India was an effect similar to the west Africans holding aggrary beads when Europeans arrived. Foreigners who adopted the gold standard were able to gain control over vast quantities of the capital and resources in China and India. This drives home a key point: every time hard money encounters a softer form of money in a trade network, the softer money is ultimately outcompeted into extinction.

This dynamic has significant consequences for the holders of soft money and is an important lesson for anyone who believes their refusal of Bitcoin means they are protected from its economic impact. History shows us repeatedly that it is not possible to protect yourself from the consequences of others holding money that is harder than yours.

Finally, for the first time in history, the majority of the world economy began operating on a gold-based, hard money standard that was naturally selected for by the free-market.

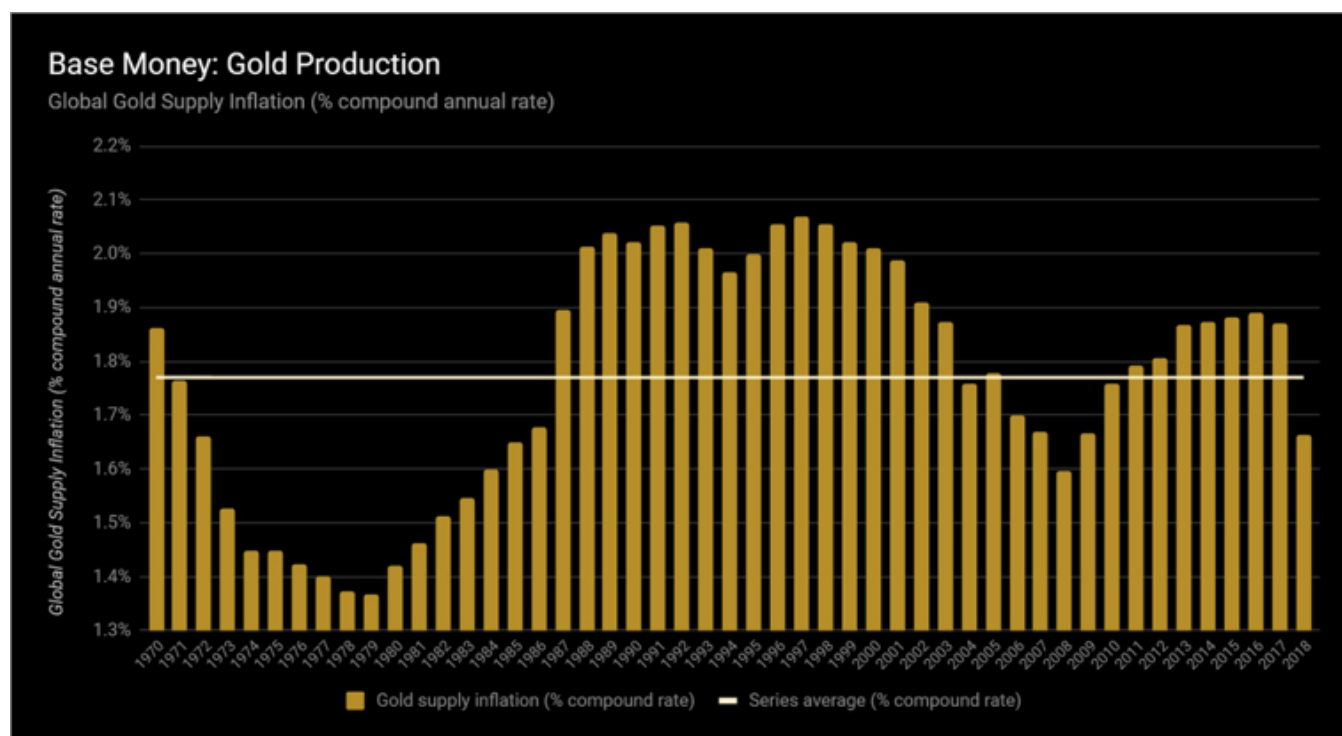
Hardness of Gold [1,3]

By this point in history, virtually everyone had come to fully trust gold's superior stock-to-flow ratio and therefore believed they could use it to reliably store value across time. After thousands of years of mining this chemically stable element, virtually all the gold ever procured by humans is still a part of its extant supply. The stock of all the gold in the world fits into an Olympic-sized swimming pool today and is valued at almost \$8T USD. Gold is rare in the Earth's crust and extraction is costly in terms of time and energy, which keeps its flow predictably low. It is impossible to synthesize gold by chemical means (as alchemy never panned out) and the only way to increase its supply is through mining.

The costliness of gold mining is the *skin in the game* necessary to increase its flow—the risk necessary to procure the reward. Skin in the game is a concept based on symmetry, a balance of incentives and disincentives: in addition to upside exposure, people should also be penalized if something for which they are responsible for goes wrong or hurts others. Skin in the game is the central pillar for properly functioning systems and is at the heart of hard money. For gold, its mining costs and risks form the disincentives which are balanced against the incentives of its market price. Unless consequential decisions are made by people who are exposed to the results of

their decisions, the system is vulnerable to total collapse (an important consideration when we discuss soft government money later).

Every market-driven evolutionary step for money has naturally selected the form with the highest stock-to-flow ratio available to its population but stopped when the form lost this key property. With the highest stock-to-flow ratio of all the monetary metals, gold is the hardest physical form of money that has ever existed, which explains its success as hard money throughout history. Even with advances in mining techniques, gold still has a relatively low and predictable flow, as evidenced by its annual supply growth since 1970:



The rarity of gold in the Earth's crust ensures that its new supply flows are relatively low and predictable. Since gold is virtually indestructible, nearly every ounce that has ever been mined throughout history is still part of current supply stocks. The combination of these factors gives gold the highest stock-to-flow ratio of any monetary metal and is precisely the reason gold became a global hard money standard.

Gold mining, of course, only makes economic sense if the cost of producing an additional ounce of gold is less than gold's market price per ounce. Relatedly, when the price of gold increases, its mining becomes more profitable and draws new miners into the market and makes new methods of gold mining economically feasible. This, in turn, increases the flow of gold until supply and demand forces again reach equilibrium. So, although gold is the hardest form of physical money, it doesn't

have perfect hardness as changes in demand for it elicit both a supply and price response, meaning:

- An increase in the demand for gold increases its price,
- An increase in the price of gold incentivizes gold miners to increase its flow,
- An increase in the flow of gold increases its supply
- An increase in the supply of gold puts downward pressure on its price

In this way, changes in demand for gold are expressed partially in its price and partially in its supply flow. This *price elasticity of supply* is true for all physical commodities. For all practical purposes, as we will see later, the Earth always has more natural resources to yield assuming the right amount of time and effort are directed towards their production (this will support an important point later when we look at the impact of changes in demand on Bitcoin's price).

Final Settlement [1]

Gold also has the advantage of being an instrument of *final settlement*. Whereas the use of government money requires trust in the monetary policy and creditworthiness of the issuing authority or payment intermediaries, known as *counterparty risk*, the act of physically possessing gold comprises all of the trust factors and permissions necessary to use it as money. This makes gold a self-sovereign form of money. This is best understood as an identity of the universal accounting equation: $\text{Assets} = \text{Liabilities} + \text{Owner's Equity}$

When you own gold free and clear, it is your asset and no one else's liability, meaning that your personal balance sheet includes a 100% gold asset matched by 0% liabilities and 100% owner's equity (since no one else has a claim on your gold asset). This makes gold a *bearer instrument*, meaning that any individual in physical possession of the asset is presumed to be its rightful owner. This timeless and trustless nature of gold is the reason why it still serves as the base money and final settlement system of central banks worldwide.

In the 19th century, the term *cash* referred to central bank gold reserves, which was the dominant self-sovereign monetary good at the time. Cash settlement referred the transfer of physical gold between central banks to execute final settlement. Central banks can only settle with finality in physical gold, and still do so periodically in the modern era, since it is the only form of money that requires no trust in any counterparty, is politically neutral and gives its holders full sovereignty over their money. This is why gold maintains its monetary role even today as only the delivery of a bearer instrument can truly be the final extinguisher of debt. In this original sense of the word cash, gold is the only form of dominant cash money that has ever existed (although Bitcoin is well-suited to serve a similar role in the digital age, more on this

later). Unfortunately, the combination of gold's self-sovereignty and physicality would lead to the demise of the gold standard.

Centralization of Gold [1,4]

By the end of the 19th century, all the industrialized nations of the world were officially on the gold standard. By virtue of operating on a hard money basis, most of the world witnessed unprecedented levels of capital accumulation, free global trade, restrained government and improving living standards. Some of the most important achievements and inventions in human history were made during this era, which came to be known as *la belle époque* across Europe and *the Gilded Age* within the United States. This golden era enabled by the gold standard remains one of the greatest periods in human history:

“La Belle Époque was a period characterized by optimism, regional peace, economic prosperity, an apex of colonial empires, and technological, scientific, and cultural innovations. In the climate of the period, the arts flourished. Many masterpieces of literature, music, theater, and visual art gained recognition.”

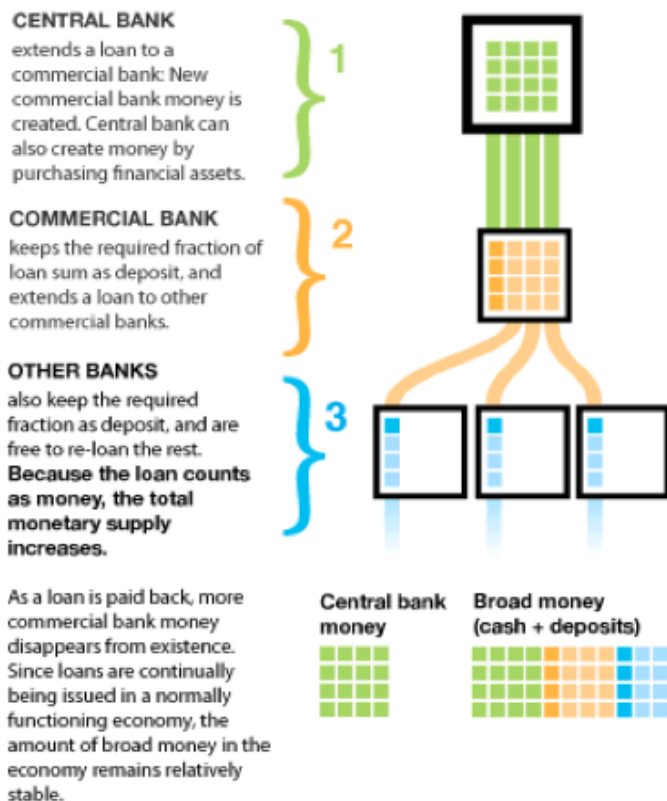
As multiple societies had now converged on gold as their universal store of value, they experienced significant decreases in trade costs and an attendant increase in free trade and capital accumulation. La Belle Époque was an era of unprecedented global prosperity. However, the hard money gold standard which catalyzed it suffered from a major flaw: settlement in physical gold cumbersome, expensive and insecure. This flaw is associated with the physical properties of gold, as it is dense, not deeply divisible and not easily transactable. Gold is expensive to store, protect and transport. It is also heavy per unit of volume which makes it difficult to use for day to day transactions. As discussed earlier, banks built their business model around solving these problems by providing secure custody for people's gold hoards. Soon after, banks began issuing paper bank notes that were fully redeemable in gold. Carrying and transacting with paper bank notes backed by gold was much easier than using actual gold. Offering superior utility and convenience, the use of bank notes flourished. This, along with government programs to confiscate gold from citizens (such as Executive Order 6102 in the United States), encouraged the centralization of gold supplies within bank vaults all over the world.

Incapable of resisting the temptation of wealth expropriation by tampering with the money supply, banks soon began issuing more notes than their gold reserves could justify, thus initiating the practice of *fractional reserve banking*. This banking model facilitated the creation of money without any skin in the game. Governments took notice and began to gradually take over the banking sector by forming central banks,

as this model enabled them to engage in *seigniorage*, a method of profiting directly from the *money creation process*:

Money creation

through fractional reserve banking (expansionary monetary policy)



In fractional reserve banking artificial money and credit is created. For instance, assuming a reserve ratio of 10% and an initial deposit of \$100 will soon turn into \$190. By lending a 90% fraction of the newly created \$90, there will soon be \$271 in the economy. Then \$343.90. The money supply is recursively increasing, since banks are literally lending money they don't have. In this way, banks magically transform \$100 into over \$1,000.

The ability to control this process was too tempting for governments to resist. Total

control of over the money supply gave those in charge a mechanism to continually extract wealth from its citizenry. The virtually unlimited financial wealth the printing press provided gave those in power the means to silence dissent, finance propaganda and wage perpetual warfare. It is a fundamental economic reality that wealth cannot be generated by tampering with the money supply, it can only be manipulated and redistributed. Civilization itself relies on the integrity of the money supply to provide a solid economic foundation for free trade and capital accumulation. With a firm grip on the prevailing monetary order established, the next logical step for central banks was to begin moving away from the gold standard altogether.

Abolishing the Gold Standard [1]

By 1914, most of the major economies had begun printing money in excess of their gold reserves at the onset of World War I. Unsurprisingly, this had many negative consequences, some of which were immediate while others came on more slowly. Eliminating the gold standard immediately destabilized the unit of account by which all economic activity was assessed. Government currency exchange rates would now float against one another and become a source of economic imbalance and confusion. This distorted price signals, which would now be denominated in various government currencies with rapidly fluctuating exchange rates. This made the task of economic planning as difficult as trying to build a house with an elastic measuring tape.

For a world that was becoming increasingly globalized and technologically sophisticated, freely floating currency exchange rates represented a significant step backwards and gave rise to what is commonly called a 'a system of partial barter'. For people to buy goods from other people who lived on the other side of any number of imaginary lines called national borders, they would now be required to use more than one medium of exchange (their own currency and the foreign currency) to complete the transaction. To an extent, this reignited the non-coincidence of wants problem which money was meant to solve in the first place. Today, over \$5T (\$5,000,000,000,000) of foreign currencies are exchanged daily, forming an annual market valued at over 12 times global GDP. This industry is purely parasitic—it enriches bankers and sucks real value out of society in the form of global trade frictions, market distortions and transaction fees. For this reason, it is excluded from GDP calculations and exist solely because of the inefficiencies caused by centrally controlled capital markets and the absence of a global, politically neutral hard money system. The resultant frictions to global trade fanned the flames of warfare.

Governments Take Control [1,3]

As 20th century wars raged, so did the printing presses. Governments and their central banks continued to grow more powerful with each new bank note printed as their citizens became poorer. The death stroke came when most governments, due to a unilateral decision of President Nixon in United States, finally severed the peg to gold entirely in the 1971. Which brings us to the modern form of dominant money: *government fiat money*. Fiat is a Latin word meaning decree, order or authorization. This is why government money is commonly referred to as fiat money, since its value exists solely because of government decree:



Today, the US Dollar is not redeemable for anything and its value is derived solely from government decree. Paradoxically, people were coerced into adopting soft government fiat money only because of their shared belief in gold as a hard monetary good.

This is an imperative point: it was possession of gold (self-sovereign, hard money) that gave governments the power to decree the value of their fiat money (soft money) in the first place. National governments were only able to achieve “sovereignty” because they drew this power from their possession of gold. Paradoxically, people were coerced into discarding the gold standard and adopting soft government fiat money only because of their belief in gold as a hard monetary good. This is proof that it is possible to create an artificial asset and endow it with monetary properties, whether by decree or by market-driven natural selection. Governments did so by stealing gold from citizens, which gave them the power to create fiat money and decree its value by force. As we will later see, Satoshi Nakamoto did so by creating Bitcoin and releasing it into the marketplace as a self-sovereign money free to compete for the trust and belief of the people based on its own merits.

Central banks also began engaging in propaganda campaigns declaring the end of gold’s monetary role. However, their actions rang louder than their words as they continued to accumulate and hold gold, a practice they continue to this day. Gold remains the exclusive instrument of final settlement between central banks. Strategically, holding large gold reserves also makes sense for central banks since they can opt to sell reserves into the market should gold start to appreciate too quickly and threaten the value of fiat money. With their monopoly position protected and reinforced by legal tender laws, propagandists and sufficient control of the gold market central banks were free to print money at will. This exorbitant privilege gives central banks extraordinary power and made them extremely dangerous entities. In the words of former US President Andrew Jackson spoken at the Constitutional Convention in 1787:

"I believe that banking institutions are more dangerous to our liberties than standing armies. If the American people ever allow private banks to control the issue of their currency, first by inflation, then by deflation, the banks and corporations that will grow up around them will deprive the people of all property until their children wake up homeless on the continent their fathers conquered. The issuing power should be taken from the banks and restored to the people, to whom it properly belongs."

Unlike to the flow restrictions associated with gold mining, there are practically no economic restraints preventing a government from printing more fiat money. Since there is virtually no cost associated with producing additional units (no skin in the game), government fiat money is the softest form of money in the history of the world. Predictably, money supplies grew quickly, especially in the heat of warfare. In the past, for societies operating with hard money systems, once the tide of war had shifted in favor of one belligerent over the other, treaties were quick to be negotiated as war is an extraordinarily expensive endeavor. The fiat money printing press, on the other hand, gave governments the ability to tap the aggregate wealth of entire populations to finance military operations by implicitly taxing them via inflation. This provided a more secretive, implicit method of funding warfare than explicit taxation or selling government wartime bonds. Wars began lasting much longer and became more violent. It is no coincidence that the century of total war coincided with the century of central banking:

Table 5.1

Conflicts steadily cost more in human lives

Period	Conflict-related deaths (millions)	World population, mid-century (millions)	Conflict-related deaths as share of world population (%)
Sixteenth century	1.6	493.3	0.32
Seventeenth century	6.1	579.1	1.05
Eighteenth century	7.0	757.4	0.92
Nineteenth century	19.4	1,172.9	1.65
Twentieth century	109.7	2,519.5	4.35

The ability to print unlimited quantities of money gives governments a means to finance military operations by implicitly taxing their citizens via inflation. This provides a more secretive method of funding warfare than explicit taxation or selling government wartime bonds. Resultantly, wars have grown in duration and violence.

As is to be expected, soft government money has an abysmal track record as a store of value. This becomes abundantly clear when we look at its inflationary effects on the price of gold. An ounce of gold in 1971 was worth \$35 USD, and today is worth over \$1,200 USD (a decrease of over 97% in the value of each dollar due entirely to inflation). Based on these figures, it is easy to see that gold continues to appreciate as its supply is increased less quickly than the supply of \$USD (government fiat money). The constantly increasing supply of government money means its currency depreciates continuously, as wealth is stolen from the holders of the currency (or assets denominated in it) and transferred to those who print the currency or receive it earliest. This transfer of wealth is known as the *Cantillon Effect*: the primary beneficiaries from expansionary monetary policy are the first recipients of the new money, who are able to spend it before it has entered wider circulation and caused prices to rise. Generally, this is why inflation hurts the poorest and helps the bankers, who are closest to the spigot of liquidity (the government fiat money printing press) in the modern economy. A centrally planned market for money like this completely contradicts the principles of free market capitalism.

Free Market Capitalism versus Socialism [1]

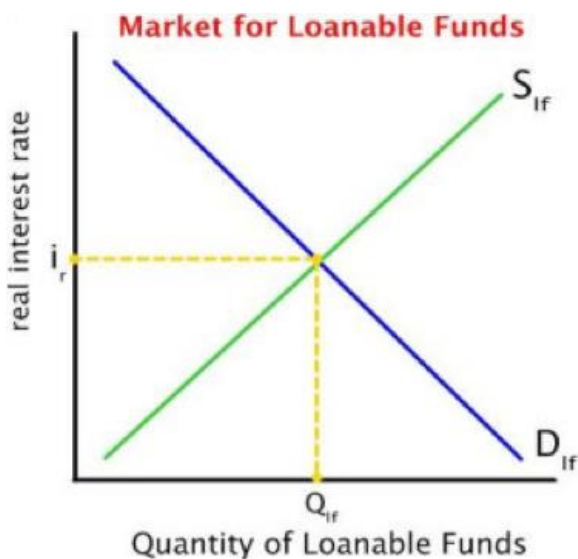
In a socialist system, the government owns and controls all means of production. This ultimately makes the government the sole buyer and seller of all capital goods in its economy. Such centralization stifles market functions, like price signals, and makes decision making highly ineffective. Without accurate pricing of capital goods to signal their relative supply, demand and relevant market conditions, there is no rational way to determine the most productive allocation of capital. Further, there is no rational way to determine how much to produce of each capital good. Scarcity is the starting point of all economics and people's choices are meaningless without skin in the game in the form of price or trade-offs. A survey without a price would find that everyone wants to own a private island but when price is included, very few can afford to own a private island. The point here is not to trumpet free market capitalism over socialism, but rather to clearly explicate the difference between the two ways of allocating resources and making production decisions:

- Free Market Capitalism places trust in Price Signals
- Socialism places trust in Centralized Planning

A free market is one in which buyers and sellers are free to transact on terms determined solely by them, where entry and exit into the market are free and no third parties can restrict or subsidize any market participants. Most countries today have well-functioning, relatively free markets. However, every country in the world today engages in centralized planning of the *market for money* (aka the market for financial capital) itself.

No country in the world today has a free market for money, which is the most important market in any economy.

In a modern economy, the market for money consists of the markets *loanable funds*. These markets match savers with borrowers using the interest rate as their price signal. In a free market for loanable funds, the supply of loanable funds rises as the interest rate rises, as more people are willing to loan their savings out at a higher price. Conversely, the demand for loanable funds decreases as the interest rate rises, as less people are inclined to borrow funds at a higher price:



In a free market for money, the interest rate (the price of money) is determined by natural supply and demand dynamics. Central banks attempt to “manage” these market forces and in doing so create recessions and the boom-and-bust business cycle which is now considered “normal” in the modern era.

Notice that the interest rate in a free market for capital is always positive because of people's naturally positive time preference, meaning that no one would part with money unless they could receive more of it in the future. These natural market forces are artificially manipulated in every market for money in the world. All markets for money in the world today are centrally planned by central banks, who are responsible for “managing” the market for loanable funds using monetary policy tools. Since banks today also engage in fractional reserve banking, they lend out not only customers' savings, but also their demand deposits (monies available to customers on demand, like checking accounts). By loaning out demand deposits to a borrower while simultaneously keeping them available to the depositor, banks can effectively create new, artificial money (a part of the money creation process from earlier). Central banks have the power to manipulate the market for financial capital and can artificially increase the money supply by:

- Reducing interest rates, which increases demand for borrowing and money creation by banks
- Lowering the required reserve ratios, allowing banks to lend more money out than their capital reserves justify
- Purchasing government debt or other financial assets with newly created money in the open market
- Relaxing lending eligibility criteria, allowing banks to increase lending activities and money creation

In a free market for money, the exact amount of savings equals the exact amount of loanable funds available to borrowers for the production of capital goods. This is why the availability of capital goods, as we saw with Harold and Louis, is inexorably linked to a reduction in consumption. Again, scarcity is the starting point of all economics, and its most important implication is the notion that all decisions involve tradeoffs.

In the free market for money, the opportunity cost of saving is foregone consumption, and the opportunity cost of consumption is foregone saving—an indisputable economic reality.

No amount of centralized planning can alter this fundamental economic reality. This is why centrally planned markets always suffer from distortions (aka bubbles, surpluses or shortages) as political agendas run up against the underlying free market forces. Undeterred, central banks continually attempt to “manage” these market forces to achieve politically established policy goals. Most often, central banks are trying to spur economic growth and consumption, so they will increase the supply of loanable funds and lower the interest rate. With the price of loanable funds (the interest rate) artificially suppressed, producers take on more debt to start projects than there are savings to finance these projects. These artificially low interest rates don’t provide any benefit to the economy, rather they simply disseminate distorted price signals that encourage producers to embark on projects which cannot realistically be financed from actual savings. This creates a market distortion (in other words, blows up another bubble) in which the value of consumption deferred is less than the value of the savings borrowed. This distortion can persist for some time but will inevitably unwind with disastrous consequences as economic reality cannot be fooled for long.

The excess supply of loanable funds, backed by no actual deferred consumption, initially encourages producers to borrow as they believe the funds will allow them to buy all the capital goods necessary for their project to succeed. As more producers borrow and bid for the same amount of capital goods, inflation sets in and prices begin to rise. At this point, the market manipulation is exposed since the projects become unprofitable after the rise in capital good prices (due to inflation) and suddenly begin to fail. Projects like these would not have been undertaken in the first place absent the distortions in the market for money created by central banks. An

economy-wide simultaneous failure of overextended projects like this is called a *recession*. The boom and bust *business cycle* we have all grown accustomed to in the modern economy is an inevitable consequence of this centrally planned market manipulation. The United States and Europe saw a great illustration of this process when the dot-com bubble of the late 1990s was replaced by the housing bubble of the mid-2000s.

Free market capitalism cannot function without a free market for money.

As with all well-functioning markets, the price of money must emerge through the natural interactions of supply and demand. Healthy markets require functional nervous systems, as market participants must have accurate price signals to make decisions effectively. Basic economics shows us clearly that central bank meddling in the market for money is the root cause of all recessions and the business cycle. By imposing an artificial price, in this case the interest rate on loanable funds, central banks inhibit natural price signals which coordinate allocation decisions among savers and borrowers. Their market manipulation creates market distortions and recessions. Attempting to remedy a recession by injecting more artificial liquidity into the system will only exacerbate the distortions which caused the crisis in the first place and blow up new bubbles. Only central planning of a soft money supply and its pricing mechanism can cause widespread failures in an economy like this, as an economy based on hard money remains firmly rooted in economic reality and resists market distortions.

Alignment with natural market forces like supply, demand and the price signal is the principal reason free market capitalism prevailed over socialism.

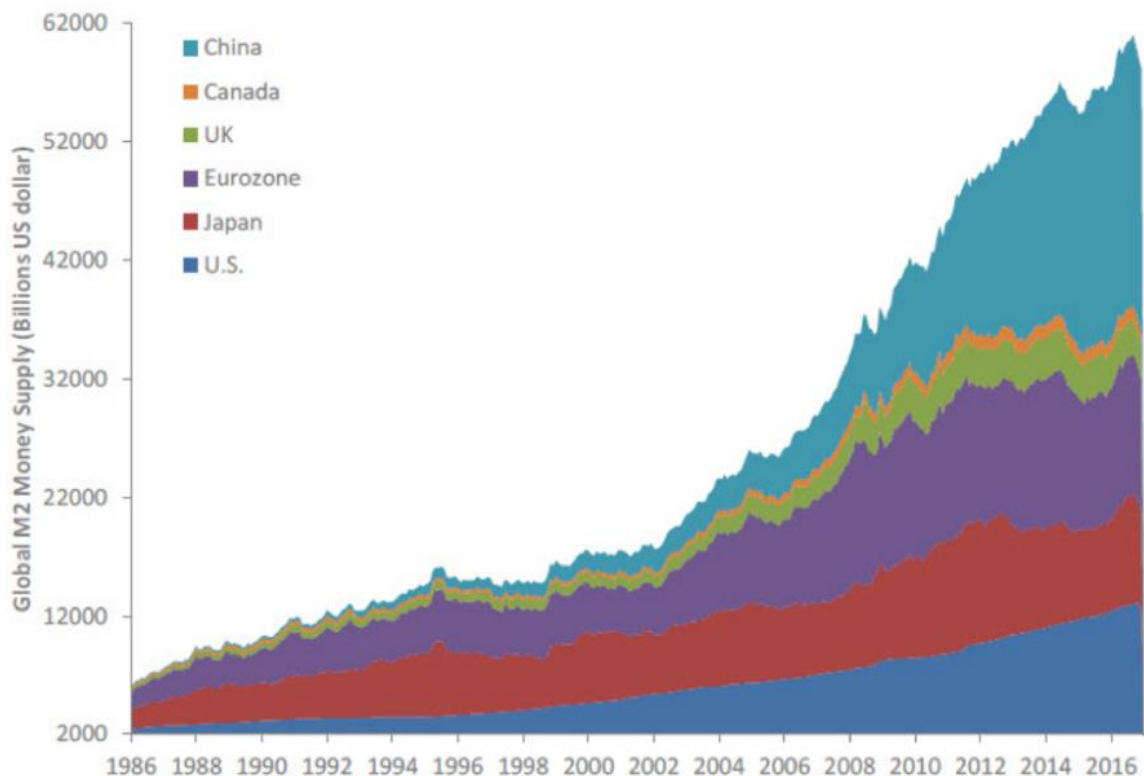
Failure of Government Fiat Money [1,3,4]

Seeing that governments have been forced to use coercive measures, such as confiscating gold and implementing legal tender laws, to enforce adoption of fiat money is a clear indication that soft money is inferior and doomed to fail in a free market. This severe inadequacy of government fiat money came to the forefront of global consciousness in the wake of the Great Recession that began in 2008. Due to gigantic market distortions driven by artificially low interest rates and credit ratings agencies with no skin in the game, US subprime real estate became the largest bubble in modern history. When it bursts, its affects were globally systemic, and central banks all over the world (predictably) began increasing their money supplies in an attempt to reflate their broken economies.

Instead of calling it what really is, central banks now deceptively refer to the act of printing money as *quantitative easing*. As we have learned, increasing the money supply creates no real economic value, it only causes market distortions and furthers the misallocation of capital. Injecting liquidity into an economic system experiencing

a recession only provides illusory, temporary relief. Printing money delays and exacerbates the inevitable correction, as economic reality cannot be deceived forever. Despite economic reality, central bank market manipulation is worse than ever.

Here we show the amount of government fiat money printed by the largest economies of the world since 1986:



Money supply growth by global central banks is accelerated after each recession. This artificial liquidity only provides illusory relief and further distorts the market signals which caused the distortions in the first place.

It was in the depths of the Great Recession that an anonymous individual named Satoshi Nakamoto introduced the open-source software project called Bitcoin to an online group of cryptographers. Many attempts at creating a digital cash had been made over the previous twenty years but none had succeeded. Initially, few in the group took Bitcoin seriously. However, Nakamoto was eventually able to convince a few other cryptographers to join and the Bitcoin network was born.

After ten years of virtually perfect operation, the Bitcoin network has gone from \$0 to \$80B in value stored on its network and has cleared \$1.38T in total transactions. It is

clear that this monetary technology is now competing successfully in the marketplace and is being used by many for real world purposes.

Synthesized Works & Further Reading

- [1] [The Bitcoin Standard: The Decentralized Alternative to Central Banking](#) by Saifedean Ammous (a masterful work on which much of this essay is based)
- [2] [The Rational Optimist](#) by Matt Ridley
- [3] [Skin in the Game](#) by Nassim Nicholas Taleb
- [4] [The Bullish Case for Bitcoin](#) by Vijay Boyapati
- [5] [The Age of Cryptocurrency](#) by Paul Vigna and Michael J. Casey
- [6] [Sapiens](#) by Yuval Harari
- [7] *Bitcoin is a Decentralized Organism*, [Part 1](#) and [Part 2](#) by Brandon Quittem
- [8] [PoW is Efficient](#) by Dan Held
- [9] [The Fifth Protocol](#) by Naval Ravikant
- [10] [Unpacking Bitcoin's Social Contract](#) by Hasu
- [11] [Antifragile](#) by Nassim Nicholas Taleb
- [12] [Letter to Jamie Dimon](#) by Adam Ludwin
- [13] [Placeholder VC Investment Thesis Summary](#) by Joel Monegro and Chris Burniske
- [14] [Diffusion of Innovations](#) by Everett M. Rogers
- [15] [Why America Can't Regulate Bitcoin](#) by Beautyon
- [16] [Hyperbitcoinization](#) by Daniel Krawisz

Money, Bitcoin and Time: Part 2 of 3

By [Robert Breedlove](#)

Posted January 26, 2019



The Simple Truth about Bitcoin: Bitcoin is the hardest form of money ever invented. It has successfully brought the advantages of physical cash money into the digital realm. Bitcoin is changing the way people organize themselves. The next chapter in the story of money is being written in a new language...

Grasping Bitcoin [7]

Bitcoin seems easy to understand at first (it's just magic internet money, right?), however truly grasping its significance is a formidable task. Once you think you have Bitcoin figured out, you'll see it from another perspective and realize how little you actually knew. This pursuit of understanding Bitcoin is like a mountain climber that continually encounters false peaks, which fool him into thinking he has reached the summit, only to realize it is higher still.

It has been said that you can judge the quality and importance of an idea by the vehemence of its opposition. Bitcoin has been called many things—digital gold, tulip mania 2.0, financial revolution, the MySpace of cryptocurrencies, environmental disaster, rat poison squared, libertarian idealism, apex predator of monetary technologies, the biggest bubble in history, the model-T of cryptocurrencies, a superior species of money—but it turns out that, in context of the history and nature of money, Bitcoin appears to be a distinct evolutionary leap forward. Bitcoin is not an internet application like MySpace, it is an internet protocol. Bitcoin is not the model-T of cryptocurrencies, it is a more like a global freeway system. Bitcoin is not like any type of gold coin, Bitcoin is more like the element gold. Its integrity is protected by the inviolable laws of mathematics. Human nature is one of its core components. It is a new form of social institution. Bitcoin is a living system unto itself that adapts to environmental changes.

This may sound mind blowing at first. Most innovations of this magnitude sound this way in the beginning as we struggle to communicate using outdated terms and analogies that cannot possibly convey their importance. However, history shows us that ignoring innovation is a terrible strategy. In light of its inherent complexity and novelty, we will view Bitcoin from many different perspectives in an attempt to create a mosaic of understanding in the minds of our readers. First and foremost, Bitcoin is *digital cash money*.

Digital Cash Money [1]

As the global economy becomes increasingly digitized and interconnected, new technological realities are taking shape which will cause the market to naturally select for the most effective species of money native to this new digital terrain. Bitcoin is the first truly digital solution to the problem of money. It is the world's first digital cash (in the original sense of the word cash discussed earlier) meaning that it is under the full control of its owner and can be used for final settlement in the same way as gold is today. Put another way, Bitcoin is digital cash money, a self-sovereign asset that contains within it all the trust factors and permissions necessary to transact with it. Bitcoin is not the liability of any counterparty, hence its nickname—digital gold.

Like gold, Bitcoin is a supranational form of money, meaning that no government needs to decree its value or permit its use, nor can it be eliminated unilaterally by regulation. The hardness of Bitcoin is superior to all forms of money, including gold, and its stock-to-flow ratio will eventually reach infinity. As a digital asset, Bitcoin has unprecedented levels of salability across scales, space and time. It is resistant to confiscation, censorship, inflation and counterfeit. Meritoriously, Bitcoin's value is attained entirely from the social consensus it earns by competing freely in the marketplace.

As one perspective of its monetary significance, Bitcoin can be understood as the successful fusion of the advantages associated with physical cash payments with the efficiencies and certainties enabled by digital technology. Cash payments have the advantage of being immediate, final and requiring no trust from either counterparty in each other nor any other intermediary. The drawback of cash payments was the need for parties to be present in the same space and time, which increases risks associated with physical custody, especially for larger transactions. As more business is conducted remotely, thanks to ever-advancing telecommunications technologies like the internet, physical cash transactions become increasingly impractical.

Since the inception of computers, the nature of all digital objects is that they were infinitely replicable. This meant that no digital object could be provably limited in quantity. For instance, when you “send” an email, you are actually sending a copy, as you still have the email in your sent folder. Before Bitcoin, there was no way to send a

digital good that could not also be resented elsewhere at a later time. This presented an intractable issue for direct digital payments known as the *double-spend problem*. Without a trusted third-party intermediary to verify the payer was not double spending, digital payments were not possible. Using intermediated digital payments (like Venmo or PayPal) exposed parties to additional transaction costs, risk of censorship, fraud and transaction disputes.

The nature of digital objects also meant creating a digital cash was impossible, since its monetary units could be reproduced endlessly and would therefore suffer from unlimited inflation. Before Bitcoin, people had to rely on physical laws (rarity and chemistry, in the case of gold) or jurisdictional laws (government and central bank monopolies) to regulate money supplies. Innovatively, Bitcoin relies on mathematical laws to protect its monetary policy. Building on top of decades of innovative trial and error by other programmers and combining a wide range of proven technologies, Nakamoto successfully made Bitcoins the first digital objects that were verifiably scarce. As the world's first instance of *digital scarcity*, Bitcoin was able to solve the double-spend problem and become the world's first functional digital cash.

“That in order to make a person covet a thing, it is only necessary to make the thing difficult to attain.”

– Mark Twain

In this way, Bitcoin would bring the desirous advantages of physical cash to the digital realm and combine them with an immutable monetary policy to inoculate its holders from all unexpected inflation. Drawing on lessons learned by other programmers during two decades of attempts at this innovative breakthrough, Nakamoto finally achieved digital cash money by combining four key technologies:

- Proof-of-Work—mathematical puzzles which require energy expenditure to be solved, solutions are rewarded with newly issued Bitcoin and user transaction fees, functions as the skin in the game necessary to keep Bitcoin's distributed ledger truthful and maintain its monetary hardness
- Distributed peer-to-peer network—a record of Bitcoin's entire transaction history is maintained by each network participant (known as a node) who mathematically verify each other's work, making the entire system resistant to censorship and manipulation
- Hashing—a method of computer cryptography that transforms any stream of data into dataset of fixed size (known as a hash), this transformation is irreversible and is the foundation of trustless verification within the Bitcoin network
- Digital Signatures—a method of authentication that relies on a set of mathematically related elements called the private key, the public key and signatures—the private key (which must be kept secret) allows its

holder to control the Bitcoin associated with it, meaning that the private key is a bearer instrument (holding Bitcoin is holding its private key, which makes it a self-sovereign monetary good like gold)

In the same way a monetary assessment of gold would not delve too deep into its chemical properties, this essay will not delve too deep into the technological properties of Bitcoin. We will instead focus on its monetary properties and its relevance in the story of money. However, some basic technical knowledge of Bitcoin is warranted to fully appreciate the importance of the innovation that is digital cash money.

Technological Properties [1]

Bitcoin is *open-source software*, meaning its source code can be inspected by anyone. This makes Bitcoin a language, its source code and transaction history are universally transparent and can even be printed onto paper (interestingly, this makes it protected under the First Amendment in the United States, more on this later). As an open-source software project, Bitcoin is supported by a global network of volunteer programmers. These programmers are self-interested in the sense that they are almost always Bitcoin owners as they are aligned with its purpose philosophically, and therefore stand to gain financially from its expanding network. Their work over the years has greatly enhanced the functionality of the Bitcoin network. However, these programmers are unable to change the rules of Bitcoin (as we will see when we discuss Bitcoin's social contract).

To become a Bitcoin network member, known as a *node*, all that is necessary is to download and run the software on a computer. Once downloaded, the software will enable you to store Bitcoin and transact it with any other node in the world. Also, by becoming a node, the entire Bitcoin transaction history will be recorded on your machine and updated in perpetuity, just as it is on every other node in the world. This is the essence of Bitcoin's *decentralized architecture*. The Bitcoin network, similar to the internet, lives *everywhere and nowhere*.

Owning a Bitcoin means owning the private key that can authorize it to be used in a transaction. The private key is purely informational, meaning that it is just a string of alphanumeric characters. This makes it a self-sovereign form of money, giving its holder the presumption of rightful ownership, which makes Bitcoin an instrument of final settlement (like gold). Bitcoin is the world's first global, digital final settlement system.

Bitcoin is entirely reliant on verification, which allows its users to completely eliminate any need for trust. All Bitcoin transactions are recorded by every node on the network so that they all share one common ledger of balances and transactions (remarkably similar to the Rai Stone system used by the Yap Islanders). Transactions

are grouped together approximately every ten minutes in what is known as a *block*. Each block is then added to the previous block of transactions, forming a chronological chain of inextricably linked blocks that stretches all the way back to the genesis block mined by Nakamoto himself exactly 10 years ago today. This is commonly called the Bitcoin *blockchain*. The blockchain is the common ledger of which each node maintains its own copy (commonly known as the distributed ledger). Each node verifies the accuracy of every other node's transaction inputs and truth is established by consensus. In this way, the Bitcoin network relies 100% on verification and 0% on trust. This gives Bitcoin the unique property of *trustlessness*, meaning it is able to operate successfully without the need to trust any counterparty or intermediary whatsoever.

Blockchain, Energy and Mining [1,3,8,11]

Economic incentives and disincentives are used to maintain truthful records in the blockchain, it what is an ingenious application of the skin in the game concept. Nodes compete to solve complex mathematical puzzles in a process called *proof-of-work*. Nodes are incentivized to perform this computing task because the first one to solve the proof-of-work is awarded a batch of newly issued Bitcoin and the transaction fees generated within the latest block of transactions—called the *block reward*. A block is sealed approximately every ten minutes, which triggers the opening of the next block and proof-of-work competition. Nodes expend processing power (in the form of electricity) to solve these complicated mathematical problems, although considerably less and much more efficiently than the systems that support gold and government money today:

	Annual Cost (\$USD)	Energy Consumption (GJ)	\$USD per GJ
Gold Mining	\$ 105,000,000,000	475,000,000	\$ 221
Gold Recycling	\$ 40,000,000,000	25,000,000	\$ 1,600
Government Fiat Money Production	\$ 28,000,000,000	39,000,000	\$ 718
Banking System	\$ 1,870,000,000,000	2,340,000,000	\$ 799
Governments	\$ 27,600,000,000,000	5,861,000,000	\$ 4,709
Bitcoin Mining	\$ 4,500,000,000	183,000,000	\$ 25

Bitcoin mining is exceptionally energy efficient relative to other monetary systems and their institutions.

Proof-of-work energy expenditure is the thermodynamic bridge from the physical to the digital world. It transmutes the fundamental commodity of the universe, energy, into digital gold. This energy expenditure is essential to the functioning of the Bitcoin network, as it disincentivizes node dishonesty. If a node attempted to include a fraudulent transaction in a block, other nodes would reject it and it would incur the cost of processing power without the prospect of earning the block reward. This

process is commonly referred to as *mining* and the competing nodes are called miners (or mining nodes). Mining is a truly capitalistic voting mechanism where energy expended equals hashes, which are votes for the proof-of-work solution, generated. The name mining is an ode to the arduous process of mining of gold. As we have learned, the costs and risks related to the mining of this monetary metal is necessary for it to maintain its hardness (skin in the game). Similarly, mining using proof-of-work is the only known method of creating digital cash money.

Money, which is the representation of the work required to generate goods, can also be considered a form of stored energy. In the early 20th century, free market proponents like Henry Ford and Thomas Edison were interested in replacing gold or the US dollar with an energy money. Showing great prescience, they foresaw the day when the world may exhaust its non-renewable energy sources and be forced to switch to alternatives. Convicted in their free market beliefs, they shared this idea and assumed a great deal of reputational risk in the process, as their views ran contrary to the established economic order. The concept of energy money was popular due to its hard money characteristics, as energy is costly to produce. However, energy money was technologically well before its time, as energy could not be transmitted or stored easily using technologies of the day. In championing a novel idea with the greater good at heart, Ford and Edison were exhibiting *soul in the game*, or the exposure to downside risks on behalf of others. As Edison said in 1931:

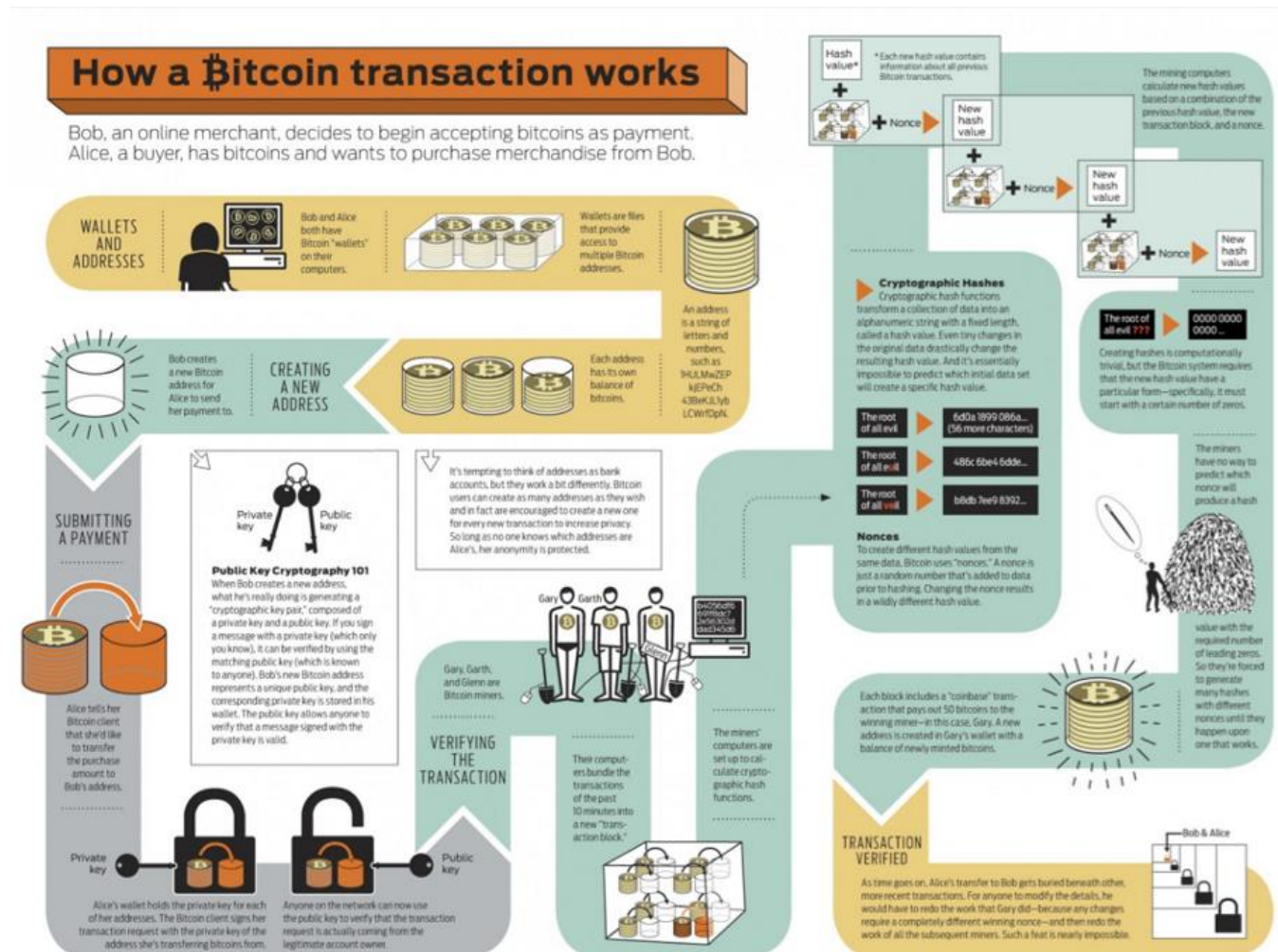
"I'd put my money on the sun and solar energy. What a source of power! I hope we don't have to wait until oil and coal run out before we tackle that."

By using proof-of-work, which was originally invented as a measure to mitigate email spam, Bitcoin became the world's first functional energy money. With physical monetary goods, we were required to build walls to safeguard our money. With the Bitcoin network, we are required to expend energy to preserve the sanctity of its ledger, secure its network and enforce the immutability of its money supply. Proof-of-work is essential for Bitcoin to function as hard, digital cash money and enables it to serve as the buyer of last resort for electricity worldwide. The Bitcoin network provides a perpetual economic incentive for everyone in the world to invent more efficient methods of harnessing energy. This global incentive will increase the rate of innovation in energy technologies. As Bitcoin expert Nic Carter puts it:

"The Bitcoin network is a global energy net that liberates stranded assets and makes new ones viable. Imagine a 3D topographic map of the world with cheap energy hotspots being lower and expensive energy being higher. I imagine Bitcoin mining being akin to a glass of water poured over the surface, settling in the nooks and crannies, and smoothing it out."

As more nodes compete to solve the proof-of-work puzzle, the difficulty automatically increases so that new blocks are added on average once every ten minutes. This automatic algorithmic change is called the *difficulty adjustment* and is perhaps the most ingenious aspect of Bitcoin. It is the most reliable engineering solution for making and keeping money maximally hard and gives Bitcoin the unique ability to adapt its network security as it grows. As we have seen, when a form of money appreciates, people are immediately incentivized to increase its new supply flow, which reduces its stock-to-flow ratio and compromises its hardness. With Bitcoin, an increase in its price does not lead to the production of more Bitcoin beyond its transparent and predictable supply schedule. Instead, it simply leads to an increase in processing power committed by miners which in turn makes the network more secure and difficult to compromise. Like a vault that becomes harder to crack the more money that is stored within it, Bitcoin offers people an incredibly effective means of value storage.

Next, we depict the entire process of a Bitcoin transaction:



The Internet of Value [9]

“The internet of value” is a popular moniker to describe Bitcoin. In reality, the Bitcoin *protocol* can be considered an integral and newly evolved layer of the commercial internet. In computer science, a protocol is a ruleset that governs the transmission of data. The internet as we know it is an integration of four successive layers of open-source protocols, called the Internet Protocol Suite, that maintain constant communication with one another:

- The Link Layer puts data packets on the wire
- The Internet Layer routes data packets across networks
- The Transport Layer persists communication across any given conversation
- The Application Layer delivers software files and applications

In this context, Bitcoin can be considered the fifth layer of the internet protocol suite:

- The Value Layer allocates scarce resources across networks

In the same way the internet is a set of open-source protocols for exchanging data, Bitcoin is an open-source protocol for exchanging value. It is trustless, as any machine can accept it from any other securely and at virtually zero cost. Bitcoin is also global and *permissionless*, meaning that any machine can speak its language and no central bank is required to authorize its use. This means that transactions on its network are essentially unstoppable as all trust factors and permissions necessary to transact with it are intrinsic to the act of holding a Bitcoin private key. Software protocol developments are being implemented that will make Bitcoin transactions even faster, cheaper, anonymous and capable of authentication. These can expand the utility of Bitcoin to enable the allocation of scarce network resources like computing power, verification of contracts or tracking identity and reputation.

Although Bitcoin is the fifth layer of the internet protocol suite, it is the base layer protocol for the value layer itself. This means that second and other higher order protocol layers may be built on top of it. A second layer protocol to Bitcoin, called the Lightning Network, is currently being implemented and is designed to sacrifice some degree of trustlessness to achieve higher transaction throughput, allowing Bitcoin to be used more effectively as a medium of exchange. The Lightning Network is an open-source protocol and functions by establishing trust channels among parties for faster, cheaper transactions that are then settled periodically to the Bitcoin blockchain. Higher order protocol development and integration is one of the many ways Bitcoin adapts to changes in its environment (more on this later).

In the same way that money is an emergent property of complex human interactions, Bitcoin is an emergent property of complex interactions occurring

between people, machines and markets. Even if Nakamoto and Bitcoin never existed, it would still be necessary for us to invent the concept of cryptoassets to enable machines to exchange value to facilitate digital economies, use smart contracts and provide the substrate necessary for the 'internet of things' to come into existence. Not only is Bitcoin a prerequisite innovation to the digital economy, it is also the hardest monetary technology ever invented.

The Infinite Hardness of Bitcoin [1]

Bitcoin is the hardest form of money in existence. Its money supply is enforced mathematically and, like the other rules of Bitcoin, cannot be broken or changed. Only 21 million Bitcoins can and will ever exist:

$$\frac{\sum_{i=0}^{32} 210000 \left\lfloor \frac{50 \cdot 10^8}{2^i} \right\rfloor}{10^8}$$

The monetary policy of Bitcoin is set in (mathematical) stone.

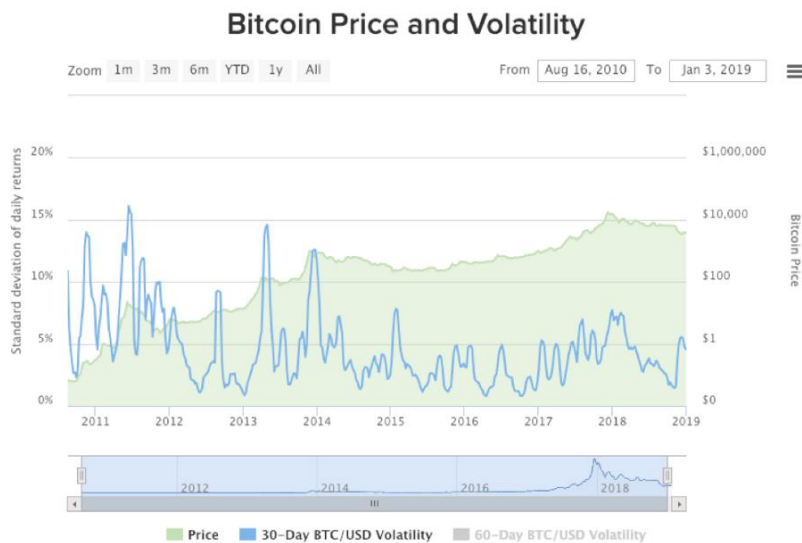
This strictly limited supply makes it the first monetary technology exhibiting *absolute scarcity*. Unlike gold and other monetary metals, no matter how much demand for Bitcoin increases there will never be any units produced in excess of its fully transparent, predictable and unchangeable monetary policy.

Before Bitcoin, only time itself had achieved the property of absolute scarcity.

Since increased demand for Bitcoin cannot affect its supply, it can only be expressed in its price. Bitcoin has perfect *price inelasticity of supply*, meaning that it has zero supply-side response to increases in its price. Unlike gold and all other physical commodities, where an increase in demand will inevitably lead to larger supplies being produced over time, Bitcoin can only express an increase in demand by becoming more expensive (and a more secure network). A perfect price inelasticity of supply no doubt contributes to the notorious price volatility of Bitcoin it is exhibiting at the earliest stages of its growth we are witnessing today.

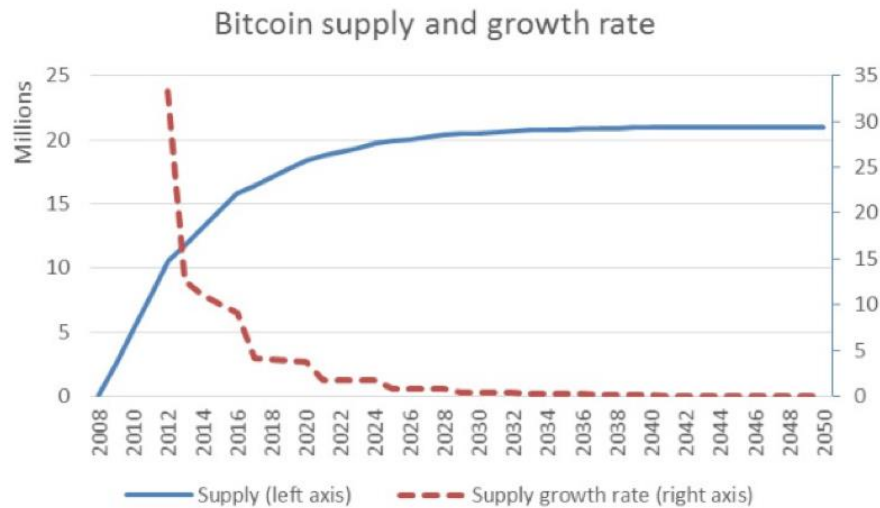
Absolute scarcity greatly exacerbates Bitcoin's price volatility. As its network continues to grow, the value of Bitcoin as an unstoppable payments channel and uninflatable money is steadily increasing over time while its price is constantly attempting to find it, dramatically overshooting and undershooting along the way. With a totally inflexible supply schedule, as long as Bitcoin is growing quickly, its price will behave like that of a startup company stock undergoing meteoric growth. Should Bitcoin achieve sufficient market penetration that its growth slows down, it would stop attracting high-risk investment flows and become a stable monetary asset expected to appreciate slightly each year as demand increases due to

productivity and population growth—like any mature hard money should. As expected, over the long-run we are already seeing a decrease in Bitcoin's price volatility:



As expected, the price volatility of Bitcoin is gradually declining as its network value grows.

Bitcoin's immutable monetary policy ensures that its supply will continue to grow at a decreasing rate and will reach its maximum of 21 million units sometime in the year 2140. To maintain salability across scales, Nakamoto designed each Bitcoin to be further divisible into 100 million units, which are now commonly called Satoshis in his honor. Once the last Bitcoin is mined, its stock-to-flow ratio will become infinite as its flow will completely and irreversibly cease. Beyond this point, miners will be compensated exclusively by transaction fees. Bitcoin's decreasing growth rate means that the first 20 million coins will be mined by the year 2025, leaving the last 1 million to be mined over the subsequent 115 years:

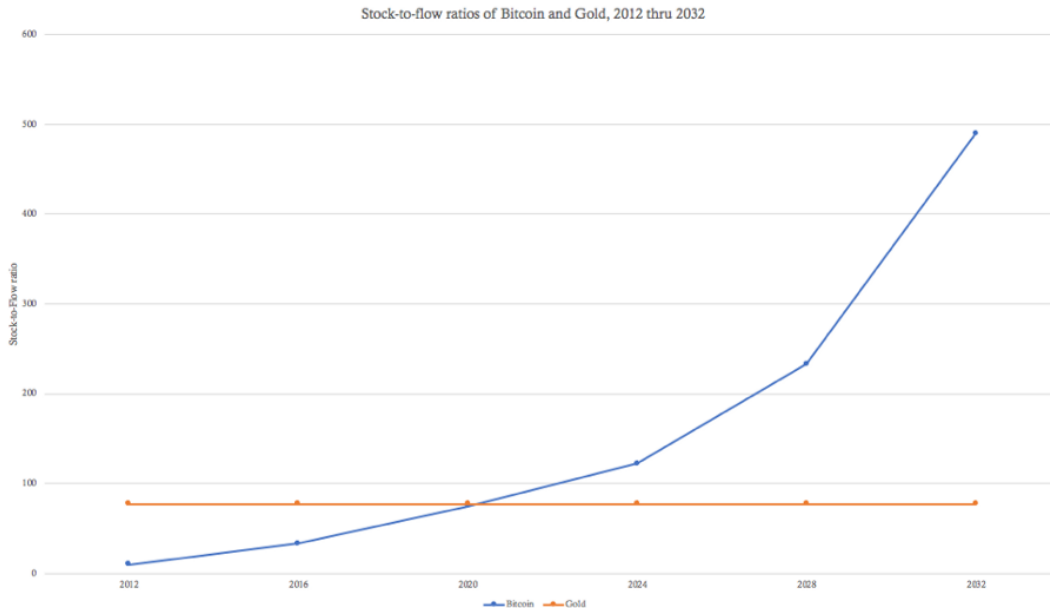


Due to its decreasing supply growth rate, over 95% of all Bitcoins will be mined by the year 2025.

This predictable, transparent and immutable supply schedule gives Bitcoin a significant advantage as it competes for the trust of the people to become a reliable store of value. Unlike government money or even gold, people know with absolute certainty that Bitcoin will never have its salability across time compromised by unexpected supply increases.

Bitcoin is uninflatable money in a world where wealth is continuously stolen via inflation.

As is the case with its other immutable laws, Bitcoin's monetary policy is enforced by the inviolable laws of mathematics. Inevitably, Bitcoin will surpass gold around the year 2020 to become the hardest form of money in history:



As sure as $1+1=2$, Bitcoin will soon surpass gold to become the hardest form of money in history.

By virtue of its natively digital nature, Bitcoin is (critically) highly resistant to centralization. As we have learned, it was the centralization of gold that led to government money backed by gold, which made gold more salable across scales and encouraged a gold standard to flourish throughout most of the world. However, as the temptation to expand money supplies seems to be irresistible for humans, governments soon took control of the banking sector, printed money in excess of its gold reserves, eventually severed their currencies peg to gold and thereby destroyed the hardness of government money completely.

Historically, people who adopted hard money systems flourished—such as the Romans under Caesar, The Byzantines under Constantine and the Europeans under the gold standard—and people who had the hardness of their money compromised suffered enormous consequences—such as the Yap Islanders, West Africans using glass beads and the Chinese under a silver standard in the 19th century. Moving a society away from a hard money system has been a harbinger of economic crisis and societal decay, an outcome that can be explained as a social contract rescission.

Bitcoin's Social Contract [10]

Social contract theory starts with an assumed hypothetical state of nature full of violence that is unbearable for people to live in. Driven by a desire to improve their circumstances, people come together and collectively agree to sacrifice some of their freedoms to establish a *social contract* and empower an institution to protect them. Government is the result of a social contract: people sacrifice some of their freedoms

to give the state control over the monetary system and armed forces. The state, in turn, uses that power to manage the economy, redistribute wealth and fight crime. In the United States, our current social contract grants the government monopoly control of money (via the Federal Reserve) and violence (via the Police and Military).

Similarly, money itself can be thought of as a social contract. If enough people are unhappy with a barter economy, they can collectively agree to use money instead. This social contract entails sacrificing certainty (requiring trust that dollars will maintain their value over time) in exchange for convenience (using dollars as a medium of exchange). The social contract for money, as we have seen, emerges and evolves spontaneously based on market-driven natural selection. Each person continuously decides which outcomes they prefer and how best to achieve them. If enough people seek the same outcome, we call the result a social contract.

Throughout history, almost every government (a form of social contract) put in charge of the monetary system (another, often interrelated, form of social contract) has abused its power by forcibly confiscating assets, censoring private transactions and printing money to steal wealth via inflation. Using the virtually unlimited financial means provided by control over money supplies, these governmental social contracts grew in successive bureaucratic layers. The larger and more valuable these social contracts became; the more freedoms were forfeited and the more others sought control over them. This led to many instances of conflict (warfare or social revolution) in which old social contracts (dictatorships or tyrannical regimes) were rescinded in favor of new ones (new laws, treaties or governments). The principal point here is that people can agree they are in a terrible situation and come together to change it, but the resultant social contract is only as strong as its credibility and enforceability.

The invention of Bitcoin can be regarded as a new implementation of the social contract for money. Nakamoto settled on the following rules for this new implementation:

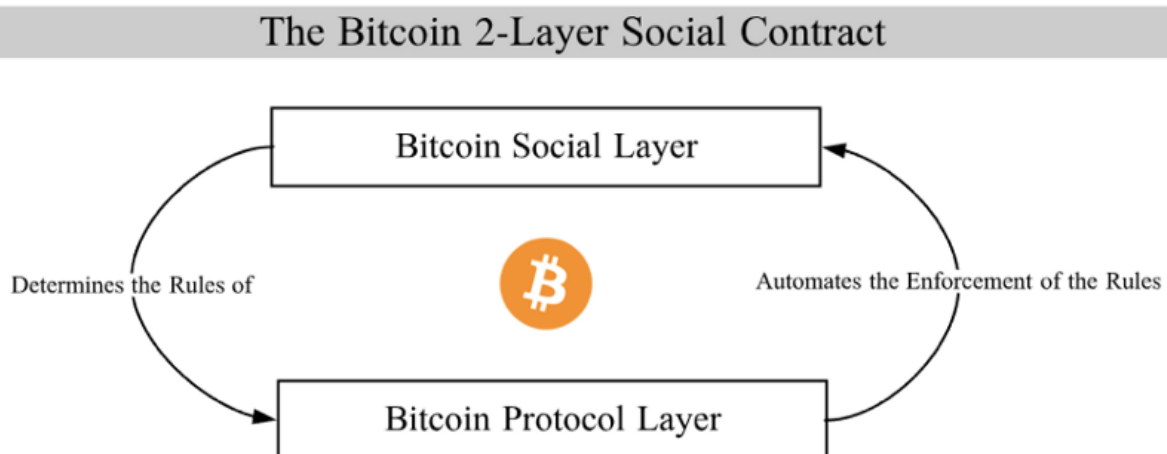
- Only the owner of a Bitcoin can produce the digital signature to spend it (confiscation resistance)
- Anyone can transact and store value in Bitcoins without permission (censorship resistance)
- There will only be 21 million Bitcoins, issued on a predictable schedule (inflation resistance)
- Anyone will always be able to verify all the rules of Bitcoin (counterfeit resistance)

Historically, social contracts intended to protect people, such as governments and their central banks, eventually became controlling and ultimately turned abusive. When a social contract loses sufficient trust of the people, it falls apart or is

overthrown, by ballot or by bullet. This dynamic has resulted in a continuous cycle of rising and falling social contracts throughout history. Bitcoin is intended to break this cycle in two ways:

- Instead of seeking security from a powerful central entity (like a government or central bank) that can be corrupted or overthrown, Bitcoin creates a hypercompetitive market for its own protection. It turns security into a commodity and the security providers (miners) into harmless commodity producers.
- By requiring its security market participants (miners) to incur real world costs to generate their economic reward (skin in the game), Bitcoin incentivizes the market to reach consensus over who owns what at any given point in time.

In this sense, the Bitcoin social contract is composed of two distinct, self-reinforcing layers: the social layer and the protocol layer. The social layer is the social consensus itself, which determines the rules of Bitcoin and establishes its value. The protocol layer simply automates the enforcement of the rules set by the social layer:



In this sense, Bitcoin is more than just a technology. Indeed, it is a new institutional form. Viewing it in this way, we are better able to answer some of the more existential questions about Bitcoin:

Who Can Change the Rules of Bitcoin?

Since the rules of the Bitcoin social contract are decided at its social layer and enforced at its protocol layer, who can actually change its rules? Bitcoin, as computer network, comes into existence when people run implementations that follow the same ruleset (think of these rulesets as speaking the same language). You remain in the network by following the same rules as everyone else. If you decided to change the ruleset on your local computer, you would simply be evicted from the network

(you no longer speak the same language as everyone else). Your unilateral decision to change the rules would not impact the actual Bitcoin network in any way whatsoever.

The only way to change the rules of the Bitcoin social contract is to convince people to voluntarily accept your proposed rule changes at the social layer. As each network member is self-interested, they will only adopt rules that benefit them. Seeing as its current rules are already optimal for Bitcoin holders (resistance to confiscation, censorship, inflation and counterfeit) it would be extremely difficult to convince a majority of the approximately 30 million network participants to change rulesets. This asymmetrical governance dynamic virtually rules out any contentious changes from succeeding, as they would never get broad social consensus. Therefore, the Bitcoin network can be upgraded in ways that align with the collective best interests of its members and is at the same time highly resilient to changes that contradict these interests.

Can a Software Bug Kill Bitcoin?

In September 2018, a software bug arose in the main implementation of Bitcoin that opened up two potential attack vectors which theoretically could have been exploited to circumvent its counterfeit and inflation resistance properties. Bitcoin developers quickly fixed the bug before either vector was exploited, however this event left many people wondering what would have happened had the vulnerabilities not been discovered in time.

Any time the social layer and protocol layer diverge in the Bitcoin social contract, the protocol layer is always wrong. Again, all rules are set at the social layer whereas the protocol layer is only responsible for automating their enforcement. Had the software bug not been discovered in time, Bitcoin's blockchain would have undergone a *fork*—meaning its protocol layer would have been split it into two networks, one with the bug and one without it. Every Bitcoin holder would then have an equal number of coins in each network, but the value of these coins would be determined solely by the free market. This is true for all forms of money, as social consensus determines the value of money. At the social layer, each Bitcoin owner would then choose either the implementation with or without the bug. To protect the value of their Bitcoin, holders would rationally choose to migrate to the mended network and its blockchain would continue without interruption.

When the Bitcoin protocol layer successfully automates the enforcement of the rules determined at its social layer, the two layers are in sync. If they diverge for any reason, the social layer supersedes, and the protocol layer is mended to reflect the economic reality of the social consensus surrounding Bitcoin. Software bugs are inevitable, and Bitcoin's 2-layer social contract construction ensures that it can withstand them.

Can Forks Compromise the Immutability of Bitcoin's Rules?

Since Bitcoin is open-source software, anyone in the world can copy its code, change it and launch their own version. This is also a chain fork which, as established earlier, affects only the protocol layer of the Bitcoin social contract. Without changing the rules at the social layer first, a protocol layer fork only evicts you from the true Bitcoin network. To successfully change the rules of Bitcoin, you must successfully fork its social layer first. To accomplish this, you would need to convince as many people as possible that your proposed ruleset is meaningfully better for them, so that they take the risk of adopting your proposed software changes. Forks like these are difficult to pull off in reality because they require buy-in from thousands of people to be successful. This asymmetry between the cost of campaigning for ruleset changes and their potential benefit to network participants makes the Bitcoin network exhibit an extremely strong status quo bias when it comes to governance.

The key to understanding this is that the value of any form of money is purely a social construct or, in other words, is derived from social consensus. Individual Bitcoins, like US dollars or any other currency, receive their value exclusively from the shared belief of their users. Forking Bitcoin's protocol layer is worthless without forking the social layer from which it derives its value. In the rare cases that the social layer itself splits, as was the case with the Bitcoin Cash fork, the result is two weaker social contracts, each agreed upon by fewer people than before. The complete failure of the Bitcoin Cash fork (its price has declined from 0.21 to 0.04 Bitcoin over the past year) is yet another battle scar for Bitcoin that pays testament to its governance model and exemplifies the winner take all dynamics inherent to monetary competition.

So long as Bitcoin network participants continue to act in accordance with their own individual self-interest, the rules of Bitcoin (resistance to confiscation, censorship, inflation and counterfeit) are immutable and, therefore, as reliable as the laws of mathematics. It's clear from this perspective that Bitcoin is more than just a technological innovation. Although Bitcoin as a network and monetary technology is groundbreaking in many respects, its social contract implementation is revolutionary. Bitcoin is the first technology that incorporates human nature as one of its core moving parts.

In essence, by believing that mathematics and individual self-interest will persist, we can reliably believe in Bitcoin's value proposition and its ongoing successful operation.

Over the past 10 years, by inventively aligning human self-interest with its own self-interest, the Bitcoin network has managed to grow organically from \$0 to \$80B in value.

A New Form of Life [1]

Although Bitcoin is intended to be a monetary technology, it is a totally unique compared to other forms of money. Ralph Merkle, famous cryptographer and inventor of the Merkle tree data structure, has a remarkable way of describing Bitcoin:

"Bitcoin is the first example of a new form of life. It lives and breathes on the internet. It lives because it can pay people to keep it alive. It lives because it performs a useful service that people will pay it to perform. It lives because anyone, anywhere, can run a copy of its code. It lives because all the running copies are constantly talking to each other. It lives because if any one copy is corrupted it is discarded, quickly and without any fuss or muss. It lives because it is radically transparent: anyone can see its code and see exactly what it does.

It can't be changed. It can't be argued with. It can't be tampered with. It can't be corrupted. It can't be stopped. It can't even be interrupted.

If nuclear war destroyed half of our planet, it would continue to live, uncorrupted. It would continue to offer its services. It would continue to pay people to keep it alive.

The only way to shut it down is to kill every server that hosts it. Which is hard, because a lot of servers host it, in a lot of countries, and a lot of people want to use it.

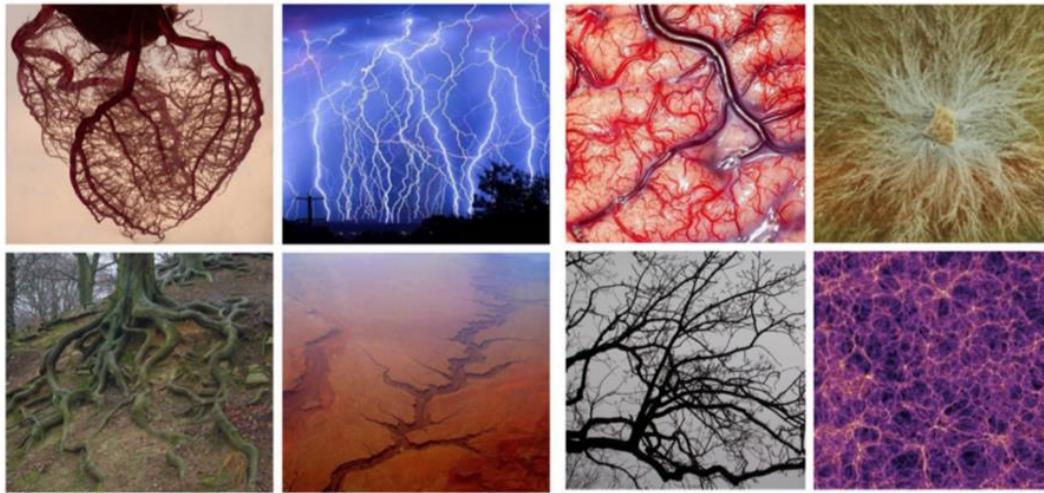
Realistically, the only way to kill it is to make the service it offers so useless and obsolete that no one wants to use it. So obsolete that no one wants to pay for it, no one wants to host it. Then it will have no money to pay anyone. Then it will starve to death.

But as long as there are people who want to use it, it's very hard to kill, or corrupt, or stop, or interrupt."

Bitcoin is a technology, like the hammer or the wheel, that survives for the same reason any other technology survives: it provides benefits to those who use it. It can be understood as a spontaneously emergent protocol that serves as a new form of uninflatable money and an unstoppable payments channel. Structurally, the Bitcoin network reflects a quintessential manifestation commonly found in nature.

The Decentralized Network Archetype [7]

The Bitcoin network mirrors one of the most successful evolutionary structures found in nature, the *decentralized network archetype*:



Clockwise from the top left: the human heart, lightning, the human brain, a fungal mycelium network, roots from a tree, an aerial view of the Grand Canyon, branches from a tree and a cosmic web of galactic superclusters in the deep Universe (which is the largest observable structure in the known Universe at over 1 billion lightyears across).

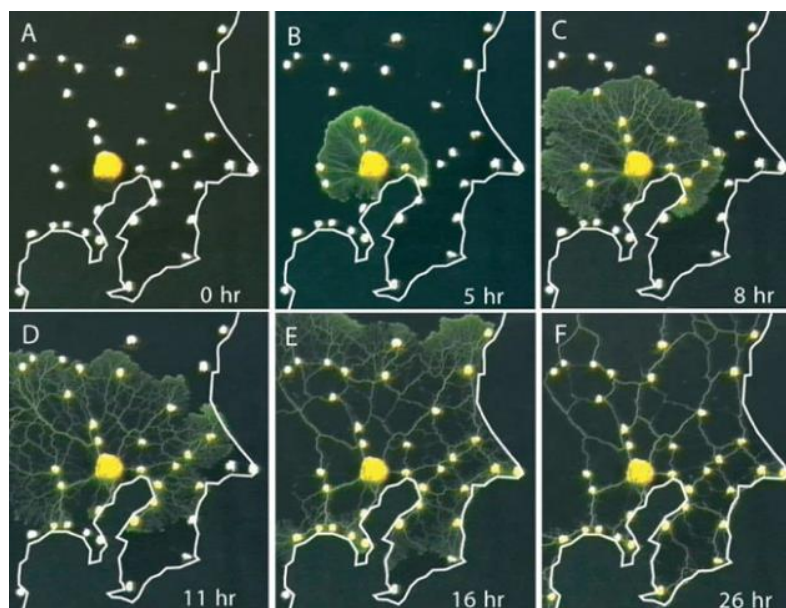
The decentralized network archetype is prevalent in nature because it is one of the most energy efficient structures possible. Energy is the fundamental commodity of the universe and nature always optimizes for its utilization. Atoms, bubbles and stars (in a state of equilibrium) always form spherical shapes, which is the most energy efficient form for minimizing surface area, precisely because they are energy conservation structures. Minimal surface area output per unit of energy input ensures that these structures optimally expend the finite energy of which they are composed. Spheres are figures of equilibrium with equal distribution their own inherent energy.

Conversely, decentralized networks always form in these tendrilled, circuitous and redundant shapes, which is the most energy efficient form of maximizing surface area, precisely because they are energy exchange structures. Maximal surface area output per unit of energy input ensures that these structures achieve the highest degree of spatial exposure to optimize the likelihood of successful exchange—whether their purpose is pumping blood, imbibing groundwater or seeking sunlight. Spheres and decentralized networks are antithetical in purpose and archetype. Decentralized networks are figures of disequilibrium which both disperse and gather energy within their environments. A decentralized form in organic systems confers

advantages such as distributed intelligence, invulnerability to singular attack vectors and accelerated adaptivity.

The decentralized network archetype found in nature is the antecedent to paradigm shifting innovations throughout history such as the railroad system, the telegraph, the telephone, the power distribution grid, the internet, social media and now Bitcoin.

To illustrate the power of this natural archetype, let's consider the story behind the design of the Tokyo subway system. Scientists conducted an experiment where an ancient fungus, the slime mold, was incentivized to recreate the Tokyo subway system. Each subway stop (node) was marked with oat flakes, the favorite food of the slime mold. In a single day, the slime mold grew to connect all the subway stops in a more energetically efficient design than that proposed by the central planning committee of engineers who spent many months at great expense to the Japanese government in the design process:



As the Scientists later reported:

*“Transport networks are ubiquitous in both social and biological systems. **Robust network performance involves a complex trade-off involving cost, transport efficiency, and fault tolerance.***

Biological networks have been honed by many cycles of evolutionary selection pressure and are likely to yield reasonable solutions to such combinatorial optimization problems.

Furthermore, they develop without centralized control and may represent a readily scalable solution for growing networks in

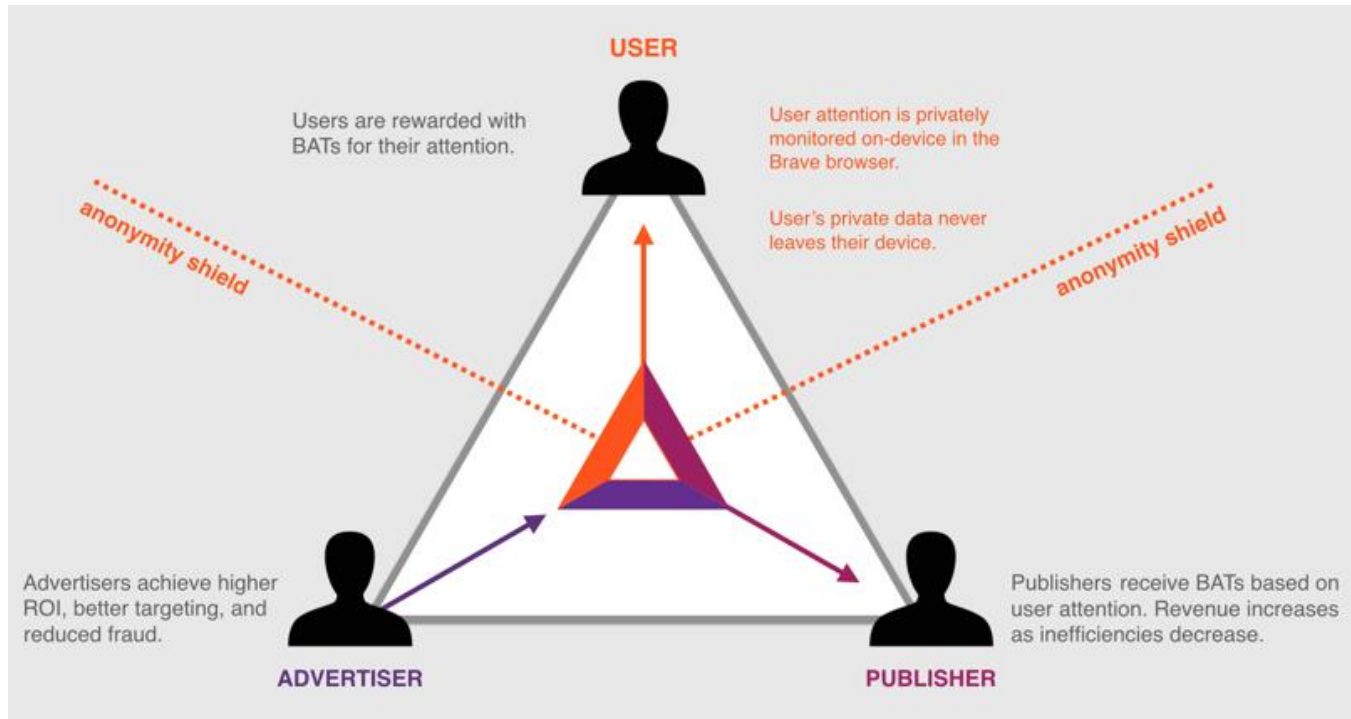
general. *We show that the slime mold *Physarum polycephalum* forms networks with comparable efficiency, fault tolerance, and cost to those of real-world infrastructure networks — in this case, the Tokyo rail system. The core mechanisms needed for adaptive network formation can be captured in a biologically inspired mathematical model that may be useful to guide network construction in other domains."*

In a similar vein, Bitcoin and its network participants receive signals from the market to create features that satisfy unmet demands or improve the functionality of its network. When block space demand exceeds capacity, as it did in late 2017, transaction fees spike and encouraged the development of a second layer protocol to increase transaction throughput (the Lightning network discussed earlier). As rent-seeking businesses, like Western Union, continue charging exorbitant fees for international remittances, market demand shifts to Bitcoin's much more cost effective and permissionless payment channel. When governments crack down on Bitcoin exchanges, trading volume on peer-to-peer exchanges like LocalBitcoins.com flourishes. To enhance Bitcoin network accessibility, Blockstream launches satellites that provide global coverage for node synchronization. The Bitcoin network is constantly adapting to optimize for its own expansion and the interconnectedness of its participants. Perhaps Bitcoin is less so digital gold, and more so digital slime mold (just kidding, or am I?).

In most forms of life, genes are only passed from parent to offspring in a process called *vertical gene transfer*. Certain fungal networks, which are modeled after the decentralized network archetype, are able to steal competitive advantages directly from physical contact with other similar organisms in a process called *horizontal gene transfer*. These fungal networks can grow to gargantuan sizes—indeed, the largest organism on Earth, at nearly 4 kilometers across, is a honey fungus in Oregon that is slowly consuming an entire forest. Fungal networks live in constant competition as they fight off predators, pests and pollutants. This environmental stress causes them to naturally synthesize a variety of enzymatic and chemical countermeasures and, when one of these measures is successful, it is stored in the distributed mind of the entire fungal network. The next time it encounters a menace for which it has even once synthesized an effective countermeasure, the fungal network will use it to neutralize the threat, no matter where the latest encounter occurs. Amazingly, these fungal networks are capable of absorbing countermeasures created by competitors in the same ecosystem purely from physical contact. Such organisms exhibit distributed intelligence, meaning they learn at the edges and distribute the lessons throughout their vast networks.

There is a common misconception that an alternative cryptoasset could develop a superior feature that will eventually outcompete Bitcoin. Similar to certain fungal

networks, Bitcoin is able to subsume features that have been proven in the marketplace from cryptoasset competitors. For example, an alternative cryptoasset called Basic Attention Token (BAT) is designed to power an internet browser called Brave that allows users to shield themselves from advertisements:



BAT is a cryptoasset designed to allow web browser users to monetize their own attention. Using a set of open-source software extensions, today you can perform browser-based microtransactions similar to BAT but using Bitcoin instead. This effectively eliminates the need for a cryptoasset like BAT. The capacity of Bitcoin to subsume market-proven features from competitive cryptoassets fortifies it from disruption.

Brave users are then given the option to open their browsing sessions up to advertisements and are paid in BAT for their attention. This blockchain-based digital advertising solution is intended to allow users to monetize their own attention, whereas in most browsers advertising revenues are allocated mostly to the content publishers. Given Bitcoin's open-source nature, it is able to absorb competitive features like this in a process similar to horizontal gene transfer. Today, by using the Lightning Joule browser extension and running a full Bitcoin node, you can perform browser-based microtransactions similar to BAT but using Bitcoin instead. This effectively eliminates the need for a cryptoasset like BAT. Further, the technologies combined to make Bitcoin all came from previous attempts at digital cash, reiterating the point that open-source software is amenable to feature absorption.

This ability accelerates the adaptivity of the Bitcoin network and insulates it from competitive disruption which further reinforces its position as the market leader.

Antifragility [1,11]

Seeing the ubiquity of the decentralized network archetype throughout nature in this way makes the invention of decentralized digital money seem less novel and more inevitable. An open and decentralized nature also enables Bitcoin to benefit from adversity. In light of its track record, Bitcoin is an excellent incarnation of Nassim Taleb's concept of *Antifragility*:

"Wind extinguishes a candle and energizes fire... Some things benefit from shocks; they thrive and grow when exposed to volatility, randomness, disorder and stressors and love adventure, risk and uncertainty. Yet, in spite of the ubiquity of the phenomenon, there is no word for the exact opposite of fragile. Let us call it antifragile. This property is behind everything that has changed with time: evolution, culture, ideas, revolutions, political systems, technological innovation, cultural and economic success, corporate survival, good recipes, the rise of cities, legal systems, equatorial forests, bacterial resistance... even our own existence as a species on this planet."

Fragility can be defined as sensitivity to disorder, whereas robustness is insensitivity to disorder. Antifragility is a property of anything that benefits from disorder, stress or adversity. The many failed attempts at killing Bitcoin thus far have only made it stronger by drawing attention to attack vectors or vulnerabilities that its global team of self-interested, volunteer programmers can then fix. These improvements have only increased the network's operational efficiency. Also, each time it withstands an external attack or a chain fork (as we are witnessing with the abject failure of Bitcoin Cash), its reputation for network security and immutability is strengthened. The resiliency of Bitcoin is hardened by hostility.

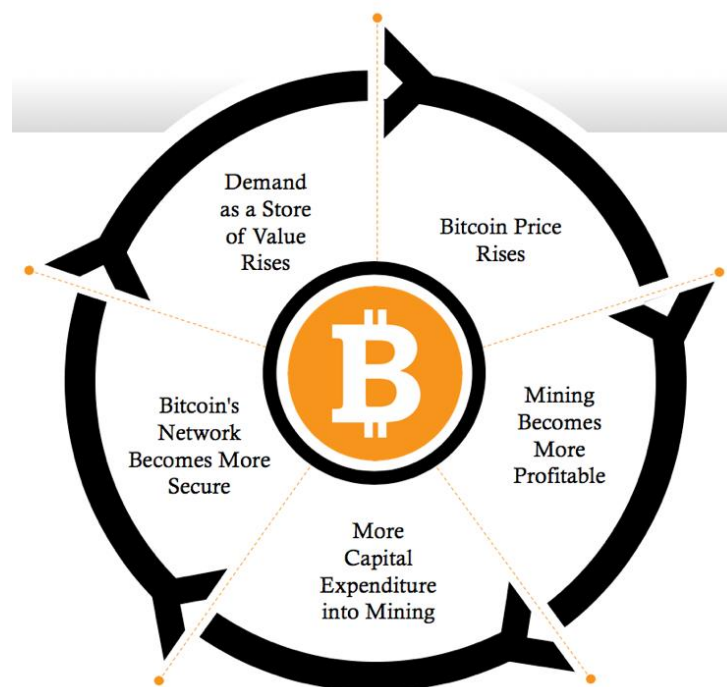
As Bitcoin has fluctuated wildly in price over the years, each new crash has triggered widespread declarations of its demise. Over 330 prominent articles declaring the death of Bitcoin, known as Bitcoin obituaries, have been written over the past 10 years. These publicity attacks on Bitcoin brought it to the attention of ever-wider audiences. As obituaries intensified, Bitcoin's network processing power, transaction volume and market capitalization all continued to ascend relentlessly—a confirmatory example of the saying 'all publicity is good publicity'.

When China took a heavy-handed approach to regulation by shutting down Bitcoin exchanges in 2017, we witnessed several informal exchanges and OTC markets appear following the demise of each centralized exchange. Although the liquidity for

Bitcoin was negatively impacted initially, soon transactions started happening off exchange in China, with volume on websites like localbitcoins.com exploding. The regulatory attack also encouraged people to hold Bitcoin for longer periods, as evidenced by a steep decline in sell volumes, which only reduced the amount of Bitcoin being traded and put upward pressure on its price. Also, these regulatory actions backfired by triggering the *Streisand Effect*, which is a phenomenon whereby an attempt to hide, remove or censor information has the unintended consequence of publicizing the information more widely, usually facilitated by the internet. As the world watched the situation in China unfold, both the Bitcoin price and global internet searches for the term Bitcoin reached new all-time highs.

Bitcoin's Positive Feedback Loop [1,4]

All of the adversity Bitcoin has faced so far has only fed its growth. Absent any top-down authority, Bitcoin is organic in the sense that it has grown from the bottom-up based solely on its own merits as money. Bitcoin perpetuates the expansion of its network and maintains truthful records by relying on asymmetric economic incentives that make fraud far costlier than its potential rewards. Network participants are all rewarded economically for their interactions with Bitcoin, which creates a flywheel effect on its price and network security:



Bitcoin autonomously proliferates its network by economically rewarding everyone who interacts with it.

As the Bitcoin network adapts to better meet the demands of its constituents, it in turn recruits more network participants. This positive feedback loop promotes the sustained growth of its network and fuels powerful, multi-sided network effects.

Bitcoin's Network Effects [1,4,5]

Bitcoin's meteoric growth has been both supported and protected by its unique multi-sided network effects. The basic example of a powerful 1-sided network effect is a social network (or a telephone network, as outlined earlier). The more people on a social network, the more valuable it is for others to be on it, as there are exponentially more possible connections. It can, however, be disrupted by a competitor that provides a more valuable service to its single customer cohort, the users, who might then transition to the new service (as happened when Facebook disrupted MySpace).

Successful 2-sided markets (like eBay or Craigslist) are significantly more difficult to disrupt. Consumers want to be there because merchants are there, and merchants want to be there because consumers are there. To disrupt a 2-sided network, you have to simultaneously introduce a superior value proposition for both parties, otherwise nobody moves. That is why Craigslist, despite its limited innovation over the years, has been able to leverage its early 2-sided lead and is still a dominant website today.

Bitcoin has a unique 4-sided network effect that insulates it from disruption and supports its growth. These are the four constituencies that participate in expanding the value of Bitcoin as a result of their own self-interested interaction with its network:

- Consumers who pay with Bitcoin
- Merchants who accept Bitcoin
- Nodes that maintain the distributed ledger
- Developers and entrepreneurs who are building onto and on top of Bitcoin

This 4-sided network effect makes Bitcoin's first mover advantage seemingly indomitable. As an adaptive monetary technology, its network effects encompass the liquidity of its market, the number of network participants, the community of software developers who support it and Bitcoin's brand awareness. Large investors will always seek the most liquid market for ease of entry and exit. Consumers, merchants and developers tend to join the largest of each of their respective Bitcoin communities, which only reinforces their social interconnectivity and cohesion. Brand awareness is innately self-reinforcing, as any cryptoasset competitor will inevitably be mentioned in comparison to Bitcoin.

An aside on Bitcoin's brand awareness: As we have learned, the value of any money is derived from its social consensus, or the mutual beliefs of its users. The notion of a "believer" has religious connotations, as the notion of one having an epiphany once the "truth" is revealed. Such religious undertones are prevalent in most forms of money (In God We Trust on the US Dollar) and they are also part of Bitcoin's aura (The Genesis Block, Bitcoin Evangelists). The most important of these quasi-religious ideas is the mythological bedrock Nakamoto laid with his enigmatic appearance in 2008 and then with his mysterious disappearance 3 years later. Whoever he/she/they were, Nakamoto gave Bitcoin its *creation myth*. As market strategist Nicolas Colas said:

"In business, creation stories reinforce the role of the individual as a societal agent of change and speak to a core audience of customers. They are the bedrock for what marketers call a brand and the source waters for Wall Street's shareholder value."

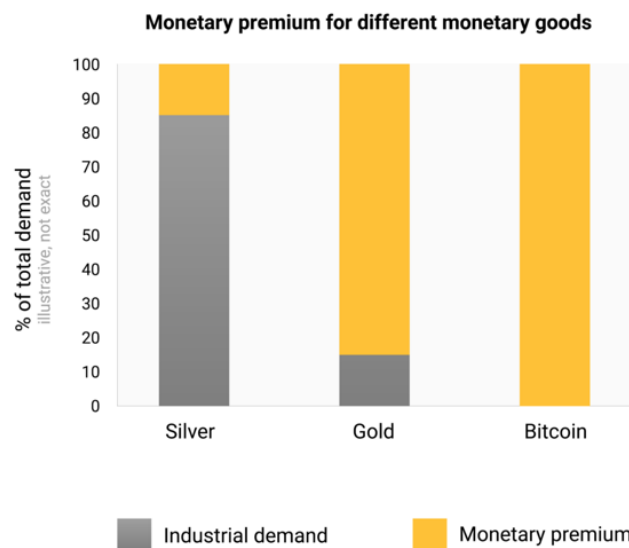
Assuming Nakamoto was a lone wolf, it is arguable that his disappearance transformed him from a person into a mythological figure. This mystery fuels the brand awareness of Bitcoin and reinforces its quality of decentralization, as there is no single individual to vilify, denigrate or otherwise target in an attempt to tarnish Bitcoin's symbolism. Like a super hero with a secret identity, all we have is the icon of Nakamoto as a cryptic genius—the godhead of Bitcoin.

As we have learned, the value of a network is a reflection of the total number of possible connections it allows. Therefore, each new Bitcoin owner increases the value of the Bitcoin network, which benefits all existing owners. This new owner is then incentivized to evangelize the benefits of Bitcoin to others, creating the next wave of new owners, and the cycle continues. As the price increases, so too do the incentives to secure the network which draws in more capital expenditure from miners, making Bitcoin's network effects even stronger and self-reinforcing as price appreciation reflexively energizes Bitcoin's positive feedback loop outlined earlier.

Since money is a social network, the price of a monetary good is a reflection of how widely adopted it has become or is expected to become. The price of a monetary good in excess of its industrial demand is its *monetary premium*. This is the only rational basis for the common criticism that Bitcoin is a bubble, as it is purely a monetary technology and has no industrial demand whatsoever. However, this premium is the defining characteristic of all forms of money, as all monetary value is based on the optionality it gives its user for exchange across scales, space and time.

Actual bubbles occur when price exceeds fair value, such as the market distortions created by central bank monetary manipulation. However, some mistake monetary premia for bubbles since they cause prices of monetary goods to exceed their underlying industrial values. If monetary premia are bubbles, then money is the bubble that never pops. Paradoxically, in this sense a monetary technology can

presently be both a bubble and significantly undervalued if it later achieves widespread adoption:



As a pure bred monetary technology, Bitcoin derives none of its value from alternative uses.

Although there is no established price pattern for a digital good that is becoming monetized, Bitcoin's price appears to follow a fractal (a recursive, self-similar shape) wave pattern of increasing magnitude commensurate with its level of user adoption. The volatility of this price pattern is exacerbated by Bitcoin's perfect price inelasticity of supply (as discussed earlier). Each iteration of the *fractal wave pattern* appears to match the standard shape of the *Gartner hype cycle*, which provides a graphical and conceptual representation of emerging technologies undergoing five phases of maturation:

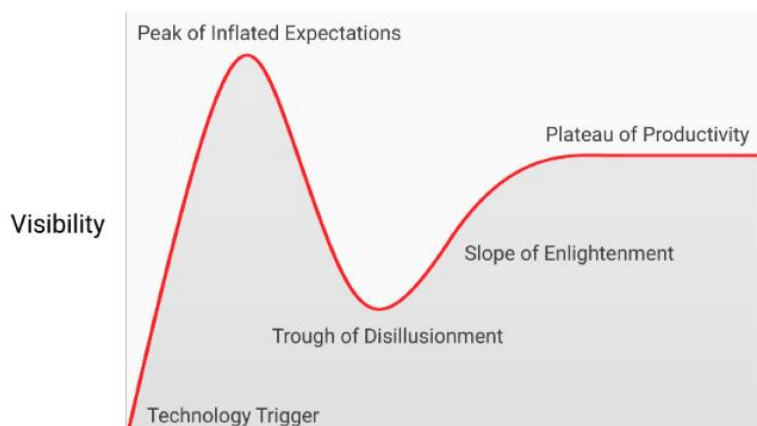


Figure 1 Bitcoin's price appears to follow a fractal wave pattern based on the archetypal Gartner hype cycle.

Bitcoin's growth, in terms of price and transactions, has been dramatic to say the least. Indeed, it is the fastest growing asset in history. Its price has gone from \$0.000994 on October 5, 2009, in its first recorded transaction, to about \$4,000 today—a total increase of over 400,000,000% in 10 years. By its 10th birthday, Bitcoin had processed about \$1.38T USD worth of transactions, with USD value calculated at the time of each

transaction. Here we show Bitcoin's entire price history, from a logarithmic perspective, with the Gartner hype cycle fractal wave pattern iterations located inside boxes:



Figure 2 Bitcoin is the fastest growing and most volatile asset in history, although both are leveling off as it grows.

These extreme price cycles draw in new Bitcoin owners as each fractal wave crests. Some of these new owners buy in near the peak, only to be crushed in the trough. Most will capitulate, but those who remain because of their long-term conviction in Bitcoin (typically the most studious of history and monetary evolution among them) become the newest *hodlers of last resort*. Hodl, which began as a chat room typo in the early days of Bitcoin, has morphed into a memetic phrase that denotes “hodling” Bitcoin long term without regard to its price volatility. Layers of these stubborn hodlers have been added throughout each of Bitcoin’s four major price cycles. A good proxy for the depth of these layers is the lowest price Bitcoin hits each year, which indicates the rising collective obstinacy of these hodlers:

Lowest Bitcoin Price Points 2012-2018

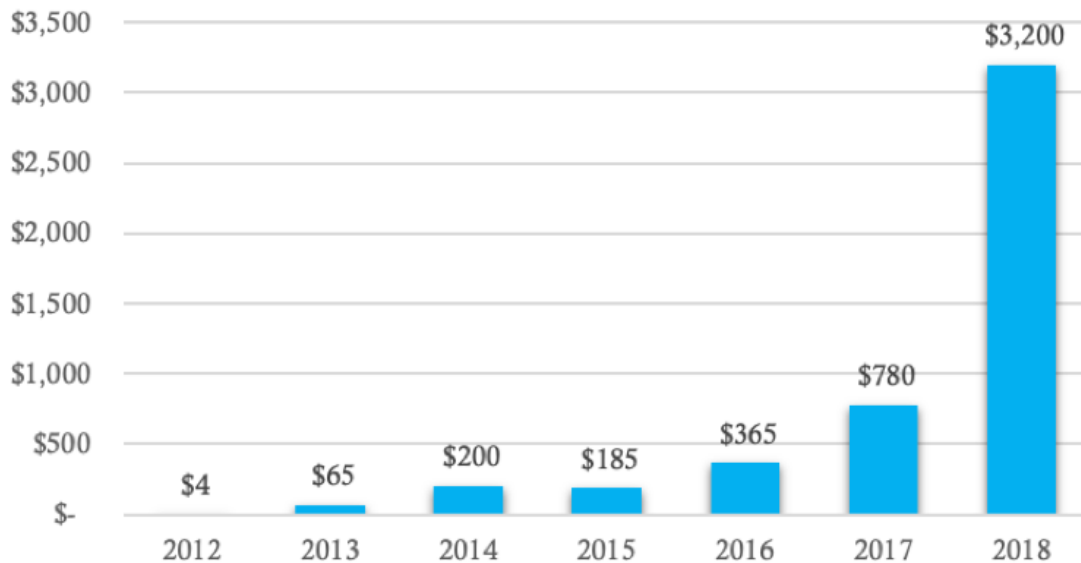


Figure 3 The annual low prices of Bitcoin provide an effective proxy for the collective intransigence of its hodlers.

These layers form the base for the next iteration of each fractal wave pattern. As more observers recognize the survivability of Bitcoin following each price crash, they realize that investing in it may not be as risky as they once thought. This larger base of believers sets the stage for the next iteration of the fractal wave pattern which will support a much larger set of newcomers at a far greater magnitude of peak price. Few people are able to accurately predict how high prices will go in each fractal wave cycle, and they usually reach levels that would seem absurd to most investors at the earliest stages of the cycle. The best proxy for the timing of these fractal wave patterns has been the quadrennial Bitcoin inflation rate adjustment, when the amount of new Bitcoin rewarded at the close of each block is reduced by half, an event commonly known as the *halving*. Historically, Bitcoin achieves a new all-time high price within 18 months of its last halving. The next halving will occur in May 2020:

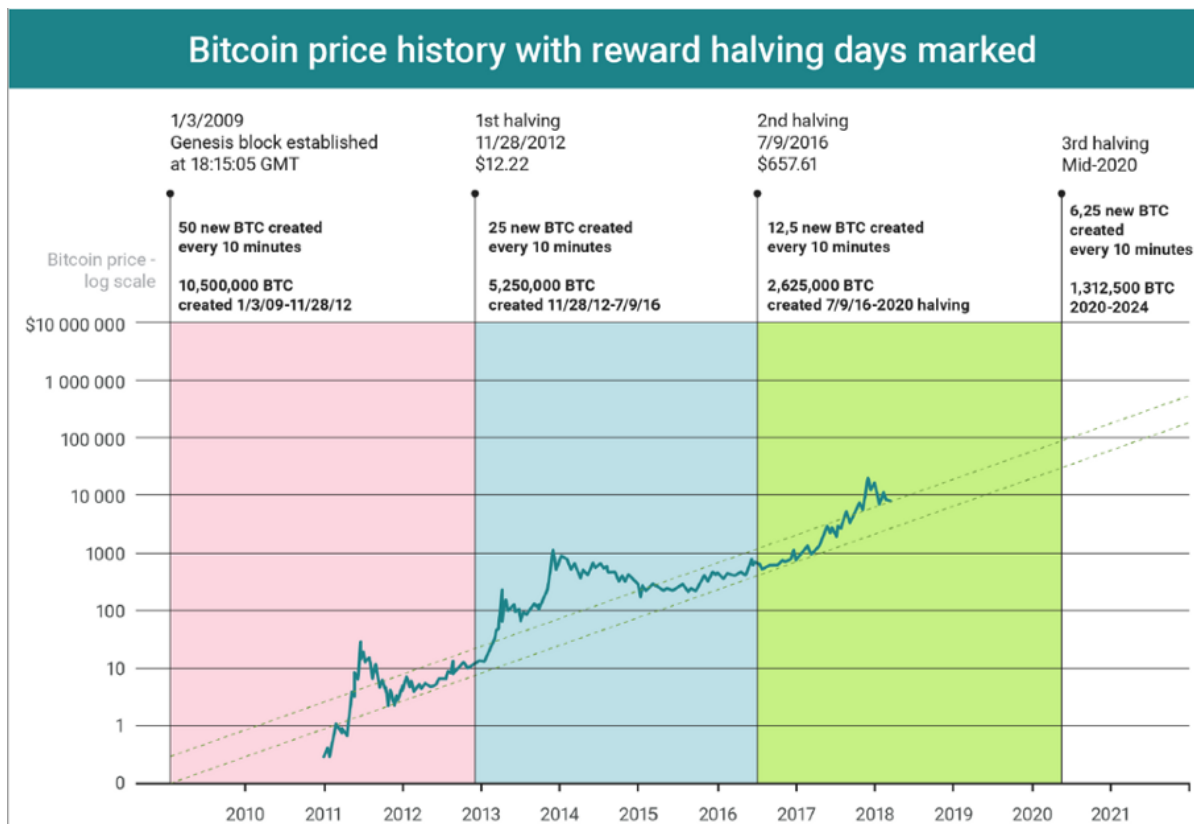


Figure 4 Every four years, the Bitcoin supply growth rate is cut in half. Each halving also cuts the Bitcoin sell pressure from miners in half and creates upward pressure on its price. Historically, this quadrennial event is the best proxy for the timing of Bitcoin price fractal wave patterns.

The fractal wave patterns inevitably crescendo and begin to crash, usually attributed to myriad factors by mainstream media. However, the Gartner Hype cycle is an archetypal market pricing pattern that is driven entirely by human psychology, game theory and the ultimate exhaustion of market participants reachable in each iteration. The magnitude of each cycle is exacerbated by Bitcoin's absolutely fixed supply schedule, as increases in demand are expressed exclusively through its price, which historically leads to market frenzies at each peak. The long game for Bitcoin, and its final fractal wave pattern, will begin when and if central banks begin accumulating it as a reserve asset (more on this later). In this way, the bedrock of the Bitcoin network's expansion is the intransigency of its hodlers of last resort. Although they constitute a small minority of the whole, these stubborn hodlers will contribute to ongoing Bitcoin adoption in a meaningful way.

Minority Rule [3]

When it comes to group preferences, certain types of minorities—those who stubbornly insist on a particular preference—that constitute even a small level of the total population (often less than 4%) can cause the majority to submit to their

preferences. Another clever concept from Nassim Taleb, called the *minority rule*, is the result of complex system dynamics, like those inherent to human interaction.

The nature of complex systems (society) is that the collective behaves in a way not predicted by its individual constituents (people). The interactions between its constituents matter more than their individual natures. Studying individual ants will never give us an idea on how the ant colony operates. For that, one needs to understand an ant colony as an ant colony, not just a collection of ants. This is called an emergent property of the whole. In other words, the whole is more than the sum of its parts because what matters is the interactions between the parts. These interactions, while complex, can obey simple rules, like the minority rule (or the rule that barter economies settle on a medium of exchange or that the hardest form of money always outcompetes). Many domains are impacted by the minority rule such as:

- **Markets**—Market prices are not the consensus of market participants, but instead reflect the activities of the most motivated buyers and sellers. In 2008, a single \$50B order, less than 0.2% of the stock market's total value of about \$30T, caused the market to drop by almost 10%, causing losses of around \$3T. The order was activated by the Parisian Bank Société Générale who discovered a hidden trade by a rogue trader and wanted to reverse the purchase. The market reacted disproportionately because there was only a desire to sell and no way to change the stubborn seller's mind.
- **Science**—Similar to markets, science is not the consensus of scientists, it is the minority body of knowledge remaining after removing disproven hypotheses.
- **Law**—A law abiding citizen will never commit criminal acts but a criminal will readily engage in legal acts, and criminal behavior has been shown to be contagious within certain social groups.
- **Imports**—In the United Kingdom, where the (practicing) Muslim population is only around 4%, a very high proportion of the meat we find is halal (or Kosher). Close to 70% of lamb imports from New Zealand are halal. The same population and import proportions hold true in South Africa (the case of imports is closely related to the example below).

Today, in the United States and Europe, companies are selling more and more non-GMO food precisely because of the minority rule. Given the possibility of food containing GMOs, food not bearing the label "non-GMO" may be assumed by some to contain GMOs which, according to the minority, contain unknown risks. People who eat GMO food will readily eat non-GMO food, but not the reverse. Assuming the price and distribution costs differences between GMO and non-GMO are sufficiently small and the intransigent minority is distributed somewhat evenly throughout the population, this will have the effect of disproportionately increasing the demand for

non-GMO food in the long run. This dynamic of scale can be explained quantitatively. In mathematical physics, renormalization groups are an apparatus that allow us to see how things scale up or down.

Here we show how the minority rule can renormalize the preferences of the majority.

STEP 1



Our graphic depicts:

- Three vertically-stacked large boxes, each representing one sequential step in the minority rule renormalization process

STEP 2



- Four medium boxes in each step, each representing a family of four

- Four smaller boxes contained within each medium box, each representing an individual member within each family of four

STEP 3



Assume that in Step 1, the daughter in the family of four is the intransigent minority (the small pink box) who eats only non-GMO food. As we move to Step 2, the group renormalizes as the stubborn daughter manages to impose her rule on her three family members (who are now all pink) as they are flexible on the matter and consistency simplifies their grocery shopping and

administrative process. In Step 3, the family of four goes to a backyard barbecue attended by three other families. As their family is known for their strict eating habits, the host will only serve non-GMO food as the other families are flexible and consistency simplifies the food preparation process, thereby making all four families (which are now all pink) adopt the minority rule originally set by the intransigent daughter in Step 1.

This minority rule will continue imposing and proliferating itself as these families attend other social events, which gradually shifts customer preferences in the neighborhood and eventually causes the local grocery store to switch to non-GMO foods to simplify its procurement processes, which impacts the local wholesaler, and so on up the supply chain. The real world result of this dynamic is the preferences of 4% of a population (practicing Muslims) driving the market preferences of 70% of their respective populations (in the UK, New Zealand and South Africa). As we can see, the minority rule spreads by interaction and renormalizes the entire group to conform with its preferences. Its proliferation is accelerated if there are incentives to switch, low switching costs or anticipated future benefits from switching (as superiorly hard digital cash money, Bitcoin offers all three). In this example, a

minority constituting 6.3% of the total population imposed its rules on the majority using pure intransigence. In reality, the minority rule often takes effect when minorities become 4% or less of the total population.

Languages also often adhere to the minority rule. For instance, French was originally intended to be the language of diplomacy as civil servants from aristocratic backgrounds used it, while English was reserved for those engaged in commerce. In the rivalry between the two languages, which are still considered two of the international languages (a third, Spanish, was added later because of its widespread use), English won as commerce came to dominate modern life. This gives us some intuition as to how the emergence of *Lingua Franca* languages, those commonly spoken across cultures, can come from minority rules. As Taleb puts it:

“Aramaic is a Semitic language which succeeded Canaanite (that is, Phoenician-Hebrew) in the Levant and resembles Arabic; it was the language Jesus Christ spoke. The reason it came to dominate the Levant and Egypt isn’t because of any particular imperial Semitic power or the fact that they have interesting noses. It was the Persians –who speak an Indo-European language –who spread Aramaic, the language of Assyria, Syria, and Babylon. Persians taught Egyptians a language that was not their own. Simply, when the Persians invaded Babylon they found an administration with scribes who could only use Aramaic and didn’t know Persian, so Aramaic became the state language. If your secretary can only take dictation in Aramaic, Aramaic is what you will use. This led to the oddity of Aramaic being used in Mongolia, as records were maintained in the Syriac alphabet (Syriac is the Eastern dialect of Aramaic). And centuries later, the story would repeat itself in reverse, with the Arabs using Greek in their early administration in the seventh and eighth’s centuries. For during the Hellenistic era, Greek replaced Aramaic as the lingua franca in the Levant, and the scribes of Damascus maintained their records in Greek. But it was not the Greeks who spread Greek around the Mediterranean — Alexander (himself not Greek but Macedonian and spoke a different dialect of Greek) did not lead to an immediate deep cultural Hellenization. It was the Romans who accelerated the spreading of Greek, as they used it in their administration across the Eastern empire.”

There is an asymmetry that those who do not have English as their first language usually know basic English, but native English speakers knowing other languages is less likely. If a meeting is taking place in an international office in say, Istanbul, among twenty executives from a sufficiently international corporation and one of the

attendees does not speak Turkish, then the entire meeting will be run in English (the commercial Lingua Franca). This is the minority rule in action.

Money is an emergent property, as it is an expected result of complex human interactions within a barter economy. Similar to language, it is a means of expression, only it is used to express value instead of information or emotion. The US Dollar is the Lingua Franca of money today, as it belongs to one of the world's largest economies (an economy which also happens to effectively control the global banking system).

As the digital age matures and the world becomes increasingly interconnected, ever-more commerce and administration will be conducted over the internet. Also, fully interconnected trade networks will level the terrain of commerce and increase free market competition among different forms of money. Considering the significant market lead already enjoyed by Bitcoin, its superior hardness, its multi-sided network effects, the impotency of capital controls on digital cash and the winner take all dynamic inherent to monetary competition; it's likely that Bitcoin will continue to outcompete and its adoption rate will increase. By considering the application of the minority rule to adoption of Bitcoin in the digital age, we can reasonably expect the following:

- Once a sufficient minority of the world's population, say 4% or less, have realized the advantages of hard money and digital cash money, their intransigent hoarding of Bitcoin will drive its price upward (Gresham's Law) and begin imposing itself economically on all other holders of money in the world. This will put downward price pressure on government fiat money, further accelerate Bitcoin's adoption rate and drastically improve Bitcoin's chances for global acceptance over the long run.
- As the first natively digital form of cash money, Bitcoin will become the Lingua Franca of digital commerce and the dominant value exchange protocol, thereby capturing nearly all the value transacted online (e-commerce alone is estimated to be nearly \$5T annually by the year 2021) over the long run.
- Bitcoin may also become the base layer for other tools of cryptographic certainty in commerce, such as smart contracts and TrustNet applications (more on these later).

The minority rule is based on a fundamental asymmetry between the intransigence of the minority and the flexibility of the majority. The minority rule shows us that a small number of unyielding people with skin or soul in the game can change the shape of the majority. Bitcoin already has the advantage of being the hardest form of money ever invented, and its rules are immutable, which is the highest form of intransigency possible. It also has unrivaled brand awareness, fed by the mystery of its creation myth, and the support of free market fanatics all over the world. Once its

obstinate minority reaches a certain size, the unbreakable rules of Bitcoin will begin to stubbornly impose themselves on the established economic order. In the words of Margaret Mead:

“Never doubt that a small group of thoughtful, committed citizens can change the world; indeed, it’s the only thing that ever has.”

A Superior Species of Money [1,4,12]

Bitcoin also introduces three new traits of money never before seen—censorship resistance, adaptivity and programmability. Censorship resistance means that no group or individual in the world can stop payments made on its network. Bitcoin gains censorship resistance by virtue of its decentralized architecture. Adaptivity refers to the ability for Bitcoin’s network to become more secure as it stores more value, its open-source nature which aligns the incentives of its global team of volunteer programmers with its own to ensure it is always up to date with state-of-the-art software enhancements and its ability to subsume features from competitors that have been proven in the marketplace. Programmability refers to the digital nature of Bitcoin and its ability to interface with smart contracts and other decentralized applications. As we have learned, the free market for money is a competitive environment that is shaped by continuous market-driven natural selection; as a competitor in this domain Bitcoin is a superior species:

Money is a social technology used to solve a problem which has persisted for all of humanity's existence: how to move economic value across time and space. Competition is at all times alive between different forms of money, subject to market-driven natural selection.

Traits of Money	Gold	Government Money	Bitcoin
Fungibility (interchangeable units)	High	Medium	High
Hardness (stock-to-flow ratio)	Medium	Low	High
Portability	Medium	High	High
Durability	High	Medium	High
Divisibility	Low	Medium	High
Security (cannot be counterfeited)	Medium	Medium	High
Easily Transactable	Low	High	High
Scarcity (predictable supply)	Medium	Low	High
Self-Sovereign (permissionless)	High	Low	High
Government Issued	Low	High	Low
Decentralized (censorship resistant)	Low	Low	High
Smart (adaptive & programmable)	Low	Low	High

The technology that is enabling Bitcoin to compete effectively in the market for money is also being applied to create new markets or disintermediate other existing markets. In technical parlance, the Bitcoin network is the world's first decentralized application. A decentralized application is a service that no single entity owns or operates. It is a new form of software and human organization that eliminates single points of failure, resists external attacks and reduces the need for intermediaries. Decentralized applications are enabled by cryptoassets. In the same way corporate equities serve companies and government bonds serve nations, cryptoassets serve decentralized applications. Owning a cryptoasset (like Bitcoin) is the only way to own a piece of a decentralized application (like the Bitcoin network). Technically, a cryptoasset is a cryptographically protected digital token representing rights within an economic network. A cryptoasset is to a decentralized application what oil is to an engine; it provides functionality and liquidity for the network and its constituents. A defining feature of cryptoassets and decentralized applications, and arguably their most alluring, is their organic nature; they are not centrally owned, governed or developed—making them highly resistant against censorship and manipulation.

Bitcoin (the OG cryptoasset) is superior in the market for money because it possesses all the ideal features of digital cash money and enjoys a market dominant position by virtue of its serendipitous first mover advantage which is fortified from disruption by

its open-source design and multi-sided network effects. With the invention of Bitcoin, the world finally has a synthetic form of money with a stock-to-flow ratio that is guaranteed to increase (until it reaches infinity) and an unstoppable, permissionless payments channel. Its digital nature makes it salable across space in a way never before seen, as it can be stored in the human mind and transmitted at the speed of light. The deep divisibility of each Bitcoin into 100 million Satoshis makes them supremely salable across scales. Its informational and nonperishable nature, when considered in combination with its superior hardness, gives Bitcoin unprecedented salability across time. This design makes it an impeccable store of value. Finally, by eliminating all intermediary control (which is inherent to government money) Bitcoin resists debasement, censorship and confiscation. It removes the central banks, macroeconomists, politicians, presidents, dictators and military leaders from monetary policy and payments authorization once and for all. The masterful book (from which much of this essay adapted) titled “The Bitcoin Standard” by Saifedean Ammous sums up Bitcoin’s historical relevance nicely:

“If the modern world is ancient Rome, suffering the economic consequences of monetary collapse, with the dollar our aureus, then Satoshi Nakamoto is our Constantine, Bitcoin is his solidus, and the Internet is our Constantinople. Bitcoin serves as a monetary lifeboat for people forced to transact and save in monetary media constantly debased by governments... the real advantage of Bitcoin lies in it being a reliable long term store of value, and a sovereign form of money that allows individuals to conduct permissionless transactions.”

Bitcoin is a tool for freedom. As the most accessible asymmetric bet in history, Bitcoin is also a unique investment opportunity.

Investing in Bitcoin [1,5,13]

Investing is all about taking intelligent risks. As Daniel Kahneman, a Nobel Prize-winning psychologist, describes it:

“Intelligent risks are based on wide and voracious data gathering checked against gut instinct; while dumb decisions are built from too narrow a base on inputs.”

Bitcoin is often referred to as digital gold, in reference to its hardness, self-sovereignty and as an instrument for final settlement. Following this analogy, there will only be one digital equivalent to gold (due to winner take all dynamics inherent to the free market for money), and if you were going to bet on which one will succeed you’d want to bet heaviest on the biggest (due to its deep liquidity and multi-sided

network effects), most renowned (due to the minority rule) and the longest lived (due to the Lindy Effect, more on this later). As people tend to think by analogy, this comparison to gold mostly works well, although it is incomplete.

As we have seen, Bitcoin is a far superior monetary technology to the golden inert metal. Technologically, Bitcoin needs little to no protocol improvement to continue to compete effectively in the market for money. There are no unsolved computer science problems standing between Bitcoin and its widespread adoption. Therefore, its primary aim is to remain extant as digital cash money, hence its minimal level of protocol functionality and the status quo bias it exhibits in relation to governance. By merely existing, Bitcoin provides a gateway for people to opt out of the prevailing inflationary monetary order. As long as it continues to operate successfully in its current form, Bitcoin will function healthily as the stateless base money protocol for the digital age—which makes it a viable contender in the \$100T market for global money:

Relative Market Sizes of Government Fiat Money, Gold and Bitcoin as of January 3, 2019

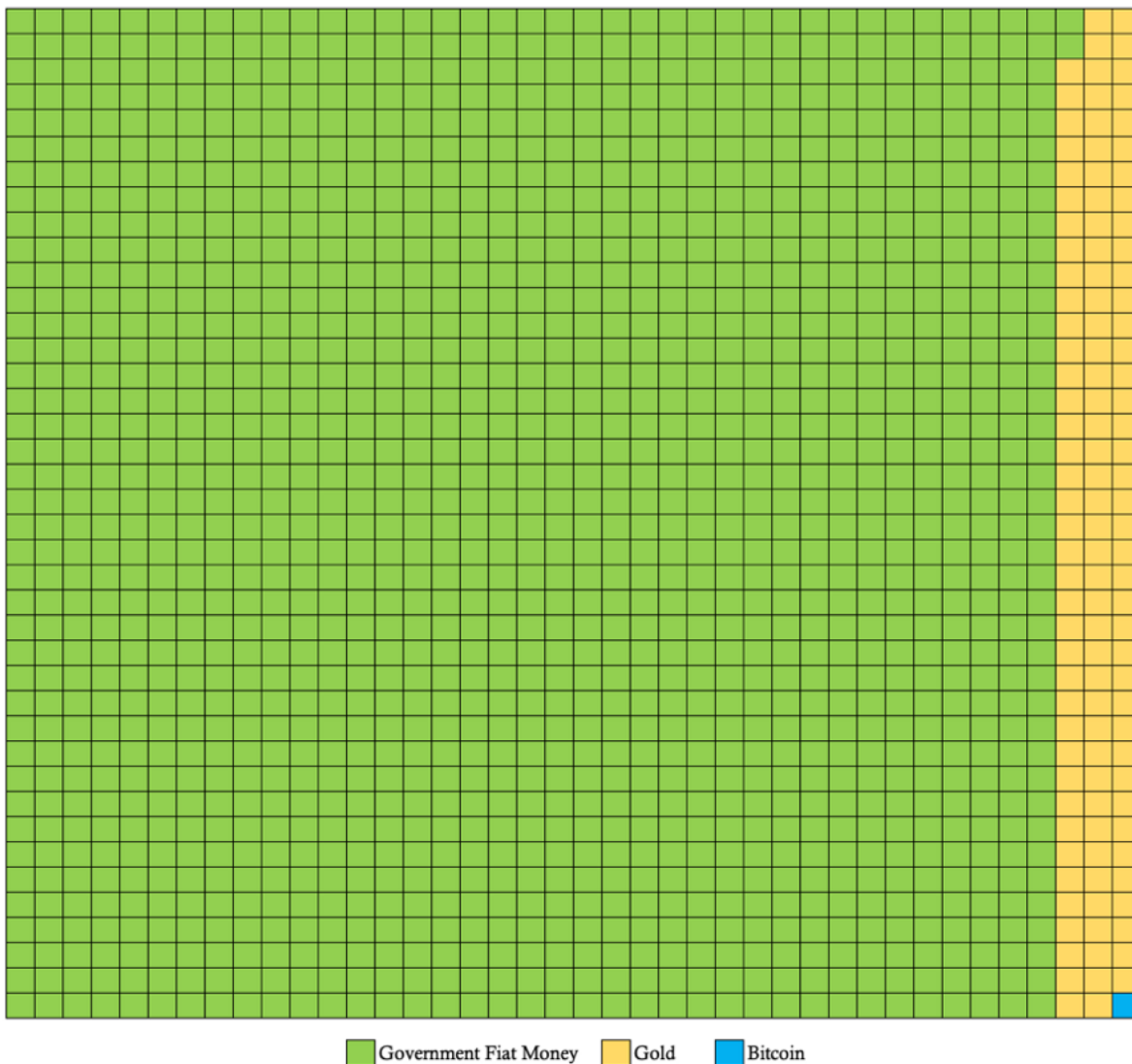


Figure 5 Bitcoin is competitively superior to both gold and government fiat money, and has plenty of room to grow.

Since it is still extremely small relative to its total addressable market, which consists mostly of gold and government fiat money, Bitcoin still has room to grow by orders of magnitude in both its network size and price. Like a call option, a bet on Bitcoin is asymmetric, meaning that an investor's downside is limited to 1x whereas their potential upside is 100x or more. Should Bitcoin achieve a majority share of the global market for money, its level of demand will become far more predictable and steady, leading to a stabilization in its price.

Investing in Bitcoin can be considered a bet on its adoption as an uninflatable, politically neutral store of value and as an unstoppable, permissionless payments channel.

Bitcoin may also become part of a much bigger wave of innovation. Although the Bitcoin network and the decentralized applications it has inspired are poorly understood by most today (similar to the internet in the early 1990s) we believe that the world will gradually awaken to the paradigmatic shift that is underway for money and markets in general. The greatest wealth is created by being an early investor in innovation. Making such investments requires believing in something before the majority of people understand it—which also often entails enduring mockery, ridicule and criticism for your non-consensus perspective. As Mark Yusko, one of my favorite hedge fund managers, describes the coming crypto era:

“Technology follows 14-year innovation cycles. These began with the Mainframe in 1954, then the Microchip in 1968, the Personal Computer in 1982, the Internet in 1996 and most recently the Mobilenet in 2010. As a result of the innovations introduced by Bitcoin, soon we will christen 2024 as the dawn of the Trustnet.”

The *TrustNet* can be thought of as the dawn of trustworthy computing. In theory, it will enable new technologies such as the internet of things, decentralized autonomous organizations, self-owning commercial assets, decentralized internet provisioning, decentralization of energy distribution, reputation markets, computing power markets, stateless identity, immutable media, AI-run organizations, token curated registries, prediction markets and circles of trust. This anticipated innovation wave is consistent with a multi-decade cycle of information technology expansion, consolidation and commoditization:

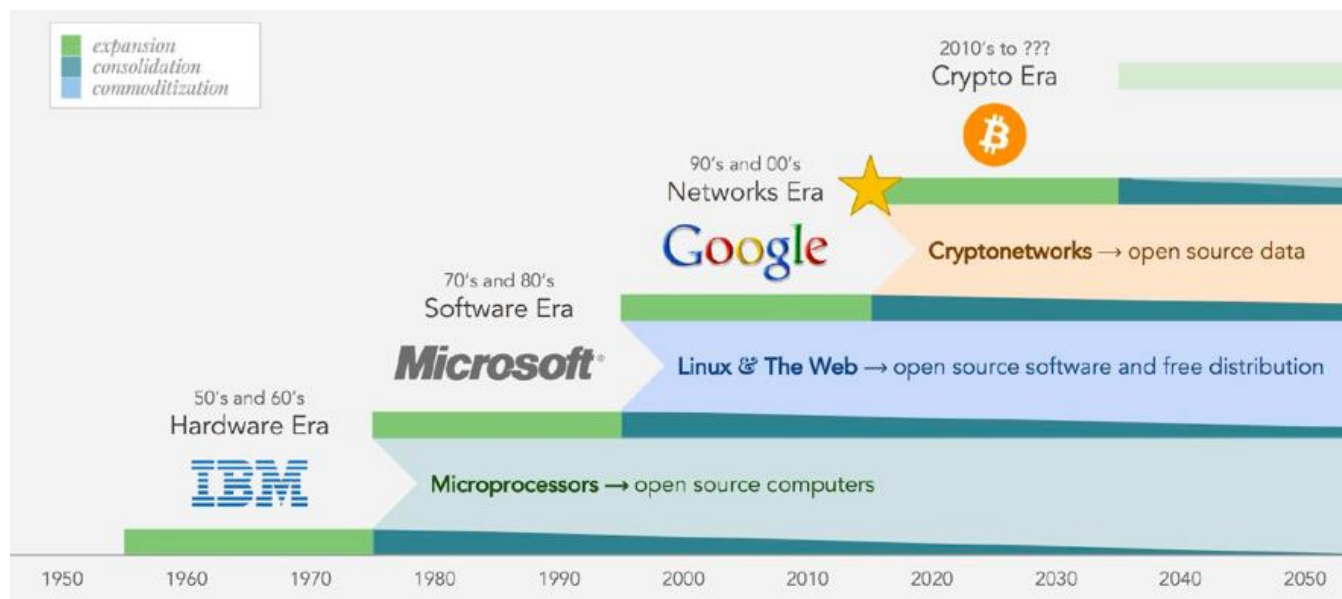


Figure 6 As innovations in information technology age, they inevitably become commoditized and create the bedrock upon which future waves of innovation are built.

Bitcoin, as the original and driving force of this innovation expansion cycle, will likely function as the systemic core and base money system of the Trustnet. During this cycle, all markets that are enabled by this technology will likely rely on the Bitcoin blockchain as a common value system, final settlement mechanism and temporal anchor point.

A Momentous Innovation [1,4,5,7,8,10]

Bitcoin is a momentous innovation of the digital age. As such, it has many unique characteristics, properties and capabilities never before seen in a monetary technology:

- Immutable Monetary Policy—Predictable, transparent and unchangeable money supply schedule. The most critical aspect to outcompeting in the free market for money, as people will naturally come to favor the hardest form of money available to them (uninflatable money).
- Digital Scarcity—Necessary to solve the double-spend problem and bring the speed and finality of physical cash settlement into the digital realm.
- Absolute Scarcity—The only asset in the world which has an absolutely finite supply, like time itself.
- Global Final Settlement System—A permissionless, unstoppable payments system with zero counterparty risk (like gold, only digital) that can be used to quickly and efficiently provide finality of settlement across scales and space.
- Self-Sovereign Network—A self-sovereign monetary good (an informational bearer instrument) whose network operates autonomously in full accordance with its own immutable rules as reliably as the laws of mathematics.
- Stateless Money—The first globally connected payments system that is politically neutral. Possible catalyst for the separation of money and state over the long run.
- Revolutionary Social Contract Implementation—A unique 2-layer social contract implementation that decentralizes power among its constituents and creates a hypercompetitive market for its own network security. A new form of social institution.
- Global Consensus—Perhaps the only truly objective set of facts in world history, its distributed ledger is created by converting processing power into indisputable truth.
- Global Energy Buyer of Last Resort—Enables anyone in the world to convert excess electricity into digital gold on demand. A perpetual

incentive for everyone in the world to develop more energy efficient innovations.

- A New Form of Life—Feeds on human self-interest and electricity to provide uninflatable money, an unstoppable payments channel and immutable governance.
- Adaptive Security—By virtue of the mining difficulty adjustment, as more value is stored on its network, the network adapts to become more secure.
- Adaptive Functionality—As an open-source software project, programmers around the world are constantly improving Bitcoin's codebase, however it is up to the users to adopt these changes, which creates a governance equilibrium in which only those changes that are in the collective best interests of users will be adopted. Enables Bitcoin to subsume superior features from competitors that are market-proven, making it highly resilient to disruption.
- Programmability—As a digitally native form of money, it can be used as a form of payment, collateral or fuel for a variety of smart contracts (self-executing software or commercial agreements). Can interface with other decentralized applications. Could function as the core value system for the TrustNet, the anticipated wave of innovation triggered by the emergence of Bitcoin.

Bitcoin has made a major impact in the world in its 10 years of existence, and it still holds a great deal of promise for the future. All in good time. Given its inextricable relationship with money and Bitcoin, the concept of time is worth exploring more deeply. It turns out that time's role in our lives, individually and collectively, is the key to understanding prosperity and the ways in which Bitcoin could play a key role.

Synthesized Works & Further Reading

- [1] [*The Bitcoin Standard: The Decentralized Alternative to Central Banking*](#) by Saifedean Ammous (a masterful work on which much of this essay is based)
- [2] [*The Rational Optimist*](#) by Matt Ridley
- [3] [*Skin in the Game*](#) by Nassim Nicholas Taleb
- [4] [*The Bullish Case for Bitcoin*](#) by Vijay Boyapati
- [5] [*The Age of Cryptocurrency*](#) by Paul Vigna and Michael J. Casey
- [6] [*Sapiens*](#) by Yuval Harari
- [7] *Bitcoin is a Decentralized Organism*, [Part 1](#) and [Part 2](#) by Brandon Quittem
- [8] [*PoW is Efficient*](#) by Dan Held
- [9] [*The Fifth Protocol*](#) by Naval Ravikant
- [10] [*Unpacking Bitcoin's Social Contract*](#) by Hasu
- [11] [*Antifragile*](#) by Nassim Nicholas Taleb

- [12] [*Letter to Jamie Dimon*](#) by Adam Ludwin
- [13] [*Placeholder VC Investment Thesis Summary*](#) by Joel Monegro and Chris Burniske
- [14] [*Diffusion of Innovations*](#) by Everett M. Rogers
- [15] [*Why America Can't Regulate Bitcoin*](#) by Beautyon
- [16] [*Hyperbitcoinization*](#) by Daniel Krawisz

Money, Bitcoin and Time: Part 3 of 3

By [Robert Breedlove](#)

Posted January 26, 2019



7 The Simple Truth about Time: Time is the ultimate resource. Its absolute scarcity bounds the entirety our stories, both as individuals and societies. With economics, we strive to use it more effectively. As the destroyer of all things and the healer of

The Ultimate Resource [1]

Scarcity is the starting point of all economics. It is commonly believed that natural resources are inherently scarce, which is true in a sense, as there is only so much gold within the Earth, for instance. However, this finite quantity of gold in the Earth is still too large for humans to even measure and in no way constitutes an actual limit to the amount we can conceivably mine. We have literally ‘just scratched the surface’, as our mining efforts haven’t even taken us half way into the Earth’s crust, its thinnest and outermost layer. Driven by need, humans have always found a way to explore farther and dig deeper to uncover ever-more natural resources. Therefore, the actual practical limit to the quantity of any natural resource is always and only the amount of human time, effort and ingenuity devoted to its production. For human beings then, the only truly scarce resource is time.

Individually, the only scarcity we face is our limited time on Earth. As a society, the only scarcity we deal with is the total amount of human time, effort and ingenuity available to be directed at the production of goods. This scarce resource, which we will call *human time*, is the ultimate societal means of production. Humans have never fully exhausted any single natural resource. The price of all natural resources, in terms of human time, has always decreased steadily over the long-run as our technological advancements have dramatically increased our productivity. Not only have we not depleted any natural resource, but the proven reserves (the amount of natural resources still within the Earth) continue to increase despite our increasing rates of production, as new technologies enable us to discover and excavate ever-more natural resources.

Oil, the lifeblood of the industrial economy, is a great example of this concept. Even as oil production has increased every year, its proven reserves increase at an even faster rate. According to data from BP's statistical review, annual oil production increased 50% from 1980 to 2015. Oil reserves, on the other hand, have increased 148% during the same 35 year period, around triple the increase in oil production. Similar statistics exist for all natural resources prevalent in the Earth's crust. Some are more common (iron, copper) and some are rare (gold, silver) but the limit of how much we can produce of any particular natural resource is always and only the amount of human time directed at its production. The best evidence of this simple fact is gold: if the annual production of the one of the rarest metals in the Earth's crust goes up every year, then it makes no sense to consider any other natural resource being scarce in any practical sense. Echoing back to the fundamental market realities related to deferred consumption and investment—the real cost of anything is always its opportunity cost in terms of goods forgone to produce it. In terms of natural resources, only human time is truly scarce, which makes time the ultimate resource.

Frozen Time [1]

As more humans exist, there is more human time to direct towards the extraction and production of natural resources. As we have learned, productive output per unit of human time (productivity) can be amplified by leveraging technological solutions to problems (tools). In economics, a tool or technology is considered to be both:

- A non-excludable good—once one person invents something, all others can copy it and benefit from it
- A non-rival good—a person benefiting from an invention does not reduce the utility that accrues to the others who use it

For example, once one person invented the wheel, everyone else could copy its design and make their own, and their use of this design would in no way reduce others' ability to benefit from it. Innovations like this spread and their benefits compound over time, leading to ever-higher productivity and division of labor. Like the candle whose flame burns undiminished even after igniting a thousand others, the benefits of innovation ultimately accrue to everyone without detracting from the innovator in any way.

Natural resources and innovation are always and only the product of human time. Therefore, in terms of production, human time is the ultimate resource and essence of value. To keep score, people needed a way to reliably store the value they produce with their time, so that they can exchange it in the future for other peoples' time, effort and ingenuity. Conceptually then, money is frozen time. It is earned by sacrificing human time and can be traded for commensurate sacrifices from others.

The age-old problem faced by people is collectively deciding which monetary technology can best serve this purpose.

Technologically, money is a spontaneous emergent property that humans ascribe to a particular good. People, acting in self-interest, live within technological and economic realities that shape their decisions and provide them incentives to persist, adapt, change or innovate. It is from the countless collisions of these complex human interactions that spontaneous monetary orders have emerged and decayed. History has shown us myriad cases of a good being subjected to market-driven natural selection, achieving a monetary role and subsequently having its role taken by a superior technology.

Whatever monetary media people chose as a store of value was always subject to being produced in greater quantity, so the producers could acquire the value stored in it. The Yapese witnessed this play out when O'Keefe produced Rai Stones using explosives. West Africans had their wealth confiscated by Europeans who shipped in boat loads of cheaply produced glass beads. Citizens in modern economies continuously have their wealth usurped as central banks gradually or quickly erode the value of government fiat money. Gold came close to solving this problem as it is indestructible, expensive to mine and its flow is relatively predictable. However, gold's physicality led to its centralization within bank vaults and its compulsory replacement with soft government money.

Until the invention of Bitcoin, all forms of money were subject to having their value stolen by producers of the monetary good. This made all monetary technologies before Bitcoin imperfect in their ability to store value across time. Bitcoin's finite supply makes it the best medium to store the value produced by finite human time. In other words, Bitcoin is the best store of value humanity has ever invented, as it is the only monetary technology that cannot be debased over time. The informational, intangible and purely digital nature of Bitcoin enables it to achieve absolute scarcity, a property that was previously exclusive to time itself.

The absolute scarcity of Bitcoin makes it the perfect modality for freezing and transacting the only other absolutely scarce resource—time.

No matter how many people use the network, how advanced mining equipment becomes or how much its price increases, there can only ever be 21 million Bitcoins in existence. In time, it is likely that Bitcoin will be regarded as the best technology for saving ever invented.

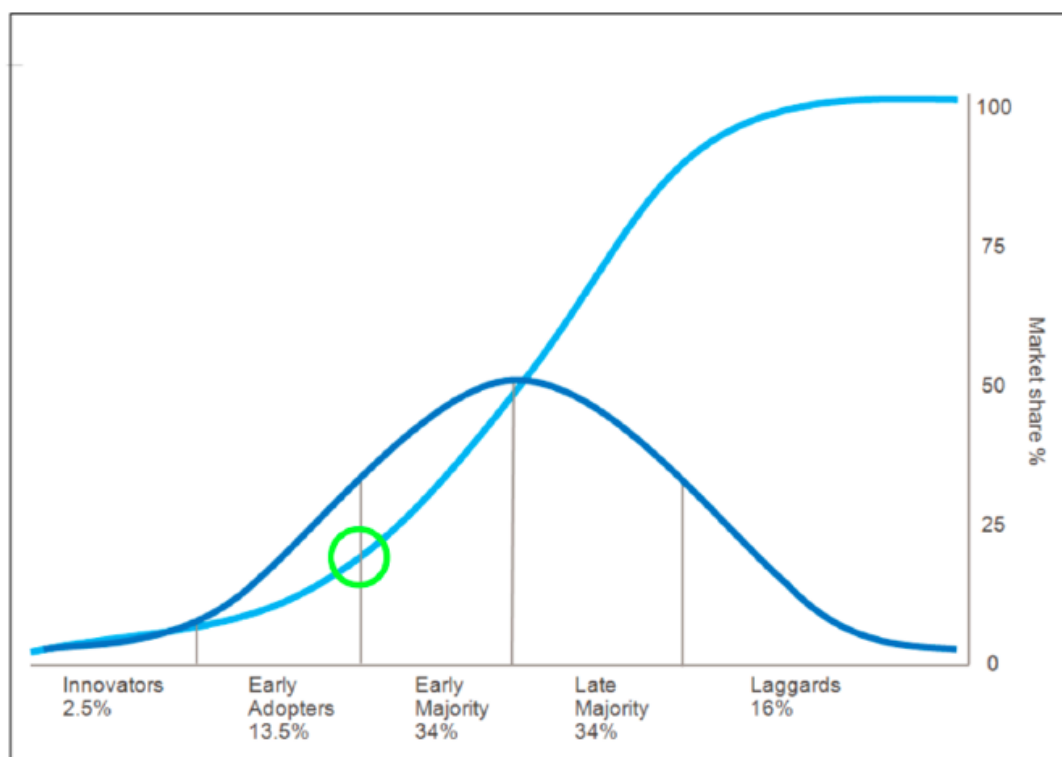
Time Arbitrage [2,13,14]

Innovations of this magnitude are virtually impossible to predict; however, they do follow a familiar adoption pattern. The book titled 'Diffusion of Innovations' lays out a

framework that seeks to explain how, why and at what rate new ideas and technologies spread. Diffusion is the process by which an innovation is communicated and adopted by participants in a social system over time. There are four main elements that influence the spread of the new idea:

- The nature of the innovation
- Communication channels
- Time elapsed since ideation
- The social systems under which it is adopted

Once a certain rate of adoption is achieved, the innovation reaches a tipping point and its continuous spread becomes practically unstoppable (a concept of preferences closely related to the minority rule discussed earlier) as people naturally prefer superior technology solutions. Such an adoption curve is especially true of, and often completed faster for, network-based technologies such as the internet and Bitcoin; as their general acceptance is driven harder and faster by network effects. Based on its estimated number of users, we are just beginning to enter the early adopter phase for Bitcoin:

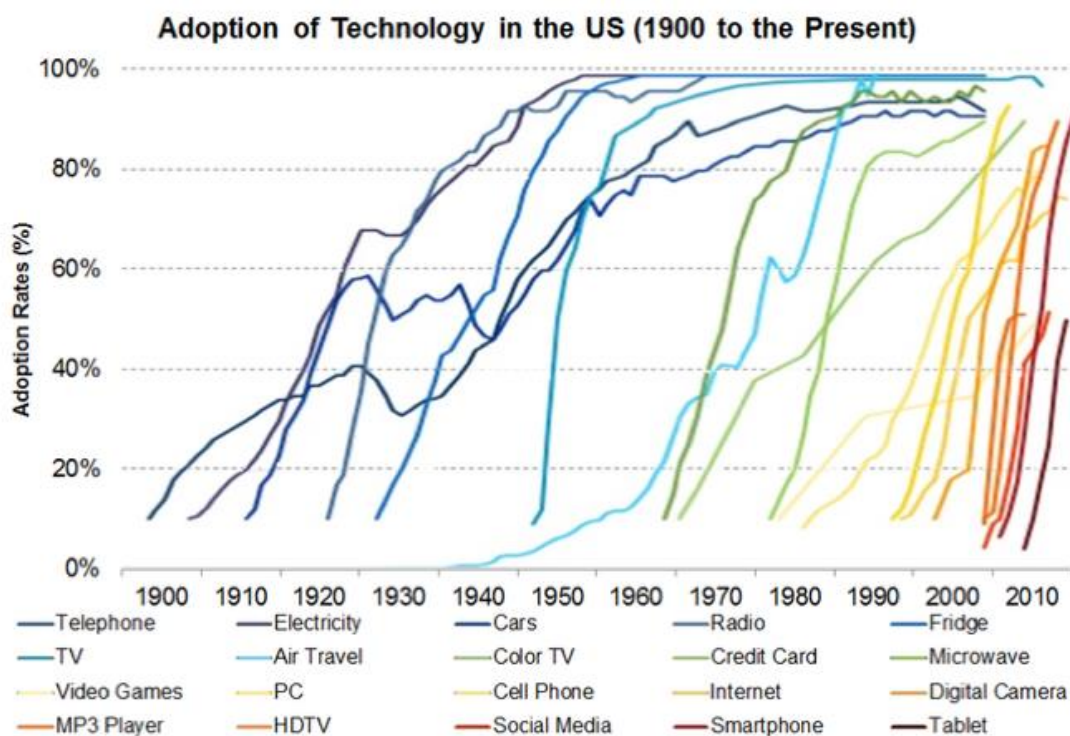


The S-curve of adoption. As successive groups adopt a new technology or idea market share rises. The tipping point (green circle) marks an inflection point and leads to rapid growth in adoption.

In investing, the concept of *time arbitrage* refers to an asset becoming oversold based on a short-term or emotional market sentiment despite its long-term outlook

or investment fundamentals remaining unchanged or even improving. Time arbitrage is essentially another form of the old investment adage “Buy on bad news, sell on good news”. Times such as these present savvy investors with an opportunity to enter a position with the same or improved value fundamentals at a lower price point.

All ubiquitous technologies today, beginning as fledgling innovations themselves, have traversed this path to mainstream adoption. Here we show some of the most impactful innovations since the year 1900 and the rapidity with which they were adopted:



8As telecommunication networks have become more advanced and ubiquitous, the user adoption rates of new innovations have accelerated dramatically.

As we can see, advances in telecommunications and distribution methods have accelerated the pace with which new innovations are adopted. Today, the internet causes breakthrough innovations to spread like a wildfire throughout the minds of people all over the world. Since it is a nascent monetary technology that is not fully understood by the vast majority of the world, Bitcoin still has low levels of adoption and therefore significant upside prospects. Also, owning a piece of the Bitcoin network today is over 80% cheaper than about a year ago even though its utility in terms of throughput, transaction fee efficiency and network security have all improved substantially over the same period. This confluence of factors indicates that now is an opportune time to take advantage of time arbitrage and invest in the

Bitcoin network. Also, as a technology, the Bitcoin network's value will continue to grow with every passing day that it successfully operates.

Lindy Effect [4,11]

Things in this world fall into one of two general categories: perishable and nonperishable. The distinction between the perishable (humans, single items) and the nonperishable is that the latter does not have a natural, unavoidable expiration date. The perishable is typically physical in nature, meaning it is subject to physical degradation, whereas the nonperishable is typically informational in nature. A single car is perishable, but the automobile as a technology has survived for a century and can be reasonably expected to persist for at least another one. An individual man will die, but his genes (which are digital) can be passed on for innumerable generations. This heuristic from Nassim Taleb, known as the *Lindy Effect*, can be summarized as follows:

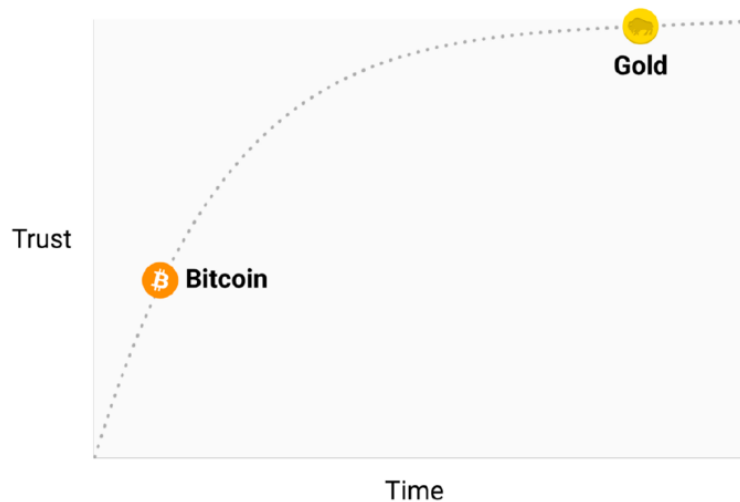
- For the perishable, every additional day of life translates into a shorter additional life expectancy.
- For the nonperishable, every additional day of life may imply a longer life expectancy.

The only effective judge of things is time, as time is the ultimate destroyer of all things. The Lindy Effect is closely related to antifragility, as the ravages of time are a potent form of adversity. Anything that gains from temporally-driven increases in disorder is antifragile and benefits from the Lindy Effect. Using arbitrary math for simplicity, if a book is still in print after 50 years, it can be expected to remain in print for another 50 years. If it's still in print for another 50 years after that, then perhaps it can then be expected to remain in print for at least an additional 120 years. At some point, the Lindy Effect may imply an unlimited life expectancy. A book like the Bible, which has been in print for thousands of years, can be reasonably expected to remain in print for the rest of human history.

If you had conducted a survey in 1995 and asked people whether they believed the internet would be a permanent feature of their lives, you would have probably received mixed responses. If you conducted the same survey today, people would resoundingly agree that the internet is here to stay. A technology, being informational rather than physical in nature, does not age in the same way humans do. A technology like the wheel is not "old" in the sense of experiencing degradation, it is a technological design that has persisted for millennia and can be reasonably expected to persist for many more.

So, the longer a technology lives, the longer it can be expected to live. Since Bitcoin is a technology, every day that it continues to successfully operate increases its life expectancy. Further, as we have learned, the core moving parts of Bitcoin are

mathematics and human nature—two concepts which are very “Lindy” and can be reasonably expected to persist for the rest of human history. Bitcoin’s ever-growing life expectancy increases its perceived trustworthiness and eventually it will be regarded as a permanent feature of our modern lives in the same way the internet is today. This heuristic helps explain why gold will likely continue to be regarded as a monetary metal for many years to come, whereas Bitcoin is still in the process earning people’s trust:



9 Hard monetary technologies become more trusted over time as they offer peace of mind to their users.

The Lindy Effect is universally applicable across time. The same competitive dynamics that caused the ascent of gold into a dominant monetary role are now driving Bitcoin adoption. In this sense, the future is in the past. As the Arabic proverb says: *he who does not have a past has no future*. Notwithstanding the past century of central bank coercion, hard money is the norm of human history and we are witnessing its reemergence with the rise of Bitcoin. As Bitcoin continues to persist, knowledge of its fundamental nature and functional capabilities will continue to spread. Threatened by its continued growth, incumbents will ratchet up their efforts to prevent Bitcoin’s ascent and protect the monopoly on money they have enjoyed over the past century.

Future of Regulation [1,4,5,15]

There is a good reason why the gold standard was forcibly ended and no good store of value has yet risen to fill the void. To preserve seigniorage profits governments must enforce an inflationary monetary policy. Otherwise, if a sound store of value existed that was accessible to its citizenry, their business model would be jeopardized as people would exit depreciating fiat currencies to shield their wealth from further confiscation. As Alan Greenspan, former Chairman of the Federal Reserve (the central bank of the United States) said in 1966:

“In the absence of the gold standard, there is no way to protect savings from confiscation through inflation. There is no safe store of value. If there were, the government would have to make its holding illegal, as was done in the case of gold. If everyone decided, for example, to convert all his bank deposits to silver or copper or any other good, and thereafter declined to accept checks as payment for goods, bank deposits would lose their purchasing power and government-created bank credit would be worthless as a claim on goods. The financial policy of the welfare state requires that there be no way for the owners of wealth to protect themselves.”

Clearly, central banks are aware that free market competition against hard money poses significant risk to the continuity of their socialistic business model. To protect central bank monopoly positions, governments have resorted to passing onerous laws against their citizens. Governments seek to insulate their national currencies from free market competition employing legal measures such as:

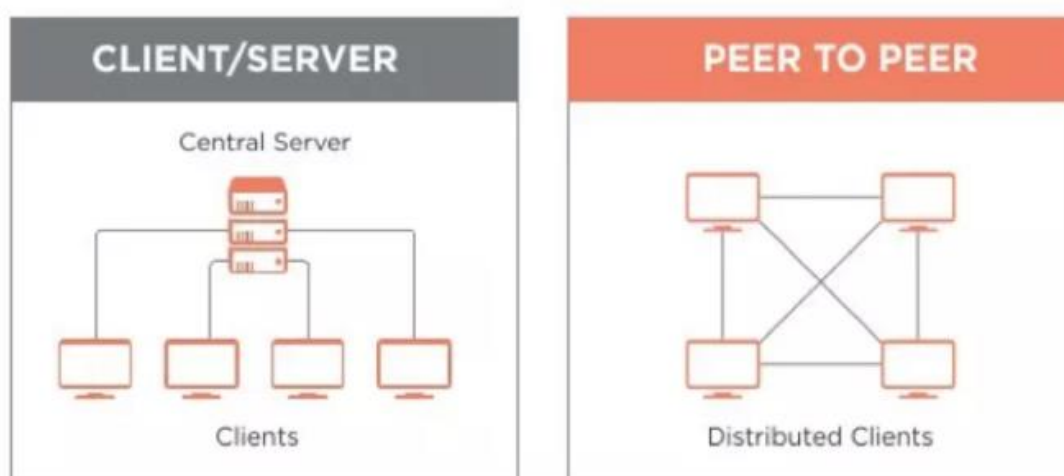
- Capital Controls—which prohibit the movement of money into or out of a country
- Confiscatory Orders—forceful seizure of assets, like Executive Order 6102 in 1933 which outlawed private ownership of gold in the United States
- Legal Tender laws—which create artificial demand for government fiat money by requiring that it be accepted in settlement of debts

With Bitcoin, regulators face a unique dilemma. Bitcoin exists orthogonally to the law, and there is virtually nothing that any authority (or anyone for that matter) can do to affect its operation. Regulations were designed to govern people and entities and are not equipped to deal with a decentralized network that autonomously proliferates itself. Regulators are really good at targeting centralized marks, like an individual business or its CEO, and enforcing laws against them. However, regulations have proven to be largely impotent against decentralized services.

To understand this point, consider the case of BitTorrent, a decentralized peer-to-peer file sharing service. In the earlier days of the internet, file sharing platforms like Napster and Kazaa had become an extremely popular way for users to share movies, music and other media directly with one another. With these free services, users would upload media to and download media from the companies' computer servers. This client-server file sharing directly threatened media monopoly profits, as it completely circumvented copyright law. Incumbent organizations quickly responded with heavy litigation. Since services like Napster and Kazaa were hosted by centralized companies complete with a headquarters, executive team and computer servers, they were vulnerable to being shut down. Filing a lawsuit, knocking on some doors, levying some fines and decommissioning some computer

servers was all it took to shut down these services and protect media industry monopolists.

The introduction of BitTorrent, an open-source decentralized protocol for peer-to-peer file sharing, was a game changer. Once installed on a computer, BitTorrent enables user nodes to upload and download movies, music and other media directly from one another using encrypted communication channels. Since files on its network do not come from a single source, BitTorrent was also able to offer superior download speeds by fragmenting the media files and pulling from multiple nodes simultaneously. Unlike the failed client-server models of centralized platforms, the BitTorrent protocol never holds any of the media files, it only facilitates the transfer of files between individual users:



10 Like the proven model of BitTorrent, Bitcoin sports a decentralized architecture that makes it highly resistant to external attack and censorship.

Architecturally, the entire software codebase of the protocol exists on every user machine that downloads it, making it virtually impossible for a regulator to target and shutdown as there is no single point of vulnerability (censorship resistance). The BitTorrent protocol exists everywhere and nowhere by virtue of its decentralized network architecture, a model that would be later employed by Bitcoin. Indeed, without a centralized target to shut down, regulators were incapable of stopping BitTorrent and the other protocols it inspired. By 2009, peer-to-peer file sharing using decentralized protocols like BitTorrent accounted for up to 70% of internet traffic worldwide.

Bitcoin has already exhibited similar properties to BitTorrent as regulators have been incapable of containing the expansion of its network or shutting it down. It cannot be contained by capital controls, as it exists entirely outside the legacy financial system. Confiscation of Bitcoin, unlike that of gold, is extremely difficult given its informational nature. This leaves legal tender laws, which are still enforceable and

could therefore require Bitcoin users to convert some of their holdings into government fiat money to pay their taxes. So, the exchanges and OTC markets where Bitcoin is traded are the only viable targets for regulators. As such, these financial gateways that connect Bitcoin to the traditional financial system are likely to see continuous intensification of regulatory scrutiny and enforcement actions. However, as we saw in China, escalated efforts will likely only highlight the need for Bitcoin, expand its brand awareness and spawn off exchange transactions (Streisand Effect).

In essence, open-source software projects like Bitcoin are just information—software written in a computer language called code. Since it is just code, Bitcoin can be printed out, written down, spoken or memorized. Bitcoin is also a form of money, so it makes money and information the same thing. This concept was summed up nicely by Naval Ravikant in 2017:

“This is one of the crazy things about this concept because money and speech turned out to be the same thing — money, information and math — they’re the same thing. In a Bitcoin world, I can literally write down my Bitcoin address and keys on a piece of paper and put it in a safety deposit box. It’s basically in cold storage, I could even put it in my head. I can memorize the key phrases and I could cross national borders with \$1 billion in my brain. It’s a very powerful but literally mind bending concept in that sense.”

The First amendment of the United States Constitution guarantees that all Americans have the power to exercise their right to publish and distribute anything they like, without restriction or prior restraint—which includes software code like that which constitutes Bitcoin. Established legal precedent in the United States explicitly protects software code under the First Amendment. Consider the case of PGP:

“In 1995, the US Government had on the statute books, laws that restrict the export of encryption software products from America without a license. These goods are classified as ‘munitions’. The first versions of the breakthrough Public Key Encryption software “Pretty Good Privacy” or “PGP”, written by Philip Zimmerman had already escaped the USA via Bulletin Board Systems from the moment it was first distributed, but all copies of PGP outside of the United States were “illegal”. In order to fix the problem of all copies of PGP outside of America being encumbered by this perception, an ingenious plan was put into motion, using the first Amendment as the means of making it happen legally. The source code for PGP was [printed out](#). It’s as simple as that. Once the source code for PGP was printed in

book form, it instantly and more importantly, unambiguously, fell under the protection of the First Amendment.”

Bitcoin unambiguously falls under the Freedom of Speech Protections offered by the First Amendment to the United States Constitution.

For these reasons, it is unlikely that any major government would attempt to ban Bitcoin outright as, not only would it contradict freedom of speech laws, it would also create a tidal wave of publicity (again, Streisand Effect). Central banks have acknowledged this reality. Former chairwoman of the Federal Reserve Janet Yellen confirmed:

“The Federal Reserve simply does not have the authority to supervise or regulate Bitcoin in any way.”

So, Bitcoin can't be shut down, is virtually immune to regulation and leverages economic incentives to grow relentlessly. Its very existence is a game changer for almost everyone in this world, especially central banks who now face an existential threat to their business model.

The Long Game [1,4,16]

Money is how we keep score in the game of life. *Game theory* explores how rational people make strategic decisions in different scenarios. It is based in purely mathematical terms and has applications in any domain where people must choose whether to cooperate or compete with each other. The standard game analyzed by game theory is the Prisoner's Dilemma:

Two members of a criminal gang, Alex and Bobby, are arrested and imprisoned. Each prisoner is in solitary confinement with no means of communicating with the other. The prosecutors lack sufficient evidence to convict the pair on the principal charge, but they have enough to convict both on a lesser charge. Simultaneously, the prosecutors offer each prisoner a bargain. Each prisoner is given the opportunity either to betray the other by testifying against them, or to cooperate with the other by remaining silent. The possible decisions and outcomes are:

- *If Alex and Bobby both betray each other, each of them serves 2 years in prison*
- *If Alex betrays Bobby but Bobby remains silent, Alex will be set free and Bobby will serve 3 years in prison*
- *If Bobby betrays Alex but Alex remains silent, Bobby will be set free and Alex will serve 3 years in prison*
- *If Alex and Bobby both remain silent, both of them will only serve 1 year in prison (on the lesser charge)*

This game decisions and its outcomes are summarized in this table:

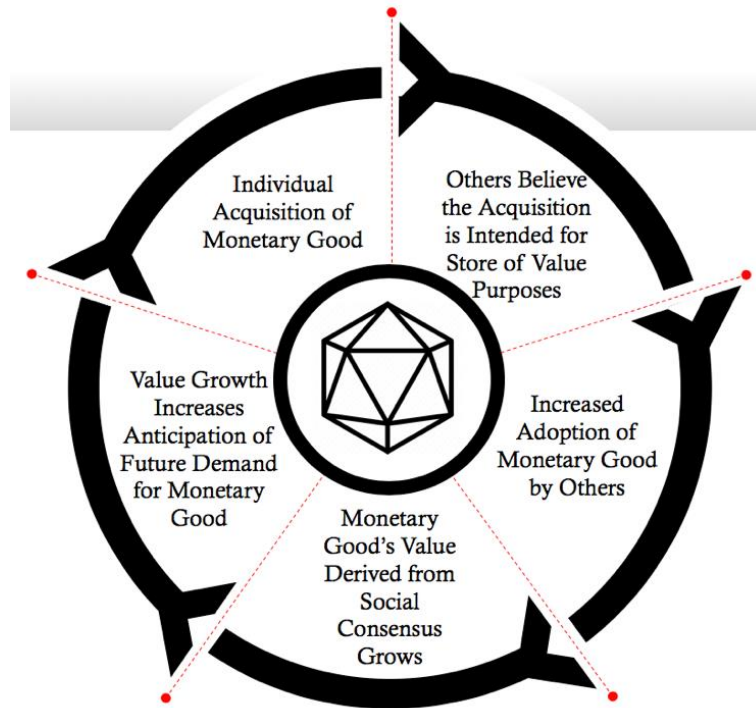
		Bobby's decisions	
		Bobby stays silent (cooperates)	Bobby testifies (betrays)
Alex's Decisions	Alex stays silent (cooperates)	Alex and Bobby each serve 1 year	Alex serves 3 years, Bobby goes free
	Alex testifies (betrays)	Alex goes free, Bobby serves 3 years	Alex and Bobby each serve 2 years

11 Game theory shows us that adversaries will often behave contrary to their mutual best interests.

This Prisoner's Dilemma game converges on a *Schelling Point*, which is a solution that people will tend towards in the absence of communication or definitive trust (in other words, in an adversarial environment). The Schelling Point in the Prisoner's Dilemma is that Alex and Bobby both choose to betray each other, as each would risk 3 years in prison if one chose to remain silent and the other testified. Since both have an incentive to testify, the optimal strategy for this game is that they both betray, despite their mutual silence offering the best outcome for them both.

Since money is an adversarial game (there are winners and losers) express communications between players cannot always be trusted. Therefore, the Schelling Point of monetary competition is to choose the available good which exhibits the highest hardness, because people (potential adversaries) must be restrained from creating new monetary units to steal the value stored within them. This is exactly the reason market-driven natural selection is so ruthlessly effective at promulgating hard money, as people are constantly seeking to acquire value and store it in the most reliably hard monetary technology available.

Monetary goods, like Bitcoin, are valued based on their game theoretic qualities—meaning each market participant values a monetary good based on their appraisal of whether and how much other participants will value it (in the same way that prisoners Alex and Bobby must anticipate each other's decisions to make effective decisions of their own). The earlier one is able to anticipate the future demand for a monetary good, the greater the advantage conferred to the prognosticator; as it can be acquired more cheaply than when it becomes widely demanded at a later time. Further, when one acquires a good expecting that it will be demanded as a future store of value, it actually hastens the adoption of the good by others for that particular purpose, as their selection of a store of value is partly influenced by their perception of your intentions which drove you to acquire the monetary good in the first place. This seeming circularity is another positive feedback loop that drives societies to converge on a single store of value (another aspect of the winner take all dynamic):



12 The game theoretic properties of the monetization process encourage people to converge on a singular money

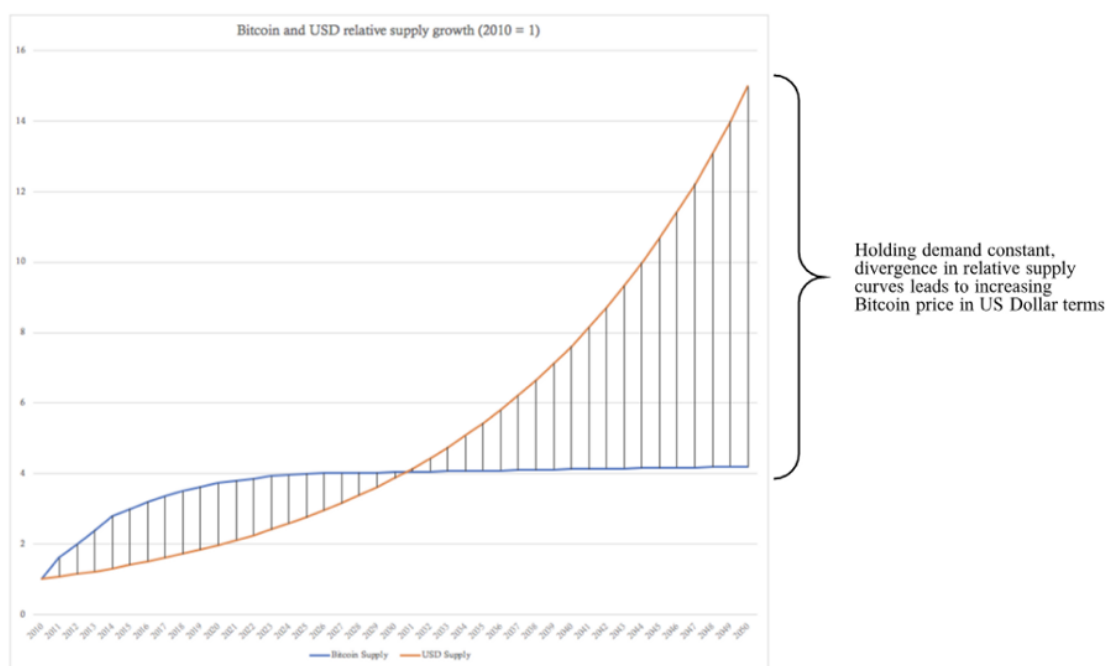
In game theoretic terms, total market dominance by a single store of value with a superior stock-to-flow ratio is known as a *Nash Equilibrium*—a game state where no player has an incentive to deviate from his chosen strategy after anticipating the most likely choices of all his opponents. Throughout all human history, societal convergence on a single form of superiorly hard money is the Nash Equilibrium of monetary competition. As we saw with gold in the 19th century, when multiple societies converge on a single store of value, they see a substantial decrease in trade costs and an attendant increase in free trade and capital accumulation (La Belle Époque). Only the past century, dominated by government fiat money, is anomalous in this respect.

Hard money is the norm of human history, and we are seeing its reemergence with Bitcoin.

The monetization process, as we saw with gold and are now seeing with Bitcoin, is game theoretic. People must decide individually how best to store the value created by their time spent in production. This decision is based on the anticipated beliefs, decisions and actions of others in relation to the monetary technologies available to them. The complex interaction of these decision dynamics is how people spontaneously ascribe a good the role of money and why the hardest money always

wins. In this way, hard money is an emergent property of indirect exchange just like money is an emergent property of direct exchange.

This emergent property perspective is exactly why value stored in softer forms of money is totally absorbed by hard money every time they interact within an economic network. Existing amid the expansionary monetary policies being practiced by every central bank in the world today, Bitcoin's price will continue to increase as the ratio of government fiat money in circulation to Bitcoin units in circulation diverges ever-further:

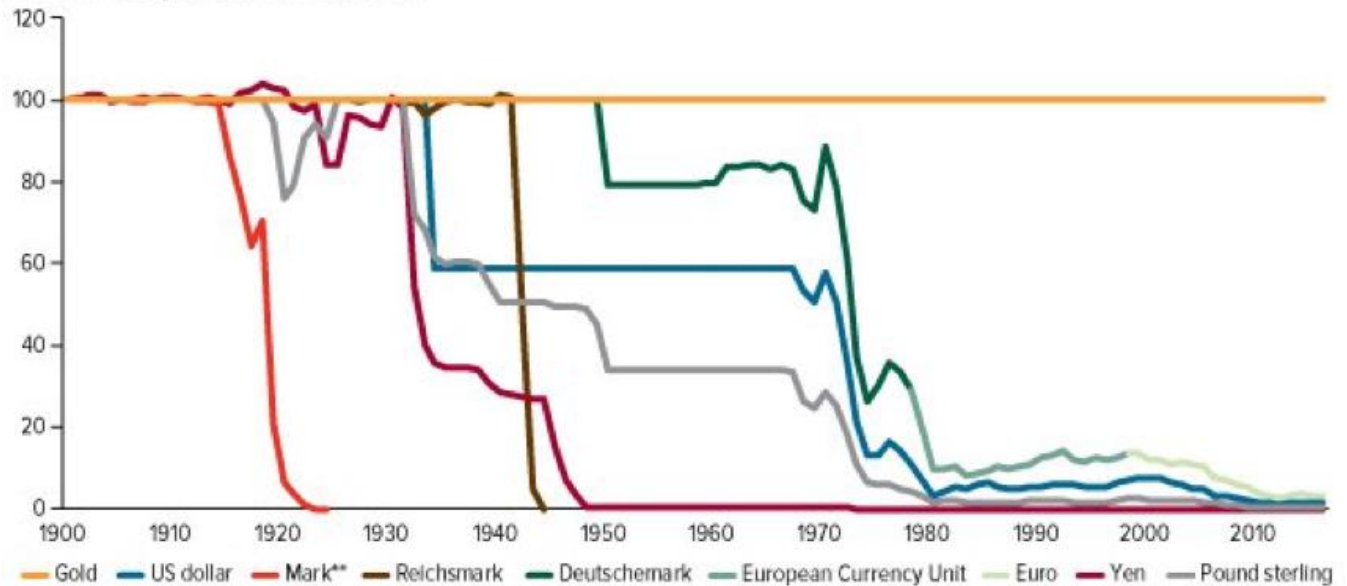


This graphic, which is strictly illustrative, simply shows that divergence in supply curves of Bitcoin and US Dollars will lead to the appreciation of Bitcoin in US Dollar terms, even without any increase in the demand for Bitcoin (as we have seen, demand for Bitcoin has been surging). The same dynamic is applicable to all modern government monies, as every central bank in the world is engaged in aggressive expansionary monetary policy. In the game of international government fiat monetary competition, the Nash Equilibrium is all currencies inflated into worthlessness. On this race to the bottom, those with easiest access to freshly printed money will expropriate as much value as possible (via the Cantillon Effect) and use it to acquire real estate, gold or other inflation resistant assets (such as Bitcoin). This game theoretic perspective clearly explains why virtually all soft government fiat currencies have trended towards eventual worthlessness.

Next, we show how all major fiat currencies have depreciated almost completely against gold since 1900 (notice the steep decline in 1971 when the peg to gold was completely severed):

All Major Currencies Have Depreciated over the Past Century Relative to Gold

Value in Gold, as of December 2016



Note: *As of December 2016. **The 'Mark' was the currency of the late German Empire.

Originally known as the Goldmark and backed by gold until 1914, it was later called Papermark.

Source: Bloomberg, CFMS-Thimson Reuters, ICE Benchmark Administration, Metals Focus, World Gold Council, U.S. Global Investors

As we have seen throughout history, every time hard money encounters soft money in a trade network, it has outcompeted it into extinction. We saw earlier how gold, possessing superior hardness, demonetized silver with dire economic consequences for those societies that remained on a silver standard the longest, such as China and India. Now it is gold that faces a monetary competitor with superior hardness, and it is likely that it will gradually become demonetized as people convert to Bitcoin for its unparalleled store of value properties. This will happen slowly, and gold may indeed maintain some of its monetary use case given the vast holdings of central banks, mankind's deep history with the monetary metal (Lindy Effect), its relatively high and predictable stock-to-flow ratio and the fact that some people may always prefer a tangible store of value over a digital alternative. For government money, the competitive situation is much more dire.

The Event Horizon [1,4,16]

Hyperinflation is a particular type of demonetization, unique to government fiat money, that did not exist under the gold standard. Hyperinflation occurs when a government produces new monetary units at an accelerating pace to finance expenditures or service debt burdens, which pushes the value of its currency down at the same accelerating rate. The value of a hyperinflating currency collapses against the most liquid goods available to the society first (like gold or the US dollar) and then, depending on relative availability, against real goods such as real estate and commodities. This sequence is caused by individual's attempting to maximize their

exchange optionality as they escape their failing currency and prepare to navigate highly uncertain economic conditions. When hyperinflation intensifies, currencies begin falling against perishable goods. It is common to see grocery stores completely emptied out in societies suffering from the late stages of hyperinflation. Eventually, the society will either devolve to a barter economy or adopt a new medium of exchange, as we saw in Zimbabwe when its failing dollar was ultimately replaced by the US dollar. This process is arduous as the replacement currency is often scarce as foreign banking institutions are either reluctant to or restricted from providing liquidity.

As Bitcoin is the hardest form of money in existence, it will continue to appreciate against a backdrop of hyperinflating, soft government fiat currencies even without any increase in demand for Bitcoin (as illustrated in the above graphic). Eventually, this will lead to an inflection point in some economies where users rush to exit from their failing currency to get into Bitcoin to protect their wealth from further confiscation. This transition will have similar dynamics to other demonetization and hyperinflation events, however it will also be different given Bitcoin's unique properties as a monetary technology. A Bitcoin-induced currency demonetization is called a *hyperbitcoinization event* and is different from hyperinflation in two critical respects.

First, hyperinflation occurs with restricted competition with other fiat currencies, since a government can easily enforce capital controls that selectively prohibit inflows or outflows of government money, whereas hyperbitcoinization occurs because of direct competition with Bitcoin, which can easily cross borders as it is immune to capital controls. This will cause hyperbitcoinization to happen much faster than a hyperinflation event, since governments will have great difficulty preventing Bitcoin trading within their borders due to its purely informational nature. Given governments' inability to shield their local currencies from direct competition with Bitcoin and the high opportunity cost of holding a depreciating form of money, once a hyperbitcoinization event reaches a critical mass it will happen quickly.

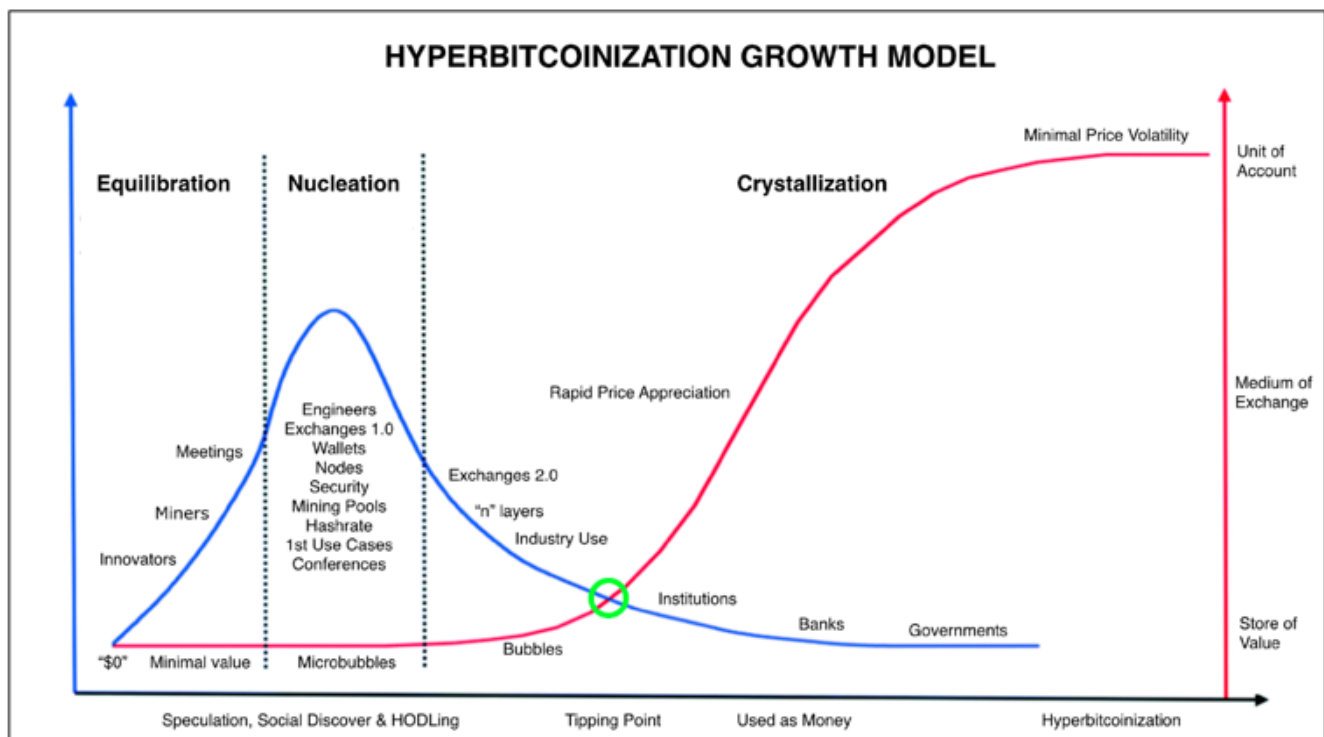
Second, in hyperinflation, the governments expand money supplies in an attempt to outpace people's inflation expectations. As governments form a habit of inflating money supplies, people form a habit of anticipating rising prices and seek alternative stores of value. Governments, in turn, must print incrementally more money to stay ahead of inflation expectations and generate the same economic effect with each new monetary unit produced. With no alternative monetary media in which to escape, prices surge until a breaking point is reached. Hyperinflation is extremely disruptive to an economy as it forces people to switch from the worst form of government fiat money available to them to some other soft government fiat money (at best) or ends in total economic collapse (at worst). In hyperbitcoinization, users have a supranational monetary media in which to escape centrally planned economies. Therefore, a hyperbitcoinization event should be much less disruptive to

the economy, as people will be trading in an inferior form of money for a superior one. Seeing as hyperbitcoinization should happen fast, people will quickly become accustomed to dealing in Bitcoin, which will protect deteriorating wealth and stabilize economic conditions.

Hyperbitcoinization will likely be a confusing, potentially chaotic, time for many people. Initially, it will probably occur at the periphery, with the countries inflating their currencies the fastest experiencing it first. Stories of this will spread quickly in the digital age and add to the believability of Bitcoin, all while it continues to benefit from the resultant increases in demand, network effects and the Lindy Effect. As more people wake up to the reality of hard money, we would expect the pace of this global transition to accelerate until all soft money is outcompeted into extinction. Fortunately, it will happen relatively quickly, since Bitcoin is immune to capital controls, and act as a stabilizing force for the world economy going forward (since hard money resists market distortions and remains firmly rooted in economic reality).

Like a star orbiting a black hole, any established monetary order that goes beyond the event horizon of hyperbitcoinization will inevitably collapse into Bitcoin's singularity.

Next, we show how a hyperbitcoinization event is likely to unfold:



Once Bitcoin's ecosystem is seeded a crystallization process begins. Growth becomes exponential and self-reinforcing. In this model, the tipping point (green circle) represents a dramatic change at which point many people and organizations adopt Bitcoin.

The estimates of how valuable Bitcoin would become after global hyperbitcoinization vary based on what weighting is included for different stores of value (gold, government money, real estate, stocks, bonds, art, oil and other commodities are all used for this purpose today) but, using simple math for our directional analysis, if Bitcoin demonetizes just gold it would be valued at about \$400K per coin (\$8T/20M coins in 2025). If it demonetizes government money as well, it would be valued at about \$5M per coin (\$100T/20M coins in 2025). As awareness of Bitcoin and its potential impact spread, the long game becomes even more interesting. Considering Bitcoin represents an existential threat to government fiat money and central banks, we must also consider their decisions from a game theoretic perspective.

Reverse Bank Run [1,4,5]

Although it is still considered magic internet money by most people today, its continued existence and appreciation will attract more attention from high-net-worth individuals, institutional investors and then, possibly, central banks. As we have learned, central banks still rely on gold as a means of final settlement, as it was (before Bitcoin) the only monetary medium entirely free of counterparty risk (cash money). However, transporting and securing gold is an extremely expensive process fraught with operational risk. These costs and risks are the reason final settlements between banks occur very infrequently.

With the transaction throughput available on the Bitcoin network today, the global group of 850 central banks can perform daily final settlement with one another. With each central bank serving an average of 10 million customers, this would more than cover the entire world's population. In a world in which central banks adopted a Bitcoin standard, governments would no longer have the ability to increase the money supply and banks would begin to compete freely with one another by offering various physical and digital Bitcoin-backed monetary instruments and payment solutions. By using the technologies introduced by Bitcoin, cryptographic digital certainty can be applied to bank accounting and help expose those that engage in fractional reserve banking. This may lead to Bitcoin realizing its ultimate use case: the fastest and most efficient system for global final settlement across long distances and national borders. Despite the clear advantages of a system such as this, central banks are unlikely to give up their monopoly control over the existing monetary order willingly.

As people begin to voluntarily exit fiat currencies into Bitcoin to protect their wealth, as is already taking place in countries like Venezuela today, it will likely grab even more attention from central banks. As central banks are effectively losing customers, they will need to hedge the *going concern risk* posed to their business model. Central banks today hold reserves mainly in US Dollars, Euros, British Pounds, IMF Standard Drawing Rights and gold. These reserves are used to settle accounts and

defend the market price of their respective currencies. Should Bitcoin remain on its current trajectory, and considering its superiority as a final settlement layer, it is possible that at least one central bank somewhere in the world will add Bitcoin to its reserves, if for no other reason than to defend the market price of its government fiat money, as is consistent with their strategy for gold.

The most likely scenario is that a central bank will seek to own part of the Bitcoin network as an insurance policy against it succeeding. Strategically, it makes sense for a central bank to spend a small amount acquiring some of Bitcoin's supply today. For example, consider that the authorities of a central bank today judge that, although chances of a hyperbitcoinization event are extremely remote, it would represent an extinction-level event for their business. Mathematically, using Bitcoin's approximate price today of \$4K and its expected post-hyperbitcoinization price of \$5M, unless the central bank is more than 99.92% certain that this event will NOT happen then it is prudent to allocate at least 0.08% of their assets into Bitcoin as a perfect hedge against its success (since price growth from \$4K to \$5M is a 1250x increase, an allocation of 0.08% of assets would keep a central bank at even-money should a hyperbitcoinization event play out).

Game theory tells us that the first central bank to buy Bitcoin will trigger a reverse bank run, as its decision will alert the rest of the central banks who will be compelled by self-interest to follow suit. The first purchase by a central bank will cause the price of Bitcoin to rise significantly, causing others to move in based on their anticipation of future demand and compounding the effect as more central banks enter the market; making it progressively more expensive for later entrants. As central banks keep trying to anticipate the moves and strategies of one another, a game theoretic positive feedback loop will ensue that converges on a hard money Schelling point similar to that of free market monetary competition, thus triggering a global competition among central banks for maximal Bitcoin accumulation. A smart play for a central bank under the circumstances would be for it be the first to buy a small share of the Bitcoin network. An even smarter play would be for a central bank to purchase Bitcoin without announcing it, allowing it to begin accumulation at lower prices.

Similar to the transition to the gold standard in the 19th century, network effects would eventually take hold as more central banks bought some Bitcoin, increasing its liquidity and making it more marketable, thus creating ever-larger incentives for other central banks to join. After a sufficient minority of central banks have purchased part of the Bitcoin network, the minority rule will reach its final step and begin imposing the immutable rules of Bitcoin on the established monetary order. Once this reverse bank run on Bitcoin became public knowledge (as tends to happen easily in the digital age), it would be the ultimate seal of legitimacy for Bitcoin adoption and would add even more force to its ascent in the marketplace as this global game of Bitcoin accumulation would reach a fever pitch. Even at the largest

scales of the financial system, Bitcoin converts individual self-interest into the growth of its network.

You may find this prospect hard to believe. About 25 years ago, handheld touchscreen supercomputers with wireless global interconnectivity were hard to believe too. Change keeps happening faster and faster. Remember, each central bank will value Bitcoin based on its appraisal of whether and how much other central banks will ultimately value it. As they will all be conducting the same strategic analyses, they will undoubtedly realize the dilemma they face—either ignore Bitcoin and watch it continue to outcompete and accelerate the failure rate of fiat currencies thereby loosening their control over the established economic order or choose to adopt Bitcoin as a reserve asset and trigger a game of accumulation against other central banks and legitimize it as an asset which will culminate in the loss of their monopoly position in the market for money. Operating in an adversarial environment, game theory tells us that so long as Bitcoin continues to operate in its current form, central banks (like the prisoners Alex and Bobby) will eventually be faced with strategic choices such as these to protect their own interests. At some point, the substantial advantage imparted to the central bank that moves first will become an overwhelming incentive to at least one, causing it to be the first to make its move, thereby triggering the reverse bank run on Bitcoin.

A Path to Prosperity [1-16]

Making predictions is risky business, wrong answers are innumerable, and the right answer is singular. Accurate predictions are rare. By weaving together historical knowledge and awareness of current trends, one can develop a perspective on what technological innovations are possible. The biggest mistakes people make when making such predictions are:

- Forming an opinion on the innovative potential without considering it deeply (Blockbuster quickly reaching a decision to pass on buying Netflix for \$50M)
- Disregarding an innovation because it contradicts a closely held worldview (Kodak refusing to accept the disruptive potential of digital photography as they spent 100 years building a business model centered on chemical film)
- Overlooking an innovation because it is too small or threatens a position of power (major newspapers refusing to develop an online presence early on)

Practicing a beginner's mindset and reasoning from first principles is critical for effective foresight. Pulling together everything we have discussed in this paper, we will now propose a potential path forward for Bitcoin based on the historical

competitive dynamics of money, current macroeconomic trends and game theory. We will start from the inception of Bitcoin:

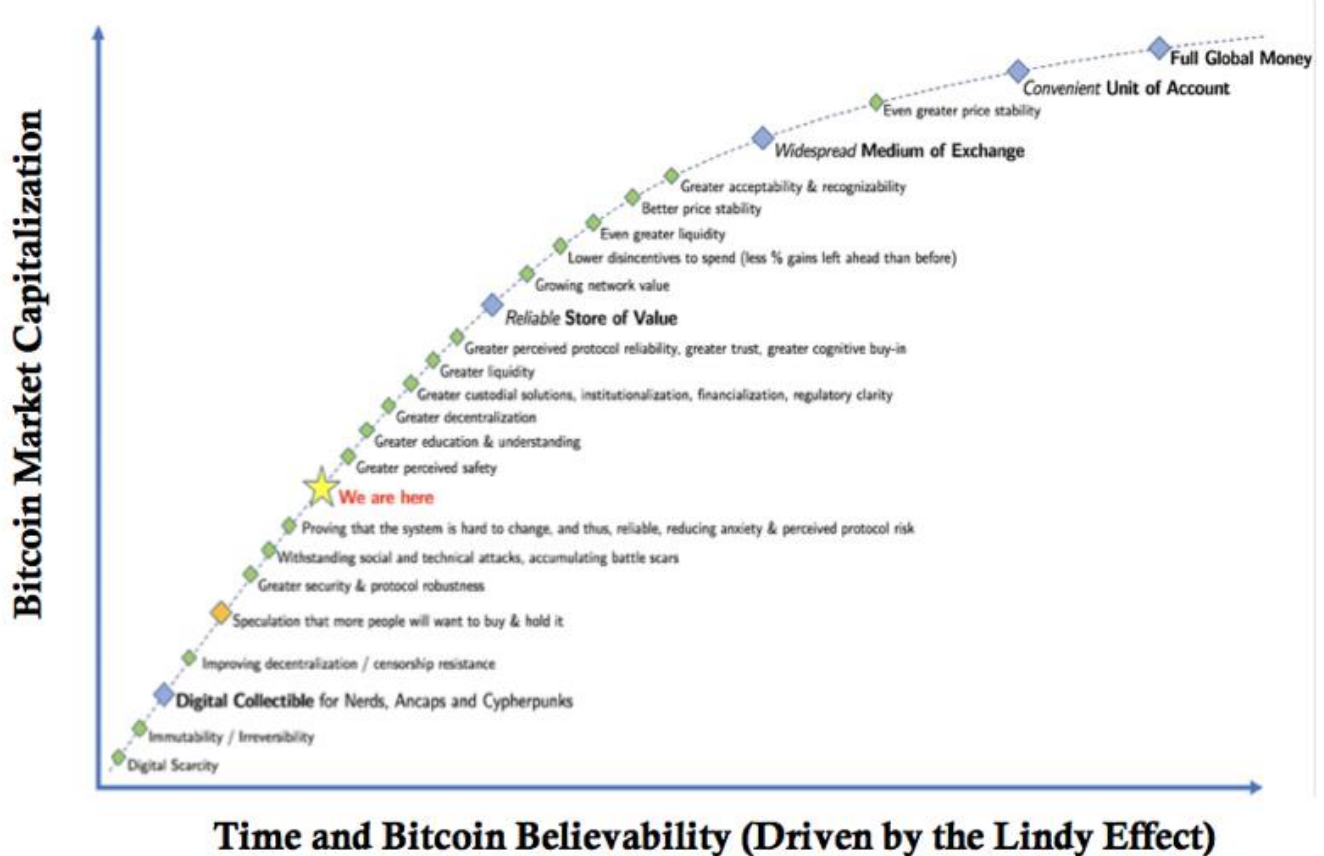
1. *Bitcoin is first perceived as an internet toy for cryptographers (Minority Rule – Step 1)*
2. *Its rapid price increase makes a small group of people rich, engages free market fanatics and brings media attention. Its hyper-volatile price presents itself early (Hodlers of Last Resort – Layer 1).*
3. *The media, financial and tech establishments – having failed to buy Bitcoin early and benefit from its meteoric rise – denounce it as a Ponzi scheme, the MySpace of Cryptocurrencies and the greatest bubble of all time (Streisand Effect).*
4. *A large number of scammers jump onto the Bitcoin hype-train and create their own cryptocurrencies claiming to be superior though lacking critical qualities including decentralization, security and immutable governance. Bitcoin's serendipitous first mover advantage, multi-sided network effects and its brand awareness fueled by the Nakamoto creation myth preserves its market dominant position.*
5. *Retail investors, venture capitalists and hedge funds – lacking understanding of monetary economics and applying inappropriate valuation models – invest into other cryptocurrencies, creating more noise and confusion as the prices of these altcoins increase at a rate higher than Bitcoin.*
6. *Well-connected venture capitalists and hedge funds are given discounts on the investments only to then dump much of what they bought onto retail investors.*
7. *Given their high correlation to Bitcoin and lacking utility, the world watches as the bear markets continue to wipe out more and more alternative cryptoassets as most fail to deliver any useful product, although some succeed in other market spaces. Features that are proven in the market by other cryptoassets are subsumed by Bitcoin (Decentralized Network Archetype). Bitcoin price volatility persists but annual low prices continue to ascend relentlessly (Holders of Last Resort – Layer 2).*
8. *Trust in Bitcoin increases over time (Lindy Effect) and its market price continues its upward yet volatile trajectory (Fractal Wave Patterns).*
9. *People, burned in the altcoin craze, witness and learn about Bitcoin's undisputed superiority across all monetary characteristics, especially its hardness (Holders of Last Resort – Layer 3).*
10. *On the eve of and during the next bull markets, Bitcoin's absolute scarcity and antifragile characteristics exacerbate investor FOMO (Game Theoretic Positive Feedback Loop). Some investors are inevitably caught in the*

subsequent Bitcoin price crash (Fractal Wave Pattern)(Hodlers of Last Resort — Layer 4).

- 11. Hyperinflating fiat currencies are further contributing to the adoption of Bitcoin as it becomes the only means of preserving wealth for many people, making Bitcoin a legitimate store of value. Governments scramble to try and enforce capital controls and create propaganda against Bitcoin, just like they did to gold in the 20th century. Capital controls prove to be impotent and the propaganda against Bitcoin incites internet and media narratives that regard it as a tool for freedom (Antifragility). Government dissent highlights the need for Bitcoin in the first place (Streisand Effect).*
- 12. Investors and high net-worth individuals are convinced to allocate a small portion of their assets into Bitcoin to capture further growth, hedge against inflation and increase the risk adjusted returns of their traditional portfolios (Minority Rule — Step 2)*
- 13. Increases in demand for Bitcoin necessarily involve a reduction in demand for fiat currencies, causing even higher inflation rates (Gresham's Law). At great expense and effort, governments messily issue their own cryptocurrencies but fail to relinquish control over monetary policy, which makes them uncompetitive against Bitcoin (Market-Driven Natural Selection). Governments covertly attempt to attack the Bitcoin network, which only strengthens it (Antifragility). Media coverage about Bitcoin shifts towards its use as hard money (Skin in the Game) and its importance for prosperity (Hodlers of Last Resort — Layer 5).*
- 14. Activists share the message that soft money creates social inequality (Soul in the Game) by disproportionately taxing the poorest via inflation (Cantillon Effect). This message spreads fast in a world of ever-more crashing fiat currencies and people rush to exit their local currencies for the safety of Bitcoin, triggering the first hyperbitcoinization events (Hodlers of Last Resort — Layer 6). Bitcoin mining hardware becomes commoditized and many citizens join mining pools (Decentralized Network Archetype)(Skin in the Game).*
- 15. Central banks, in an attempt to adapt to the new conditions and hedge going concern risks, quietly start to accumulate Bitcoin as a reserve asset, consistent with their gold strategy. A former central bank employee leaks a confidential strategy document regarding Bitcoin (Soul in the Game) which triggers other central banks to begin purchasing Bitcoin, causing its price and perceived legitimacy to increase at an accelerating rate (Game Theoretic Positive Feedback Loop)(Final Fractal Wave Pattern)(Hodlers of Last Resort — Layer 7).*

16. *Bitcoin's market capitalization reaches tens of trillions in US Dollar terms. Bitcoin's volatility subsides as both its market capitalization and liquidity are larger than ever (Mature Hard Money).*
17. *Early Bitcoin investors are now sitting on significant unrealized gains and are willing to part with some of their Bitcoin to pay for their purchases. With its purchasing power stabilized, the opportunity cost of transacting with Bitcoin is diminished and its use as a Medium of Exchange increases.*
18. *With the world more digitized than ever before, people increasingly demand to be paid in Bitcoin now that it has proven to be a good store of value given its disinflationary, and later deflationary, monetary policy (Schelling Point)(Hodlers of Last Resort — Layer 8).*
19. *With the addition of highly performant transaction layers, Bitcoin's use as a Medium of Exchange becomes a widespread. Bitcoin, functioning as the core of a new innovation wave called the TrustNet, is christened as a momentous innovation.*
20. *As more consumers and merchants become accustomed to transacting in Bitcoin, it gradually becomes used as a Unit of Account.*
21. *Due to the emergence of a superior, uninflatable monetary standard, people increasingly store their wealth in Bitcoin rather than fiat currencies (Minority Rule — Step 3)(Hodlers of Last Resort — Layer 9).*
22. *Central bank monopolies on money are described by historians as a relic of the past. Bitcoin is regarded as the catalytic innovation behind the separation of money and state. A free market for money is now the defining feature of free market capitalism (Nash Equilibrium).*

This path to full global money will take Bitcoin through many stages:



Time Will Tell

All time beyond the present is unknown. All predictions should always be taken with a grain of salt. The future is uncertain, and the end can always be near. Anyone who claims they can tell you what is going to happen in the future is wrong. All we can do is study the patterns of the past and use them as our map to navigate the ever-advancing territory of the future.

In a free market, hard money has always outcompeted soft money into extinction. Hard money has been the norm throughout all of human history, except for the past 100 years in which we have been coerced into using soft government fiat money. Societies operating on hard money systems optimize for the allocation of the ultimate resource, human time, which increases prosperity for everyone.

In the digital age, markets are increasingly interconnected. Bitcoin is digital cash money. It is a new social institution that lives in accordance with its own laws. Its core components are human self-interest and mathematics. Bitcoin is the hardest monetary technology in history. Will it continue to outcompete and win the throne of full global money?

Only time will tell.

Synthesized Works & Further Reading

- [1] [*The Bitcoin Standard: The Decentralized Alternative to Central Banking*](#) by Saifedean Ammous (a masterful work on which much of this essay is based)
- [2] [*The Rational Optimist*](#) by Matt Ridley
- [3] [*Skin in the Game*](#) by Nassim Nicholas Taleb
- [4] [*The Bullish Case for Bitcoin*](#) by Vijay Boyapati
- [5] [*The Age of Cryptocurrency*](#) by Paul Vigna and Michael J. Casey
- [6] [*Sapiens*](#) by Yuval Harari
- [7] *Bitcoin is a Decentralized Organism*, [*Part 1*](#) and [*Part 2*](#) by Brandon Quittem
- [8] [*PoW is Efficient*](#) by Dan Held
- [9] [*The Fifth Protocol*](#) by Naval Ravikant
- [10] [*Unpacking Bitcoin's Social Contract*](#) by Hasu
- [11] [*Antifragile*](#) by Nassim Nicholas Taleb
- [12] [*Letter to Jamie Dimon*](#) by Adam Ludwin
- [13] [*Placeholder VC Investment Thesis Summary*](#) by Joel Monegro and Chris Burniske
- [14] [*Diffusion of Innovations*](#) by Everett M. Rogers
- [15] [*Why America Can't Regulate Bitcoin*](#) by Beautyon
- [16] [*Hyperbitcoinization*](#) by Daniel Krawisz

Against Szabo's Law, For A New Crypto Legal System

By [Vlad Zamfir](#)

Posted January 26, 2019

Earlier this week (on Sunday night, in fact), I came across a definition and understanding of “legal systems” that has really cleared up a lot of things that have been weighing heavily on my mind for a long time. Here it is:

Legal systems are protocols for the management of disputes.

This includes protocols for preventing disputes and for managing the whole lifecycle of disputes, from inception to resolution. It captures both descriptions of these protocols (“legal code”) and their execution (“operation of law”). It might need to be refined, but it’s useful enough as given here.

Disputes arise in blockchain governance. We follow protocols for managing them.

Ergo, crypto law exists.

The purpose of this writing is to 1) document some of today’s crypto law, to 2) agitate for a change in crypto law; to convince the cryptocurrency community to abandon a crypto law (a law that I’m calling “Szabo’s law”), and 3) to agitate for the inception of a new crypto legal system.

I am prepared to die on this hill.

Crypto Law, Today

I have identified a number of crypto laws, and believe that the following three crypto laws are the most important laws in cryptocurrency today, in the sense that they are the most operative in the day-to-day management of disputes in blockchain governance:

Crypto Law #1: Don't Break the Protocol.

The spirit of this law is simple and natural. Disputes in blockchain governance are not to ever be resolved by the introduction of known critical bugs into the blockchain protocol. Critical bugs can cause the bridge to collapse, and there are people on the bridge at all times. Systemic collapse and noticeable degradation in the system’s quality always lead to disputes, and these disputes are to be avoided by preventing collapse.

It is the responsibility of developers, engineers, and architects to ensure that the software is maintained, that systemic failures don't occur, and that when they do (as will happen, because of the sorry state of the software development industry), to remedy the situation as quickly as possible.

Anyone can halt a proposal to merge a change to the blockchain protocol by clearly pointing out that a critical bug is introduced by the proposal. This is crypto law (in fact, and not because I have just declared it to be the case).

How this law is interpreted, however, can get complicated. Blockchain core developers have precise and detailed pictures of what is considered a breaking change, and what is not. Their views are generally overlapping (for example, everyone agrees that the system crashing or having a consensus failure is breaking), however, but they also have disagreements (for example, backwards incompatible changes are considered to be breaking changes in more cases in Bitcoin governance than in Ethereum governance).

Crypto Law #2: Keep Crypto Law Legal.

This one came as a surprise to me, so it might come as a surprise to you, too. Or maybe not!

Crypto law operates inside many jurisdictions of many legal systems and is very much structured by attempts to avoid disputes with/in these legal systems. Developers and other crypto people structure their affairs in an effort to prevent disputes that might be brought to (and by) existing legal systems. As a result, crypto law operates legally in the jurisdictions of these legal systems. At least for now.

Devs make technical decisions in order to minimize their exposure to possible liability; they will choose a solution that involves assuming less liability over one that involves more, all else being equal. They will often cite their concerns that something might be illegal under some existing legal systems, or that they will be sued for their exercise of power, as motivations for their decisions.

I am not commenting on the effectiveness of efforts to keep crypto law legal, but I want us all to observe that the management of disputes in blockchain governance are very much structured by attempts to avoid disputes with existing legal systems.

The cryptocurrency community didn't come up with this law. That crypto law is structured by existing legal systems is a natural consequence of the fact that crypto law operates in the jurisdictions of existing legal systems. And while for some participants in blockchain governance it may be possible to remain anonymous or somehow else avoid structuring their affairs in accordance with the operation of law, most participants in blockchain governance are public people who make an effort to

position themselves in a manner that doesn't get them in trouble with existing legal systems. Because of this reality, "keep crypto law legal" is crypto law. At least for now.

Crypto Law #3: Szabo's Law.

I'm naming this crypto law after Nick Szabo, since I am pretty convinced that he created it, popularized it, and brought it into crypto law. I'm sorry if I'm missing anyone else who deserves credit for it, but I'm just going to assume that Nick is responsible so I can keep my sentences short.

Szabo's law is simple: Do not implement changes to the blockchain protocol unless the changes are required for the purpose of technical maintenance.

It's called "blockchain governance minimization", but it can also justifiably be called "crypto law minimization", because of the following crypto legal consequence:

Crypto law does not (at least not crypto legally) manage disputes by making changes to the blockchain protocol, unless they are justified as needed tech maintenance.

It's a law that completely excludes other crypto legal processes from touching the blockchain protocol. Except as it is related to tech maintenance.

Nick Szabo has popularized (and legalized) his law in a few ways:

1. By popularizing autonomous software in the crypto legal form of smart contracts
2. By arguing that the minimization of responsibility for developers isolates them from legal risk
3. By arguing that crypto legal systems with Szabo's law are more socially scalable than systems with more legal and political power.

Nick's crypto law is responsible for a lot of the talk (and law) around the blockchain being immutable, and needing to remain immutable, and has justified decisions by developers to refuse to make changes to the blockchain protocol when they are engaged in blockchain governance disputes (for example in the Bitcoin block size debate). The DAO hard fork was a clear violation of Szabo's Law, and it offended Nick enough that he disowned Ethereum in favor of Ethereum Classic. But Szabo's law has been cited in Ethereum blockchain governance disputes after the DAO hard fork (specifically, in the still-unresolved stuck funds dispute). Indeed, Nick Szabo's law is often cited by core developers to justify their choices in blockchain governance disputes. Szabo's law is therefore crypto law.

In Awe of Nick Szabo's Crypto Legal Achievements

Before I dig in, I'm going to take the opportunity to express humility in light of the crypto legal work that Nick has managed to do, apparently working with only the power of his crypto legal mind, and his writings on blogs, mailing, and the like. It's an impressive—groundbreaking—achievement.

Nick Szabo forged a crypto law and popularized a legal theory that created software that is way more autonomous than society is capable of creating without the use of law.

In truly revolutionary cypher-legal-punk style, he created autonomous software with a crypto law and a legal theory that is profoundly and radically anti-legal and anti-political.

That the political and legal climate of the world was ready to embrace a legal theory and a law that is premised on the idea that legal and political processes are unworkable and need to be *ruthlessly minimized*, that software needs to be autonomous to be trusted is absolutely astonishing.

What a time to be alive!

Certainly Nick has vision and judgment—there is no way that the blockchain space could have gotten to where it is now, with crypto law the way it is, if people across the globe weren't jaded enough by the evolution of legal and political processes to be attracted to Szabo's law. Nick saw the opportunity and acted on it to create a truly global (crypto legal) revolution. It's really something remarkable. I am humbled by his insight, his foresight, and the effectiveness of his cypherpunk activist work.

And all things considered, it seems like cryptocurrency is going to remain more—or less—legal. At least for now!

So I take my hat off to you, Nick Szabo, in awe of your mindnumbingly brilliant and successful crypto legal activism! Thank you! No really—Thank you! Mad respect to you, sir!

But now—sorry Nick—I'm going to do my best to persuade the reader that we need to abandon Szabo's law as soon as possible.

Against Szabo's Law

Unfortunately for everyone, Szabo's radically anti-legal crypto law is too radically anti-legal to be part of a sensible crypto legal system. Szabo's law minimizes crypto law. It comes at the exclusion of all other crypto law that might be concerned with making

changes to the blockchain protocol. Hopefully you already see how absurd this is, but I'm going to spell it out as clearly as I can, in the following four parts:

1. Szabo's Law breaks Crypto Law #2 (Keep Crypto Law Legal)
2. Szabo's Law is politically loaded, not politically minimal, apolitical or anti-political
3. Szabo's Law has an insecure and aggressive legal posture
4. Szabo's Law is not a part of the most socially scalable crypto legal system

Szabo's Law breaks Crypto Law #2 (Keep Crypto Law Legal)

Nick Szabo sold blockchain developers on the idea that the minimization of blockchain governance and of crypto law would minimize their exposure to legal risk, by requiring them to exercise only the minimum amount of crypto legal power and judgement possible.

Unfortunately for these developers who probably had no legal training of any kind, Nick's legal theory is actually very stupid, and based on a naive interpretation of how existing legal systems will interact with crypto legal systems.

If the response when a legal system brings a dispute to blockchain developer is "sorry, we can't do anything for you", as it will almost always be under Szabo's law, then it has two natural reactions (assuming that the legal system believes that the devs can't do anything). The first is for the legal system try to handle the disputes without any recourse through changes to the protocol. The second is to minimize the damage caused by unresolved or irremediable disputes by making the use and development of the blockchain protocol illegal.

Szabo's firm hypothesis is that legal systems will be satisfied with their ability to manage the disputes that arise in blockchain governance but which cannot be remedied by crypto law thanks to Szabo's law.

I can imagine lots of possible disputes that can't be resolved (and will be ongoing) without changes to the blockchain protocol, and so my hypothesis is that Szabo's law will make cryptocurrency illegal in many jurisdictions. Disputes that are not being adequately resolved by crypto law will be brought to existing legal systems, who in turn in some cases will not be properly able remedy the situation because they cannot change the blockchain protocol.

It should not be surprising, but a crypto legal system operating on principles as anti-legal as Szabo's law will naturally eventually become illegal. As a result, Szabo's law is in conflict with Crypto Law #2.

I'm not done arguing this point, I am going to come back to it after describing the legal posture of crypto legal systems that adopt Szabo's law.

Szabo's Law is politically loaded, not politically minimal, apolitical or anti-political

While Szabo's Law is sold on the principle that politics is to be minimized, its crypto legalization was a deeply politically motivated act. I don't know what Szabo's political goals actually are, but it is safe to assume that he believes that they can be brought closer to reality by legalizing autonomous software into existence.

Not only does the legalization of Szabo's law determine governance outcomes (always in favor of not intervening with the execution of software), it minimizes the space for political and legal conversations that question whether those outcomes are desirable.

It locks blockchain governance and crypto law on a collision course with the consequences of creating autonomous software. It's impossible to predict all of the ways that this can go wrong, impossible to predict all of the disputes that will arise if we go down this route, but it is the route that Szabo chose for us based on his worldview.

He imagines a world in which crypto political and legal processes are necessarily going to go against either his personal preferred political outcomes, or against the public good, and therefore must be minimized.

This positioning makes sense if Szabo wants to do something very politically unpopular or something very illegal. It also makes sense if Szabo is so radically jaded that he believes that crypto law and politics cannot be worth the effort, no matter what form the crypto legal system might take.

But in either case, Szabo's clear intention is to use crypto law to determine blockchain governance outcomes without participating in blockchain politics (which, conveniently, is to be minimized according to Szabo's law). The legalization of Szabo's law was therefore a highly politically charged crypto legal action.

Szabo's law is not anti-political. It is a law that is aimed at shutting down political debate in order to guarantee Nick's preferred political ends.

I regard this kind of anti-social behavior to be [bad-faith participation in blockchain governance](#).

Szabo's law has an insecure and aggressive legal posture

I don't just mean that shutting down political debate is an insecure way to achieve your political goals.

Crypto law's current posture of "we don't deal with disputes that aren't related to maintenance" and "sorry, there's nothing we can do for you" is insecure and aggressive.

"We don't deal with disputes that aren't related to tech maintenance" is insecure in crypto law's ability to legitimately manage the disputes that might arise in blockchain governance.

"There's nothing we can do for you" is an aggressive posture, when someone has a legitimate dispute.

And why is crypto law insecure and aggressive?

Because of a radical law born of the view that politics and law are completely unworkable and not worth trying in any circumstance or configuration whatsoever. Because of Nick Szabo's insanely stupid crypto law.

Nick is insecure in his ability to participate in political and legal process, and in his ability to come up with legal systems that actively manage disputes, and his crypto law reflects it. He is very aggressive in his quest to create autonomous software, and his crypto law reflects it.

This legal posture is in direct conflict with Crypto Law #2. It invites conflict with existing legal systems. **Legal systems don't like to be involved in disputes with insecure, aggressive legal systems.**

Who does?

Nick's legal posture might be cool as a kind of radical cypherpunk crypto legal philosophy. Maybe. But it's not appropriate for blockchain governance, not today, and probably not ever.

Szabo's Law does not create the most socially scalable crypto legal systems

I don't think that Nick imagines that an aggressive and insecure legal posture is the most socially scalable legal posture. And it obviously isn't.

Nick believes that a crypto law that legalizes autonomous software will form a better basis for socially scalable society than is possible under any conceivable crypto legal system that is more political or legalistic.

I am very skeptical about his position, because I don't believe that autonomous software is at all safe, you know, for humans in society.

Nick knows that autonomous software isn't always going to be legal or politically popular, and he is determined to use crypto law to shut down any legal and political coordination that would undermine his mission. This antisocial behavior makes me question whether Nick is even concerned with the social scalability of public blockchains.

Assuming that Nick has good intentions, then I am absolutely certain that Nick Szabo is not the best legal thinker in the world. Someone can come up with crypto law that is more socially scalable than the crypto law Nick came up with so he could bring autonomous software into the world. *There's no doubt about it.*

Maybe enough people are as radically paranoid of legal and political processes as Nick that even a slightly more reasonable crypto legal system will be broadly seen as untrustworthy. I don't know. But I'm ready to have faith and to bet my life that we can do much, much better than the insecure, aggressive crypto law we have today.

A much more secure crypto legal posture is possible if we abandon Szabo's law

Crypto law doesn't have to be this way.

Legal realities do not warrant the posture of today's crypto law.

Cryptocurrency is more-or-less legal. We need to relax.

Szabo's law is anti-legal and anti-political. We need to abandon Szabo's law to adopt a more open and secure legal posture. One that acknowledges rather than shrugs off its responsibility to carefully manage disputes. One that does not write crypto law to push politically unpopular outcomes on society. We can't adopt a secure and open crypto legal posture without first abandoning Szabo's law.

But we don't need to know anything about the future of crypto law to assume a more secure posture, and benefit from the more comfortable position. **We can immediately embrace a much more correct position, one that does not change crypto law except by abandoning Szabo's law:**

Crypto Law is responsible for managing disputes in blockchain governance, and making sure that they are resolved via legal processes that don't break the protocol.

Crypto law is still nascent, and I have no clear picture where it will go in the future. But I don't need to know where it will go to see that it needs to abandon Szabo's law in order to develop in a healthy way.

We cannot foresee the nature of all of the blockchain governance disputes that will arise in the future, and need to retain the ability to remain flexible enough to adapt to changing circumstances, we cannot afford to blindly pledge our fates to a future with autonomous software.

We have crypto law because we have protocols for managing blockchain governance disputes. We need these protocols to be sensible, so that we don't create unnecessary headache and hardship when disputes arise. We need to believe in our ability to manage blockchain governance disputes based on sound crypto legal work—which means not breaking the protocol and keeping crypto law operations legal—at an absolute bare minimum.

We should admit that we need more legal principles, and more crypto law. We should admit that we need to come to a new understanding of how disputes in blockchain governance ought to be resolved.

We should admit that we collectively have an obligation to manage the disputes that will arise from the operation of global public blockchains to the best of our crypto legal ability, so that as many people as possible can enjoy the benefits of global public blockchains.

This secure, open-minded posture is much more comfortable than the aggressive, insecure posture we have today.

I hope you're already feeling more comfortable!

If crypto law fails to tactfully manage disputes, the result is more plausibly going to be that blockchains (and the operation of crypto law) become illegal, than that blockchains remain legal and autonomous and become as widely adopted as Nick Szabo imagines they will. The only way the law-abiding public can have the most benefit from global public blockchains is with a new crypto legal system.

For A New Crypto Legal System

Nick Szabo took it upon himself to use crypto law to summon autonomous software.

In response, we must take it upon ourselves to use crypto law to conjure up a new crypto legal system, one that is able to keep Szabo's beast in check.

I am calling upon crypto law people to recognize that they uphold principles of law that are incompatible with Szabo's law.

I am calling upon crypto law people to strike down Szabo's law, and to establish a new crypto legal system in its wake.

No one should do this alone. Not me, not you, not Nick Szabo. It needs to be a global best effort that taps into the best legal thought available, that is rigorously treated by the best legal minds on the planet, from as many legal traditions and schools of thought as possible. We can't afford to screw it up. And we have no idea how it's going to turn out.

We can't let Nick Szabo stop us from establishing a new crypto legal system. His paranoid conviction that legal systems are completely unworkable and are best ruthlessly minimized cannot be justified by impartial reasoning in legal or political analysis. The genius crypto legal footwork that Nick did to legalize Szabo's law is an impressive feat, and says a lot about our current legal and political climate, but his legal theories are not a sound basis for any system of crypto law.

His attempt to create autonomous software that is above any (other) law must be foiled by law people who are able to see through Nick's bogus legal theories.

But we must stand in awe of the astonishing success of Nick Szabo's law, and of Nick's evident ability to tap into the distrust that permeates the modern legal and political climate.

And we must pay due tribute to the legal and political climate that legalized Szabo's law.

Nick Szabo's crypto law does not do it justice!

If no one should be in charge, then how does Nick Szabo get to use crypto law to ban us from using crypto law?

Nick is insecure about his ability to participate in politics and law, and he wants to use the force of law to conjure up autonomous software, and he doesn't want us to have a say in the matter.

So why should we take tips from him about how we should handle disputes?

And why should *he* write *our* laws? How does he imagine that he can deny us our ability to create our own crypto law?

Nick Szabo's personal effort to minimize our use of crypto law is not a good crypto legal embodiment of the ethos of our sociopolitical movement today, and it never was.

We need to stop buying into his bullshit.

I don't trust Nick Szabo to write our laws, or to have sound, impartial judgment about how we should prevent and resolve disputes. And neither should you. Nick Szabo does not represent me, and I am sure that letting Nick dictate our future is not what decentralization is about at all.

Crypto law is a collection of protocols for handling and preventing disputes that arise in blockchain governance.

Nick Szabo has a narrow imagination for what crypto legal systems can be like, and doesn't even bother thinking about it too much because he categorically dismisses all non-minimized crypto legal systems.

Nick is a visionary cypherpunk activist, that's for sure, but the legal and political theories that he spreads do not reflect sound, impartial judgement. They reflect his insecure and aggressive crypto legal style.

I will not follow his lead.

Crypto law isn't decided. It isn't final. Law doesn't ever actually operate like that. It's an institution that humans use to coordinate the management of disputes. We can always coordinate politically to create new institutions, although it may not always be easy.

Crypto law doesn't need to be Szabo's law.

And I don't think anyone has the ability to defend Szabo's indefensible law.

Nick Szabo says that crypto law is decided and that it must be minimized. But Crypto law isn't decided, and it must not be minimized.

Nick Szabo wrote and decided on the "decided" crypto law himself, and he propagated legal theories in order to legalize it so that he could have autonomous software.

But crypto law doesn't need to be Szabo's law.

We need to be free to build a crypto legal system that embodies the ethos of the blockchain space, one that we can actually be proud of, as opposed to Nick's insecure and aggressive crypto law (that we should be ashamed of).

We cannot allow Nick Szabo to stop us from using crypto law.

Crypto law will become more secure when we let go of Szabo's law. Crypto law without Szabo's law doesn't suddenly become centralized, hierarchical, or captured by existing legal systems.

Even without Szabo's law, [crypto law has technical and legal limitations](#), and it is up to crypto law people to have the judgement to make sure that crypto law operations are not in violation of Crypto Law #1 (Don't Break The Protocol) or Crypto Law #2 (Keep Crypto Law Legal).

But notwithstanding the technical and legal constraints that we cannot escape, crypto law can be almost anything we can imagine, and it can develop to match our changing circumstances.

The future of crypto law isn't set in stone. It depends on crypto legal actions taken by crypto law people.

For my part, I will start by attacking the legitimacy of Szabo's law.

And if the stars align and I have the opportunity, I will break Szabo's law.

Sue me. I don't care. I am prepared to die on this hill.

Links

- https://medium.com/@Vlad_Zamfir/how-to-participate-in-blockchain-governance-in-good-faith-and-with-good-manners-bd4e16846434
- <https://medium.com/@VitalikButerin/i-replied-why-i-disagree-with-your-anti-immutability-position-not-the-same-as-disagreeing-with-93694b565e2b>

In Defense of Szabo's Law, For a (Mostly) Non-Legal Crypto System

A Lawyer's Response to Vlad Zamfir's "Against Szabo's Law, For A New Crypto Legal System"

By [Gabriel Shapiro](#)

Posted January 26, 2019

Lawyers! Are you sick of devs holding all the power in blockchain-land? Do you wish you could go back to the good ol' days when devs came to you with questions about how their software comports with the law instead of you going to devs with questions about how the law comports with their software? Do you feel (or secretly suspect), like no-coiner crypto-lawyer Angela Walch, that it's puzzling to "[act as if blockchains are all about math or science when they are really just about people deciding to work together...](#)"?

Becalm thee! Rejoice! Vlad Zamfir, a leading Ethereum developer and sharding theorist, has [announced the birth of "crypto-law."](#) Now you can again feel relevant by helping define a new, bespoke legal order specifically applicable to the social governance of blockchain technology (& presumably agreed upon and enforced among some cross-section of devs, users, miners, exchanges, police forces and legislators? but query how that works...). Your job security is assured! Your social standing, restored!

Unless, like me, you think that "crypto-law" in Vlad's sense is something only a non-lawyer could dream-up, and while it may represent the kernel of a very interesting, creative and intelligent approach to blockchain, is in dire need of—well, for lack of a better word, some lawyering.

I'm trying to keep this brief and informal, so, without further ado, I'll just say I disagree with aspects of Vlad's proposal (though think he has the kernel of quite an interesting idea) and present a somewhat hastily hacked-together mix of criticisms and proposed alternatives in the three core proposals that follow:

1. *We stick with REAL law about crypto rather than trying to invent "crypto law."*

What is "REAL law about crypto?" Well, it turns out a lot of it already exists, in the form of statutes and common law (including the common law of contracts, which allows for a high degree of private ordering), even though the vast majority those laws do not expressly mention (and were articulated long before the invention of) blockchain technologies.

Admittedly, some of this law suffers from either or both of two problems:

(a) Existing law can have gaps regarding blockchain tech, and these gaps should be filled—which can happen when legislators amend, or courts construe, old laws to cover new tech like blockchain. A great example of this can be found in [Wyoming's pending addendum to the Uniform Commercial Code](#), which attempts to gap-fill the UCC by defining different categories of blockchain tokens, tying them to the traditional UCC rules for a given category where reasonably possible, and creating new rules where necessary—for example, by creating a new concept of “control” for the perfection of security interests in blockchain tokens.

(b) Existing law can have bad (unintended?) consequences or innovation-stifling results when applied to blockchain. Again, this can only be solved by changing the law legislatively or judicially through normal political-legal processes. An example of this, in my personal opinion, are the U.S. federal securities laws, some of which make sense as applied to blockchain (anti-fraud, some disclosure requirements), and some of which don't (Sarbanes-Oxley anyone?)—but which the SEC largely seems to currently believe should apply to many blockchain tokens on a largely wholesale basis. The solution for such issues is to engage with regulators to the extent they have authority to grant waivers and modifications of existing law appropriate to blockchain, or, where that approach is insufficient, to prevail upon judges or legislators to modify the applicable law insofar as it pertains to blockchain.

Despite the limitations described above—which we would expect apply to ANY highly innovative and thus “disruptive” new technology—law is law: the vast majority of it already exists and has enjoyed centuries of testing, debugging and (mostly) conservative, incremental optimizing. Whatever changes need to be made to it to accommodate a new technology like blockchain (and of course, as described above, there are some) cannot be just decided by Vlad Zamfir and other denizens of the blockchain (chainizens? blockchainites? popolo chainos?), no matter how many of them there are or how broadly they agree on it. Rather, the most Vlad and other blockchain devs/users can do is one or both of the following:

→ engage in the traditional law-making/influencing process by doing things like lobbying, writing influential thought pieces, voting for the politicians and judges they think will represent their interests when it comes time to legislating and adjudicating, etc; and/or

→ enter into contracts (which to be contracts must comply with real contract law, not “crypto law”) to agree among themselves to a certain set of governance rules as a matter of private ordering.

Note: The second possibility (private ordering via contracts) is actually really, really powerful, and is a path that could enable chainizens / blockchainites / popolo

chainos to do more with law, more quickly, in sort-of-but-not-quite the way Vlad Zamfir might like, than creating a whole new “crypto legal system.” I talk more about this possibility at the end of the article, but, for now, suffice it to say that’s part of my recommended approach and ultimately means I don’t disagree with Vlad nearly as violently as it might appear so far.

2. We Preserve Space for the Exploration of Szabo’s Law by Letting the Communities Who Want to Use It Do So

A. What is Szabo’s Law?

Vlad describes “Szabo’s law” thusly:

Szabo’s law is simple: Do not implement changes to the blockchain protocol unless the changes are required for the purpose of technical maintenance.

Most people may not notice it, but defining this as a law, as a law believed by Szabo, and as meaning exactly this “simple” thing are brilliant rhetorical maneuvers on Vlad’s part that, if we let them slip by unquestioned, could win half the debate before it has begun. Therefore, we must not do that.

If you read Vlad’s article closely it becomes clear that his critique is not restricted to this “law” of Szabo’s (which, to my knowledge, Szabo has never defined, and certainly has never defined as a “law”), but rather to what one might more ordinarily and naturally refer to as an “approach,” “philosophy” or “ethos” of Szabo’s. For example, he repeatedly refers to Szabo as being “insecure” and to various ancillary behaviors of Szabo (described in a not terribly flattering light) that have supposedly bolstered the spread and acceptance of “Szabo’s law.” Thus, it is clear that Vlad has beef not only with the simple “law” or rule he calls “Szabo’s law,” but rather also the cluster of norms, assumptions and objectives associated with that “law.”

Although I don’t agree that the thing Vlad is criticizing is a “law” and think it is extremely confusing and counterproductive to refer to it as such, I **do** agree it is a very real cultural force in the blockchain world and is sufficiently discrete that it can be reified, held up, reviewed and criticized, lauded or built upon. Unlike Vlad, I don’t refer this real thing as “Szabo’s law,” but rather as the “social-trust-minimization approach” to blockchain technology. While various people have described and advocated for this approach in various ways at various times, I think it is justly traced to the most articulate and famous expression it has received to date and a personal favorite of mine: Szabo’s paper “[Money, blockchains and social scalability](#).” Thus, I do not disagree that Vlad is criticizing a real thing—the social trust minimization approach to blockchain—and that Nick Szabo is the poster-boy for that thing.

Nick Szabo and I have one thing in common: we're both lawyers (although in Nick's case he may not be practicing, he has a J.D. and is a very keen and longstanding student of the history of law, and that makes him a lawyer in my book). The similarities end there, since Nick is far more technically adept than I am and spent years developing revolutionary software, and I would venture to guess that I am more legally adept than Nick and spent eight years doing high-stakes deals for real high-stakes clients at real AMLAW10 law firms. But in this case, our similarity in both having a DEEP understanding of the law (rather than one developed mainly, by Vlad's own admission, by reading what I consider a very controversial, scatter-shot and uneven blockchain-focused legal blog) explains why we'd likely both see the merits of social-trust-minimization and arrive at similar conclusions on the issues Vlad raises in his article.

I invite anyone who doubts the merits of at least exploring where social-trust-minimization-via-blockchain can take us to do one simple thing: read Nick's article. I don't have much to add to that, beyond referring back to the gloss I gave it in my article "[Tokenizing Corporate Capital Stock](#)":

[F]rom a pure performance point of view, blockchains suck. Worse still, there is nothing that blockchain technology can do that can't be done on a network utilizing a so-called "client-server/master-slave architecture" ...Worse worse still, since these "client-server/master-slave" architectures can rely on centralized coordination mechanisms to achieve byzantine fault tolerance and sybil resistance, they are faster, cheaper and easier to use [than blockchain technology]. Thus, blockchain technology's "unique selling point" (USP) for most applications is not "doing the same exact thing as centralized technologies, but materially faster, cheaper and more conveniently." ...[Instead, t]he USP of blockchain technology ...is that it furthers the values of individual asset sovereignty by creating the technological predicates necessary for ordinary persons to hold, manage and transact with assets in an environment that is [socially-]trust-minimized while also being secure.

This is the **real** Szabo's law, and how it relates to blockchain, in a nutshell.

B. What is Zamfir's Law?

What does Vlad want instead of the Szaboist (Szabbic? Szaboean?) social-trust-minimization approach? Well, it's frankly a little hard to tell, but one way of interpreting him would be that he would like chainizens to come together and define their own "laws" (albeit not really "laws" — more like just a socially agreed

ruleset) for how/when/where to fork blockchains/blockchain protocols, so that they could be forked relatively often, delivering swifter “justice” to the wronged, ensuring the enforcement of non-crypto-law and crypto-law on the blockchain, and facilitating blockchain innovation at a faster pace. So, what I surmise that he wants is a body of rules (including, presumably, meta-rules for how those rules can be amended or supplemented) that everyone agrees on after a long debates whereby, if, for example, Parity has lost funds due to a hack, Parity can submit the issue through some kind of social process (query what that is) and that process would work swiftly, decisively and legally to determine whether, how and in what amounts the funds should be returned to Parity via a fork.

Does this sound familiar at all? It should. IT’S BASICALLY THE CURRENT LEGAL DISPUTE MECHANISM PROCESS, BUT APPLIED TO BLOCKCHAIN UNDER A NEW QUASI-LEGAL SET OF RULES AND A NEW QUASI-LEGAL SET OF JUDGES/LEGISLATORS/REPRESENTATIVES AT THE BEHEST OF A NEW QUASI-BLOCKCHAIN-GOVERNMENT. Essentially what it appears Vlad would like to do is create an entire crypto legal system that runs parallel to, but outside of, without conflicting with or being in violation of, the traditional legal system. Vlad, if I have that wrong somehow, feel free to pipe up and correct me, but you have to admit that although you have been very clear about your critiques of immutability, you have not been very clear in the alternative about how/when/where mutability decisions would be made under your vision—so, in fairness, I don’t have a whole lot to work with on the latter score.

Let’s call the law that such a system should exist and should govern blockchains “Zamfir’s law”.

While Zamfir’s law represents an admirable/interesting goal, it is also arguably a very wasteful and implausible one. WE ALREADY HAVE A GREAT LEGAL SYSTEM, BUILT OVER CENTURIES. At least in the United States and other highly developed parts of the world, that is. It becomes a very reasonable and natural question to ask why we think “crypto law” patched together by a maybe motley (albeit maybe lovable) group of crypto enthusiasts is likely to do much better—at least at scale (again, see below under #3 for some contrary points re: private ordering).

C. A Hypo: Why Do Szabo’s Law and Zamfir’s Law Conflict?

To understand why/how Szabo’s Law and Zamfir’s law may conflict, and why Szabo’s law (or, really, Szabo’s social-trust-minimization approach) is something worth preserving/exploring, let’s consider a variation on a hypo that personally has been very influential in exciting me about smart contracts on the blockchain and the potential value of social-trust-minimization as applied thereto.

1. You live India.

2. I live in the United States.
3. We meet on /r/mechmarket and I learn you have a fancy custom keyboard — brass weight, carbon fiber plate, HHKB layout, retooled vintage nixendorf switches, full RGB with hotlites, types like a dream—I'd like to buy.
4. We have the idea of entering into a contract where I agree to buy and you agree to sell your keyboard for \$1,000.
5. For keyboard deals, payment in advance is customary, and, moreover, you are not willing to send me the keyboard unless I first pay you the funds.
6. But in doing my due diligence, I learn that India has a notoriously inefficient, byzantine legal system that is hard for even Indians (no less Americans like me) to navigate successfully—clearly, if I pay you, but you breach the contract by failing to deliver the keyboard, I am effectively going to have no remedy, since there is no way I am going to endure the time and expense of suing you in India—particularly since it's unlikely I'll get a satisfactory remedy even if I do.
7. I therefore consider doing the agreement under U.S. law, but then realize that even if I clearly, quickly and efficiently prove a breach of the contract under U.S. law, it will do me no good unless I can enforce the judgment in India where you and the keyboard reside—thus all the problems of the Indian legal system remain unavoidable.
8. But, I have an idea—"let's do the deal through a trusted intermediary!" "If we use PayPal," I say, "PayPal will effectively insure me against the possibility of your fraud. If I don't get the keyboard from you after paying for it, PayPal will refund me. While that's not as good as being able to get "specific performance" of the contract as a remedy (i.e., a court forces you to deliver me the keyboard you agreed to sell) like I would be able to do if you were in the U.S., at least I will have a remedy, which is better than no remedy, and I think for the sake of being able to do a deal to get this dank-ass keyboard, that's a risk I'm willing to take."
9. You don't like that idea, though, you tell me, because PayPal places almost all the risk of a fraud claim on the seller. PayPal also charges the seller transaction fees, which is part of how it makes economic sense for PayPal to insure the risk of fraud in these types of transactions—in effect, me using PayPal means I am paying a lower price for the board as a discount reflecting my distrust in the Indian legal system. Finally, you note that it so happens you have been burned by PayPal before—you sent someone a keyboard bought through PayPal, and the buyer attempted the non-blockchain version of a "double-spend" by immediately filing a claim with PayPal for non-receipt, which resulted in the purchase price funds being held-up at PayPal for six months while PayPal investigated the claim. Even worse, PayPal got it wrong and decided against you, and thus you were out both your keyboard and your funds, with no effective remedy—since you were no more willing to wind your way through U.S. courts for a \$1,000 claim than I would be willing to wind my way through Indian courts. You will never forgive PayPal, don't trust PayPal, and believe PayPal has a pro-American bias and will never give you a fair shake.

10. I don't trust India's legal system, and you don't trust my proposed intermediary (PayPal) that would enable me not to trust India's legal system. What do we do?
11. *The Arena Lights Dim*
12. *Metallica's "Enter the Sandman" Fades Up*
13. *Lights Start to Twinkle, Digital Coins Cascade on the JumboTron*
14. *Blockchain Enters the Arena, Strutting like Ric Flair in his Prime, to Thunderous Applause*
15. What about this? Let's say you know code, I know code, and we both have a strong confidence level about the way a particular blockchain and code on it works. What could we do then?
16. Although you don't trust PayPal, and I don't trust India's legal system, in general, any two people can find at least one other person they both trust. And in this case we have —/u/Ripster—a paragon of virtue, a hero, a legend in the mechanical keyboard community, who (we'll posit) conveniently happens to be located in the United States within driving distance of me.
17. Now, couldn't we do something like this?

→ deploy a smart contract on Ethereum that we both feel we understand

→ I deposit \$1,000 worth of ETH there

→ the smart contract gives Ripster's private key the sole authority to either send the \$1k to you (upon successful delivery of the keyboard) or back to me (if keyboard isn't delivered by deadline x)

→ you mail the keyboard to Ripster

→ Ripster releases the ETH via a transfer command sent to the smart contract, signed by his private key (or first shows me the keyboard so I can inspect it and then releases the ETH)

→ I take the keyboard from Ripster.

THIS IS MY (AND, I SUSPECT NICK SZABO'S) DREAM FOR BLOCKCHAIN. One can play with the details and probably imagine ways that social trust can be even further reduced, but the point is that this technology opens up massive, massive opportunities to enhance dealmaking through private ordering. Deals that wouldn't be done, or would only be done more expensively or with more problems and risks, can get done, or get done more cheaply or with less drama, leveraging blockchain than not. Or, at least, such is the dream—it is up to us to make it a reality.

However, you know what could really potentially limit the value of this dream? That's right, you guessed it—Zamfir's law could. Notice again #15 in my hypo. For this

scheme to break our dealmaking logjam, it is critical that we eliminate all forms of trust other than the two forms of trust we happen to share—social trust in Ripster and mathematical/computational trust that such-and-such smart contract code deployed on such-and-such blockchain will lead to such-and-such predictable results. But if the blockchain can be changed through a socio-legal but extrajudicial “crypto-law” process, there is an additional piece of social trust we need beyond that of our shared trust in Ripster—trust in “crypto law” and the people that apply it. To me, this is a major problem and could drastically undercut the potential benefits of blockchain.

Of course, Vlad and critics like Angela Walch will point out that such trust is always needed—even Bitcoin, the most change-averse blockchain, *can* be changed, and thus in using Bitcoin I am “trusting” those who could change it adversely will not do so. But, as a general matter, what is easier to trust:

(a) a blockchain “governed” by a highly ingrained, time-honored and widely touted “Szabo’s law” that both in theory and practice means the blockchain is almost never changed except for super important reasons that nearly any reasonable person would agree upon? or

(b) a highly complex Zamfir’s law/“crypto law” that, in practice and by design, entrusts the decision of whether, when and how the blockchain is changed to a group of people, the complex principles they have agreed upon and the particular way that they might decide to apply those principles in a given case?

I would submit that, in general, the blockchain governed by Szabo’s law is easier to trust, and thus in a certain sense helps “minimize trust,” or minimize the amount or complexity of trust, that is needed to facilitate private ordering via blockchain, whereas Zamfir’s law vastly increases such trust, and thus begs the question of why blockchain would even be preferable to existing alternatives that also require high amounts of social trust. ***After all, isn’t it possible that you distrust “crypto law” and its administrators just as much as I distrust Indian law, and that therefore by using blockchain we would merely shift, rather than solve, the trust problems that led us to consider using blockchain in the first place?***

On the other hand, here is what I will acknowledge: people can have very different preferences for what they place their trust in. Some people (presumably like Angela Walch) see everything as “ultimately being about people” and have little faith in or desire for automatic, mathematical decision-making. Others (like me and presumably Nick Szabo) think there is huge promise in being able to make deals while minimizing the number of people, social variables and social institutions that must be trusted to do so, and the degree of trust that must be placed in those things to whatever extent such trust is needed. It’s a free world, and there’s lots and lots of

room to have different technologies, and even different blockchains, that cater to those varying preferences.

This brings me to my next point.

D. Why Are Szabo's Law and Zamfir's Law, Despite Conflicting, Not Mutually Exclusive?

I think [Reluctant Raccoon](#) put it well:



Long story short: there are different blockchains. Some can use Zamfir's law. Some can use Szabo's law. One can even fork a given blockchain that uses Zamfir's law or a given blockchain that uses Szabo's law, and try convincing people to instead apply Szabo's law to the forked version of the former or Zamfir's law to the forked version of the latter. We can let the market and history decide which approach is better (either absolutely for all purposes or relatively for some purposes). There is no need to call for a repudiation of either, or to condemn either. Let the world experiment.

3. We Preserve Space for the Exploration of Zamfir's Law by Letting the Communities Who Want to Use It Do So – But Through Private Ordering (Contracts) Rather than “Law”

As described above in point #1, in my opinion “crypto law” as Vlad seemingly conceives it (something voluntarily agreed upon by a cross-section of blockchain people) is neither a necessary nor viable alternative to what I’ll somewhat comically call “legal law”—I mean real law, the law established by states and enforced by threat of coercion in the form of violence, imprisonment and/or deprivation of property. You know, “old-fashioned” law—your Dad’s dad’s dad’s law.

HOWEVER, you know what Vlad’s “crypto law” sounds like, aside from the ill-advised name for it? Oh, I don’t know, how about “governance agreed to via contract in a system of enforceable private ordering”? I know that’s a mouthful, but isn’t that, at the end of the day, both what he is apparently really proposing and all he really needs? Corporations do this. LLCs do this. Private parties making deals do this. All the freaking time. And legal law, real law, helps them.

I don’t really like/support EOS, but one interesting feature of EOS is that it combines blockchain tech with wet contract tech via a purported “[constitution](#)” written in natural language and inscribed to the EOS blockchain in a Ricardian fashion. I’ve been very critical of the particular way the EOS powers-that-be decided to implement that approach, and one can query whether their constitution is enforceable and quibble with the extra-legal manner in which it has been enforced. Also, in general I share [Vlad’s concerns about on-chain governance](#) (and so really I just disagree with him, as I hope I’m elucidating here, about the extent to which blockchain governance (whether on-chain or off-chain) is necessary or advisable).

However, the core of the idea behind the EOS constitution—i.e., combining blockchain technology with a sort of contractual “terms of service” and potentially a “terms of forking” for its various users/maintainers—is very interesting and potentially powerful, and might be a great way to implement ideas like Vlad’s within the framework of existing law.

For example, AFAIK there is nothing to stop Vlad from forking Ethereum, declaring that his version of Ethereum can only be used in, modified by, or participated in by people who sign (under whatever meaning of “sign”—might include a click-through agreement) a contract that agrees that all disputes regarding stuck funds, hacks, forks, whatever other issues will be decided by a “Council Of Vladdites” who follow “Crypto-Law”—as defined on Exhibit A thereto and as it may be amended or supplemented from time to time pursuant to Crypto Law #5 regarding amendments. That would seemingly achieve most of what Vlad wants to achieve by rejecting Szabo’s law, but would not do so at the expense of eliminating the existence of systems that happen to like and/or just want to play with and explore the possibilities of Szabo’s law.

I would humbly ask—what is wrong with this version of “crypto-law”? What is wrong with an approach that utilizes current truly legal contract law to allow a community of like-minded people to come together and have a sophisticated blockchain

governance system for a particular blockchain, thus enabling it to fork often? I see nothing wrong with it. I'd even love to see it adopted and experimented with, and of course as a lawyer I would kill to be able to help advise what the contractually agreed "crypto law" should like. As a lawyer it'd be like advising on one of the coolest deals of all time—a deal to set up a platform for deal-making!

But I also do not see why this model should be universal or why it should be the **only possible** type of blockchain. And one question I have for Vlad is whether that is part of his position, or whether he just wants crypto-law to be one of many options for blockchain. One might argue (and I suspect, but am not sure, that Vlad would/will argue) that blockchains are "too dangerous without crypto law".

But why? "Legal law" still exists, no matter what we do, and legal law can regulate blockchain's dangers just fine. Maybe not **perfectly**, but fine. And such law will continue to evolve, and get better, as we lawyers grapple with this fascinating new technology. Why presume in advance that it is unworkable and try to impose a parallel "crypto law" that essentially depends on the existence of a new "crypto state"? For all we know, the "cure" to blockchain's supposed dangers could end up being more corruptible and dangerous than the disease. And, if experience is any guide, when new governments/legal systems are set up from scratch, they usually suck, give power to weirdos, and end up as catastrophes. There is good reason to be cautious.

Conclusion

Vlad is quite a brilliant and interesting fellow, and I'm glad he's working on and publishing his ideas—including those about blockchain governance and "crypto law." That doesn't mean I can't criticize them. Just as if I were to write some screed about some aspect of coding, I would most likely badly mangle it in one way or another, but maybe also strike upon some interesting ideas, I analogously believe (truly without knee-jerk condescension) that Vlad is missing quite a few nuances about law and governance as he has ventured into legal terrain while being a non-lawyer. **BUT**, to Vlad's credit, there is nevertheless quite an interesting idea he has implicitly cottoned onto—namely, that of combining blockchain technology with the power of private ordering via legal contracts. I would humbly suggest that this (perhaps combined with some real legislative and regulatory lobbying), rather than proclamations about how blockchain governance should be, what "crypto laws" should be created, etc., would be a much more constructive frame within which to tackle the issues Vlad is, very very rightfully, concerned about regarding the maximization of blockchain's benefits and the minimization of its harms.

I would welcome further dialogue with Vlad or anyone else interested in these topics.

Links

- https://twitter.com/angela_walch/status/1083069503335002112
- https://medium.com/@Vlad_Zamfir/against-szabos-law-for-a-new-crypto-legal-system-d00d0f3d3827
- <https://wyoleg.gov/Legislation/2019/SF0125>
- <https://unenumerated.blogspot.com/2017/02/money-blockchains-and-social-scalability.html>
- <https://gabrielshapiro.wordpress.com/2018/10/28/2/>
- https://twitter.com/ypical_
- <https://github.com/EOSIO/eos/blob/5068823fbc8a8f7d29733309c0496438c339f7dc/constitution.md>
- https://medium.com/@Vlad_Zamfir/against-on-chain-governance-a4ceacd040ca

A Conflict of Crypto Visions

Why do we fight? A framework suggests deeper reasons

By [Yassine Elmandjra](#) and [Arjun Balaji](#)

Posted January 29, 2019

Conflicts raging within “crypto” are endless. Heated debates take place on a wide spectrum of issues, with little attempt to devise compromises acceptable to both sides. Interestingly, it is the same people who consistently position themselves on opposite sides of these issues. From monetary maximalism and wealth distribution to governance and consensus algorithms, the issues vary tremendously while the formed groups of opposition remain the same. Naturally, this creates an unproductive habit of each side blindly talking past the other.

In [A Conflict of Visions](#) and [The Vision of the Anointed](#), political economist and social theorist [Thomas Sowell](#) argues that this phenomenon comes from fundamental differences in people’s assumptions about the nature of systems and their limitations. While seldom consciously recognized, these sets of assumptions are the largest drivers influencing people’s opinions. Since visions are rarely examined but have profound impact, Sowell introduces the “conflict of visions” as a mechanism to think about these assumptions.

By highlighting how these assumptions play a fundamental role in shaping our views, we shed light on the “conflict of visions” and ideological battles raging within proponents of cryptocurrencies.

We begin our analysis by laying out the framework of conflicting visions. Using this framework, we proceed to explain the conflict of “**crypto**” visions. From an understanding of the conflict of crypto visions, we then comment on the structure of arguments taking place within crypto, before diving into the meat of our analysis: an exposition of four episodes exemplifying the conflict of crypto visions.

Setting The Scene

- I. Defining Visions
- II. The Conflict of “Crypto” Visions
- III. The Structure of Arguments

Episodes

- IV. Episode 1: Monetary Maximalism vs. Multicoinery
- V. Episode 2: The “Fairness” of Crypto Distribution
- VI. Episode 3: Governance
- VII. Episode 4: Proof-of-work vs. Proof-of-stake
- VIII. The Future Remains To Be Built

Defining Visions

In order to understand the conflict of “crypto” visions, it is important to first establish *what a vision is* per Sowell’s work. Simply, a vision is a gut feeling about how things *should* work—a set of assumptions about the limitations and nature of the world that enables someone to understand (or at least believe to understand) why things work the way they do. Sowell defines two opposing sets of assumptions and assigns them the terms “constrained” and “unconstrained.”

Constrained Vision

At the core of each vision is some strong belief or recognition of limitations. Those with a constrained vision see certain realities as unalterable, “scarcity, self-interest, human fallibility, evil.” [1] Under the constrained vision, the only way to improve is to understand the fundamental laws of nature and the only way to innovate is to remain consistent with the specific parameters set forth by these laws.

The constrained vision realizes that while A may be better than B, it does not matter if A simply cannot be done. For instance, while achieving flight by wishing away gravity or ending war by wishing away violence would be great, it is simply not within the realm of possibilities. Consistent with the constrained vision are concepts like Smith’s [Invisible Hand](#) and Zhuangzi’s [Spontaneous Order](#), which recognize the limitations of man and prescribe ideas that transform these limitations into progress.

The constrained vision encourages decision making by identifying tradeoffs rather than solutions. Given the limited options available, the constrained vision attempts to make the best trade-offs with an understanding that “unmet needs” will necessarily remain. As such, “particular solutions to particular problems are far less important than having and maintaining the right processes for making trade-offs and correcting inevitable mistakes.” [2]

Unconstrained Vision

Those with an *unconstrained* vision believe that the only limitation to achieving a desired outcome is our lack of imagination. Through this lens, the underlying problems in any system exist only because people are not wise, caring, imaginative, or bold enough: with the right mindset, scarcity can be eliminated, man’s self-interest can be corrected, imperfections perfected, and all evil eradicated. Instead of

building mechanisms to work around any fundamental limitations, the unconstrained vision sees it possible to re-engineer the world to eliminate its flaws. As such, “intractable problems with painful trade-offs are simply not part of the unconstrained vision.” [3]

The questions posed under the unconstrained vision are centered around how to remove particular negative features in an existing situation to create a solution. By doing so, decision making boils down to choosing the perfect solution instead of identifying tradeoffs. With the right innovation in place, few, if any, sacrifices must be made to achieve a particular improvement. In the unconstrained vision, questions of feasibility are not of primary concern, as trade-offs merely reflect varying scales of preferences and circumstances among individuals.

In both cases, regardless of the assumptions held, the desired outcome remains the same. **The goal in both visions is to create the best possible outcome.** As these assumptions are so fundamental to decision making, very rarely is there agreement on how to achieve desired outcomes. Both visions acknowledge that the world has unlimited desires and believe there to be an optimal way to accommodate for these desires.

As the labels “constrained” and “unconstrained” suggest, one vision acknowledges that we cannot get everything we want (constrained) and the other affirms our potential to be limitless (unconstrained). It should therefore come as no surprise that each vision reaches opposite conclusions on how to accommodate for a desired outcome.

The Conflict of “Crypto” Visions

With this framing in mind, it is easy to begin to see how many of crypto’s major intellectual fault lines lie along the constrained/unconstrained divide. The space is nascent: a large canvas with a massive surface area for experimentation and tens of thousands of participants, each with their own distinct end game.

In the absence of widespread adoption, participants fall back to narrative. When defining these narratives, we see intra-blockchain divides—is the end vision of “crypto” a hyper-capitalist [Galt’s Gulch](#) or a [radical markets](#)-inspired disintermediated society (or both)? Even inter-blockchain narratives are inconsistent as we’ve seen narratives around Bitcoin and Ethereum transform over time.

This post builds on [prior work](#) from Nic Carter and Hasu exploring Bitcoin’s evolving narratives (and Felipe Pereira’s similar efforts [with Ethereum](#)). While researchers have focused on describing how narratives have evolved over time, less analysis has been done to frame these evolutions in context: are these evolutions simply opportunistic, the result of shifting commercial (and investment) opportunity in the cryptocurrency

ecosystem, or do they reflect more fundamentally disjointed philosophical orientations?

The most salient distinction people have made, [between “money crypto” and “tech crypto”](#), is a good starting point but incomplete. In our view, these distinctions don’t come down to “Silicon Valley” v. “cypherpunk”—many cypherpunks are not strong advocates of base-layer privacy and many SV entrepreneurs are wary of the “move fast and break things” culture of their peers—these distinctions are more foundational, reflective of constrained and unconstrained views of the future that technologies can help build.

The Structure of Arguments



Hasu's model of Bitcoin's [social contract](#) illustrates the dualistic relationship between the social contract and implementation details in public blockchains.

Virtually every debate about cryptocurrencies happens at the social layer. This is for good reason, given the nature of the [network governance models](#) many public blockchains follow, decisions around consensus often reinforce precedents for the future. As such, design is approached carefully and with thoughtful consideration in some major historical debates:

- Is it possible to have a sustainable long-term security model with a fixed money supply (v. mild or high inflation)?
- How important is programmability and expressiveness considering the increased attack surface and increased security cost?
- Is “absolute” base-layer privacy worthwhile if it increases the difficulty of verification of the money supply (or requires greater trust in the issuers or maintainers of the system)?

- Is increasing the block-size—lowering transaction fees and allowing full node cost to scale up linearly—a short-sighted decision given the uncertainty of future advancements?

These debates are rarely presented as such. Rather than presenting ideas as a question of tradeoffs, discourse—whether in a tiny Telegram chat or on stage at a conference—devolves into religious fervor and ad hominem. Cryptocurrency prices serve as a real-time scoreboard for winning narratives, with ownership creating bias as people “shill their bags” in the face of presenting debates with nuance.

Much of the debate ends up substituting opaque proclamation for arguments. Enthusiasts fall back to simple quips and vacuous rhetoric—technical features that are favored and already exist are “here to stay” while proposed features are “inevitable.” Unpopular existing features are “obsolete” and unpopular, ambitious pitches are “unrealistic.”

	Existing	Non-existing
Favored	“Here to Stay”	“Inevitable”
Opposed	“Obsolete”	“Unrealistic”

To see through this vacuous rhetoric, Sowell suggests applying general principles of common sense (which are nevertheless often ignored) illustrated below:

1. All statements are true, if you are free to redefine their terms
2. Any statistic can be extrapolated
3. A can always exceed B if not all of B is counted or if A is exaggerated
4. For every expert there is an equal and opposite expert, but for every fact there is not necessarily an equal and opposite fact.
5. Every policy is a success by sufficiently low standards and a failure by sufficiently high standards.
6. Most variables can show either an upward trend or a downward trend, depending on the base year chosen.
7. You can always create a fraction by putting one variable upstairs and another variable downstairs, but that does not establish any causal relationship between them, nor does the resulting quotient have any necessary relationship to anything in the real world

A careful examination of Sowell's principles sheds light on the lack of thoughtful consideration that much of "crypto" debate is predicated upon.

Episode I: Monetary Maximalism vs. Multicoinery

First, we only had Bitcoin, released by Satoshi, who by all evidence was likely an outsider to the establishment. As Bitcoin was strictly focused on offering a new electronic cash system without the reliance of a trusted central mint, the utmost focus of enthusiasts and developers has always been security (of the codebase) and security again (of the monetary policy). Historically, changes to Bitcoin have been debated not just on their merits but in their second and third-order effects on security.

The original grassroots cypherpunk movement of Bitcoin was never focused on "blockchain technology". To this day, the majority of "Bitcoin maximalists" or "shitcoin minimalists" see Bitcoin's focus as a grassroots bottom-up effort in engineering in stark contrast to the more formal top-down efforts employed by projects like Ethereum, Tezos, and others.

Inspired by the view of Austrian economists, Bitcoiners have historically opted for a "simplistic" & "adversarial" view of the world, grounded in an understanding of monetary history: that the "killer app" is money and that Bitcoin, a potential global money competitor, has the largest potential TAM. In their view, other projects attempting to create a better Bitcoin and iterate on its "fundamental design limitations" misunderstand its intended use.

What Bitcoiners attack with historicism, multi-coiners defend with vision, often criticizing this limited, "simplistic" view held. The unconstrained vision [believes](#) it to

be “a major failure of imagination (or really just plain observation, frankly) to think that crypto has nothing more to offer than a slow and volatile form of sound money.”

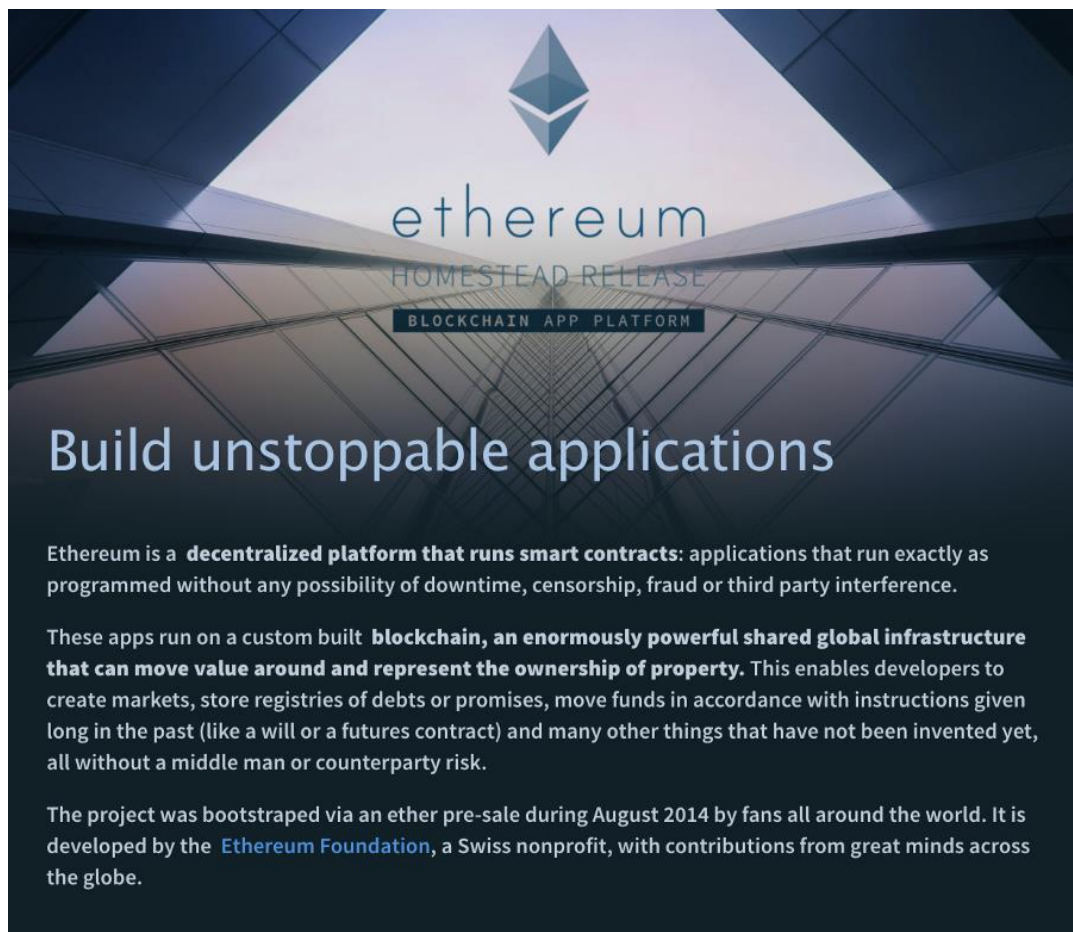
Under these sets of unconstrained assumptions, Bitcoin might instead be described as a part of the “calculator era” of cryptocurrencies, as recently [explained](#) by Andreessen Horowitz partner Jesse Walden:

Many argue that that the most important property of a decentralized money system is security, not programmability, and that a limited scripting language is thus a feature, not a bug. Through that lens, we can view Bitcoin as more of a calculator than a computer (and that is intended as a positive remark!). **It is purpose built and good at its task, but for developers keen to tinker and build new applications an evolution to a new architecture was required.**

To people biased with an unconstrained view of the world, Bitcoin suffers from a lack of vision. As such, the same feature (e.g. complex programmability) might be viewed by the constrained vision as a bug and by the unconstrained vision as a feature. Sowell (135) clarifies this distinction:

To those with the unconstrained the question is: What will remove particular negative features in the existing situation to create a solution? Those with the tragic vision ask: What must be sacrificed to achieve this particular improvement?

On the other hand, to the constrained vision **there are no solutions, only trade offs**. Bitcoin developers like Jimmy Song argue that [blockchain technology comes with significant tradeoffs](#) ranging from the high costs of development and maintenance, to the challenges of coordinating complex incentives across many parties. Bitcoiners view capital-b “Blockchain” and “tokenization” advocates as missing the point: with a distributed ledger hammer, every incentive problem looks like a nail.



Ethereum’s marketing from late 2016 proposed “unstoppable applications”, enabling developers to do lots of things, many of which have not been invented yet. While Turing Completeness may have its advantages, it does not come without significant tradeoffs.

Many Silicon Valley investors have historically thought of the killer app of blockchains as creating new markets, with Naval Ravikant [famously noting](#) that blockchains can replace networks with markets. Pantera Capital CIO Joey Krug sees disintermediation of traditional companies as a core part of their “blockchain technology” thesis, [suggesting that](#) in their strongest form, blockchains can create marketplaces in industries far from financial services, massively up-ending traditional businesses in the process:

Blockchain tech is good for multi-sided marketplaces—particularly for finance. Other use cases, which really just converge with financial markets, include: file storage markets like Filecoin; computational markets; markets for items in video games; namespaces like Handshake; regular betting/gambling like FunFair; and sharing economy protocols like Origin. **These projects will fuel a classic disintermediation**

play: cut out the existing profit-seeking corporations and replace them with software. As software eats the world, software is eating software.

Silicon Valley's bias for the unconstrained view is straight-forward. By defining networks like Bitcoin as software-first, the role of the technologist precedes that of a monetarist. As such, "blockchain" simply becomes one amongst a number of emergent platforms in the ever-evolving internet infrastructure (Web 3.0). In ["What comes after open source?"](#), Andreessen Horowitz's Denis Nazarov elegantly explains this view:

Years of state accumulated by innovative companies produced tremendously useful services (search, maps, social, commerce), but further combinatorial innovation is off-limits to outside developers and entrepreneurs. **Rebuilding services from scratch on the same terms and this late in the game is hopeless.**

As crypto networks evolve, they are likely to provide strong incentives to unlock further state and create open services in many areas dominated by closed ones today. **Open services powered by crypto networks will present unprecedented opportunity for a new generation of developers and entrepreneurs to innovate.**

The Use of Language

The technologist's articulation of the potential of blockchain technology rejects current constraints with a bias to technological progress. Not seeing this vision is often attributed to a lack of imagination on the part of the "doubters." Who could've seen the potential of the internet in 1995 given the nascent state of internet architecture or the explosion of mobile applications transforming the world given the limited capabilities of the first iPhone? Sowell clarifies:

Intractable problems with painful trade-offs are simply not part of the vision of the unconstrained. **Problems exist only because other people are not as wise or as caring, or not as imaginative and bold, as the unconstrained.**

This is visible even in the linguistic choices of the unconstrained view, with Sowell noting that "the vocabulary of the unconstrained is filled with words reflecting their rejection of incremental trade-offs and advocacy in categorical solutions."

More generally, the use of language becomes a strong reflection of an individual's views. The term "shitcoin minimalist", for instance, indicates a constrained view of the potential of blockchain-based solutions to human problems.

The term "Bitcoin maximalism" itself was a derogatory claim made by Vitalik Buterin, who started Ethereum after categorical rejection of his proposals to materially expand the available feature set on Bitcoin. It has since been weaponized, with

[Vitalik noting](#) that “I do wish ill on *bitcoin maximalism*, but only because bitcoin maximalism as an ideology seeks elimination of all non-bitcoin platforms.” While the term [has been co-opted](#) by Bitcoiners to reflect a descriptive monetarist view rather than a prescriptive ideology, it is still a major point in the multi-coiners sieve to discount Bitcoiners’ claims, with Vitalik [clarifying](#) his view, even going so far as to use the word “constrain”:

Because **I view single-coin maximalism as an oligarchic rent-seeking ideology that seriously *constrains* the possibilities of cryptocurrency innovation** and makes it dependent on a political process (Bitcoin governance) rather than market competition?

Sowell preempts this conflict in his work, clarifying that “the anointed often place permanent labels on people, on the basis of transient circumstances” in order to more solidly position themselves as the underdog, fortifying “us v. them” dynamics. These labels aren’t useful—the interests of a few “toxic” Bitcoiners don’t reflect the views of most bitcoin holders, who are not even aware of the nuances of online cryptocurrency discourse.

Bitcoiners push back on this unconstrained view further, noting that they are largely divorced from science. Even the strongest proponents of the unconstrained view acknowledge the delta between the realities of today’s technology and appeal to tomorrow’s, with Walden further [noting](#):

How exactly this will work is very much in the realm of open research. Proponents of “server era” architectures posit that a “cloud era” experience will emerge through standardization and abstraction of inter-blockchain communication among heterogeneous blockchains. Others, like Ethereum 2.0 (Serenity) and Dfinity, are converging on sharded versions of homogenous, turing-complete chains. And still others are researching entirely new architectures that move computation off-chain.

Through the lens of technological utopianism, or [nirvana fallacy](#), feasibility is an afterthought to be attacked by a portfolio of diversified bets—the venture capital model—rather than an exploration of tradeoffs in an ever-exploding design space.

Episode II: The “fairness” of crypto distribution

Since the very beginning, debates about the “fairness” of various cryptocurrencies have sparked fiery conversation about what future wealth distribution should look like. This is expected—if cryptocurrencies actualize the full cypherpunk vision for the future, they represent one of the greatest wealth transfers of all time. With discussions of current income inequalities dominating global discourse, the potential

for cryptocurrencies to exacerbate existing problems have been top of mind for many.

Over the years, there have been many attempts to quantify this disparity, including Balaji Srinivasan's [work](#) exploring different networks' Gini coefficients. These research efforts have sparked outrage from cryptocurrency enthusiasts and external critics alike, including:

[Dogecoin creator Jackson Palmer:](#)

[Cryptocurrency analyst Ferdous Bhai:](#)

Additionally, NYU professor and notorious cryptocurrency critic Nouriel Roubini [remarks](#) that "the inequality coefficient of BTC is worse than North Korea that has the worst inequality on earth."

This conflict is another example of the strain between bottom-up constrained views of Bitcoiners, who believe attempting to design "ideal" wealth distribution is futile, and critics, who believe that Bitcoiners are "unfairly" rewarded for their early adoption. Defenders of the constrained view maintain that Bitcoin's purpose is simply offering a non-sovereign money alternative—explicitly money that is designed *not* to be confiscated or debased—and that the distribution of bitcoins is perfectly calibrated by the free market to reward investors based on their place in the risk curve. Some further argue that given [empirical suggestions that ownership concentration turns over with market cycles](#), concern over distribution is excessive—a problem solved by free markets.

Where holders of the unconstrained view project their desire for a certain wealth distribution in society, the constrained view clarifies that this is a violation of Bitcoin's single purpose: preventing forced wealth redistribution. Sowell, once again, thoughtfully comments on wealth disparities in practice:

If one believes that income and wealth should not originate as they do now, but should instead be distributed as largess from some central point, then that argument should be made openly, plainly, and honestly. But to talk as if we currently have a certain distribution result A which should be changed to distribution result B is to misstate the issue and disguise a radical institutional change as simple adjustment of preferences. The word 'distribution' can of course be used in more than one sense....**What is really being said is that numbers don't look right to the [unconstrained]-and that this is what matters, that all the myriad purposes of the millions of human beings who are transacting with one another in the marketplace must be subordinated to the goal of presenting a certain statistical tableau to [unconstrained] observers.**

Despite this, conflicting visions persist. More ambitious experiments than ever are being pushed, including attempts to create “UBI via mass airdrop” or Bitcoin-alternative money systems specifically designed to prevent long-time wealth hoarding. Subscribers to the constrained vision push back against these forms of idealism with practicality: despite having good intentions, early iterations of these systems are often naively designed and ignore the second or third-order effects of top-down incentive manipulation. In many cases, these policies could end up hurting those they purport to help by creating gamifiable or broken incentives that exacerbate existing inequalities.

Episode III: Governance

The meta-problem of open-source protocol governance has been a longstanding debate where a fault line can once again be identified along the constrained and unconstrained divide.

The constrained vision believes that optimal governance is achieved through a bottom-up approach that attempts to minimize subjectivity and maximize trustlessness, while the unconstrained vision believes optimal governance is achieved through a formalized on-chain approach that interfaces with existing, top-down legal frameworks.

Nick Szabo’s mental model of [wet code and dry](#) further illustrates the nature of these conflicting visions. At the highest level, “wet code” is interpreted by humans, and “dry code” is interpreted by computers. Examples of wet code include law and traditional contracts. Examples of dry code include smart contracts, secure property titles, and the domain name system. Human language might be somewhere in between wet code and dry: if a computer program is able to translate text to multiple languages, for instance, human language may be considered dry.

The distinction between wet code and dry raises questions around the extent to which formalizing governance is possible without exposure to human subjectivity. If wet code is inherently human-readable and dry code computer-readable, the constrained vision would posit that transforming a wet code legal system into dry code would not only add additional complexity but also introduce elements of human subjectivity.

Because the specifics of law and governance are complex and unknowable, the constrained vision opposes fully formal on-chain governance: implementation of “law as code” becomes heavily subjective and unlikely to account for the unpredictable changes in the real world.

Since avoiding human subjectivity and maximizing a network’s trustlessness is the constrained vision’s [top priority](#), “law as code” becomes unattractive. As Bitcoin Core

developer Matt Corallo [highlights](#), “trustlessness is the ability to use Bitcoin without trusting anything but the open-source software you run.” The constrained vision posits that a formalized governance system, which adds unyielding subjectivity to the open-source software, would come at the cost of automated integrity and trustlessness.

Through formalized on chain governance, changes to dry code are completely arbitrary, a reality the constrained vision avoids by prioritizing and questioning the process first. As Sowell suggests:

To those with the vision of the anointed, it is simply a question of choosing the best solution, while to those with the tragic vision the more fundamental question is: Who is to choose? And by what process, and with what consequences for being wrong?

A software’s formal governance system is created from a dry code implementation of something that is inherently wet code. As a result, the control and trust of the software transfers to humans. Under the unconstrained vision, humans *should* be able to change a network’s implementation in an ongoing fashion, as humans are the final arbiters of truth. As such, the vision pushes back on the subjective claim that trust-minimization through software automation is optimal, refusing to accept such a claim as “law.”

In practice, under the constrained vision, automated governance is limited to maintaining the set of verification rules, as seen in Bitcoin’s governance model. In the case of a failure in a wet code process, such a system would resort to a fork, a change in the protocol influencing the validity of the set of rules. Since forks are seen as bugs to the unconstrained, the value proposition of an on-chain governance system is that it precisely avoids forks and encourages high upgradeability. However, by formalizing governance, the risks of undergoing a fork under what at the time would have been considered to be a perfect implementation may potentially speak to the subjective nature of the implementation. For the long term sustainability of the protocol, the constrained vision posits this to be detrimental.

Episode IV: Proof-of-work vs. Proof-of-stake

Bitcoin’s proof-of-work is an embodiment of the constrained vision, a mechanism to work around fundamental limitations rather than re-engineer them. First explained by Nick Szabo in [Money, blockchains, and social scalability](#), Bitcoin’s proof-of-work accommodates our cognitive limitations and behavior tendencies by making a necessary and intentional tradeoff: **greatly sacrificing computational scalability to improve social scalability.**

A feature to the constrained, a bug to the unconstrained.

The ability to participate in an “institutional technology” is predicated on the technology motivating participation and protecting the system and its participants from malicious activity. By improving social scalability, which proof-of-work does so effectively, the number of people who can beneficially participate in the system is maximized. Therefore, the constrained, “proof-of-work” vision posits that Bitcoin’s success should not be determined by its computational efficiency but by its ability to increase social scalability through trust minimization.

What the unconstrained vision deems computationally inefficient and unscalable, the constrained vision not only deems an intended tradeoff, but a fundamental feature: specialized, dedicated hardware *should* perform a function whose sole output is to prove that the computer *did* indeed execute a costly computation. As Nick Szabo [highlights](#), “prolific resource consumption and poor computational scalability unlocks the security necessary for independent, seamlessly global, and automated integrity.”

While an implementation of both computational and social scalability is optimal, the constrained vision acknowledges that it cannot be done without compromising security. Embedded in computer science is a fundamental understanding of tradeoffs in security and performance where inevitably, automating integrity requires high resource utilization. Even with breakthroughs in computer science, the constrained vision recognizes that total integrity and absolute trustlessness is infeasible, making the delicacy of explicit and intentional tradeoffs all the more imperative. As such, the constrained vision fully accepts that such tradeoffs are unavoidable, and “it is probable no such big but integrity-preserving performance improvement is possible.” [4]

To the unconstrained vision, the assumptions around proof-of-work are entirely different. Instead of asserting that proof-of-work sacrifices computational inefficiency for social scalability, the unconstrained vision asserts that proof-of-work unjustifiably consumes significantly more resources than it creates, making it a wasteful and archaic system in dire need of improvement.

A commonly used statistic the unconstrained vision employs to illustrate proof-of-work’s “wastefulness” is a measurement of the amount of energy the system expends as a proportion of the total transaction volume the system processes. By employing such a statistic, it becomes obvious why under the unconstrained view, proof-of-work is so scandalously inefficient: “[Bitcoin consumes](#) five Hiroshima’s worth of energy per day” only to process “[a mere fraction](#) of what a payment service like Visa processes.”

The use of this argument to illustrate proof-of-work’s wastefulness implies that trust minimization is not viewed as a necessary feature in the unconstrained vision. If it were, comparing Bitcoin to Visa would be futile: **Visa does not provide the same improvements in social scalability through trust minimization *precisely because***

it is more “computationally efficient”. Such a comparison not only dismisses the existence of limitations, but attempts to associate two completely unrelated variables (i.e. energy expenditure and transaction volume are not functions of each other). As Sowell highlights, wrongful association of these variables leads to “statistical extrapolation without any analysis of the actual processes from which these numbers were generated.” [5]

A costless alternative?

Deeming proof-of-work wasteful suggests a cheaper, more prudent alternative exists. To the unconstrained vision, the reason proof-of-work has not fully succumbed to an alternative may come from a lack of care for the environment or a lack of imagination of technological advancements as Emin Gun Sirer [suggests](#):

100 years from now, future generations will talk about the PoW craze with the same bemused view we hold for other mass manias. The absurdity of wasting energy to make chicken scratch marks on an electronic ledger is going to become more obvious. We are going to look back the same way we look at the use of CFCs and leaded gasoline. We should replace it with systems that can do better.

As previously highlighted, the unconstrained view is to remove specific negative features in the existing situation to create a solution. In the context of proof-of-work, the question posed by the unconstrained is then: “how can we **remove** the computational inefficiency and energy wastefulness of proof-of-work to create a better sybil-control mechanism and consensus algorithm?”

Attempting to answer this question, mechanisms like proof-of-stake have emerged as the most popular solution, as Ethereum’s Vitalik Buterin highlights:

“The philosophy of proof-of-stake is not ‘security comes from burning energy’, but rather ‘security comes from putting up economic value-at-loss’.

In a proof-of-stake system, a blockchain appends and agrees on new blocks through a process in which anyone who holds coins inside of the system can participate and the influence an agent has is proportional to the number of coins (or ‘stake’) it holds. **This is a vastly more efficient alternative to proof-of-work ‘mining’ and enables blockchains to operate without mining’s high hardware and electricity costs.”**

Under the unconstrained view, proof-of-work is classified solely as a sybil-control mechanism. As such, there is greater justification for removing energy spend on coin production. Emin Gun Sirer [explains](#):

Thus, the goal in the unconstrained vision is to implement an inherently costless system without leakage. In proof-of-stake, network participants are not required to

use inordinate amounts of energy to maintain ledger immutability, significantly reducing labor intensity. A reduction in labor intensity would be more fair and help encourage community participation due to lower barriers to entry. Specifically, the unconstrained vision claims that taking mining out of the hands of entities with access to excessive amounts of low cost energy would help redistribute the work evenly and lead to a more democratized system. By removing the feature that secures value in a proof-of-work system, security in turn is derived from the value stored *within* the system itself. As David Yakira [notes](#), “in a sense, a PoS system is recursive, augmenting the value it stores implies better security which further allows the value to increase and so on.”

Under the constrained vision, however, defining proof-of-work as merely a sybil-control mechanism is non-exhaustive and trivializes its purpose. Proof-of-work is also seen as essential for maintaining unforgeable costliness “[giving digital blocks real-world weight](#)” and enforcing a predictable, meritocratic distribution mechanism.

Because the constrained vision believes there to be “no solutions, only tradeoffs,” a costless mechanism without leakage would also be definitionally impossible, as Paul Sztorc [notes](#):

“Switching the payout-trigger to a social or political dimension would merely transpose the work-expenditures correspondingly to the realms of bribery and propaganda.

If an object has value, people will spend effort to chase it, up to whatever the object is worth ($MC=MR$). This effort is also “work”. [Thus], a stable solution to these problems is **definitionally impossible**, as there is always an incentive to work until marginal cost equals marginal revenue.”

The Future Remains To Be Built

As we’ve highlighted, these divisions between cryptocurrency enthusiasts, investors, and builders can be seen across the “unconstrained” and “constrained” axes, two conflicting ideologies that transcend geography, professional associations, or backgrounds.

We believe that the most likely outcome after the full possible actualizations of these visions is convergence in some form. While the future remains uncertain, a conflict of *visions* persists because in reality, visions are all we have to focus on ahead of a multi-decade roadmap of adoption and integration.

The dominant visions of the constrained view are not mutually exclusive with the more abstract unconstrained view. While on the surface, inter-currency battles persist, [the final boss](#) (third party disintermediation)—which unites everyone alike—is

shared. Though differences emerge upon squinting, high-level goals are not divergent. Privacy-aware cypherpunks want to see the destruction of ad-driven technology monopolies and Bitcoin remains a useful tool against tyrants independent of political, social, or religious affiliation. While cryptocurrency adoption appears zero-sum, experimentation is at the core of open-source and expands the size of the pie in the short-to-medium term by bringing new entrants to the market with disparate views while concurrently validating existing implementations.

It may be that for creating a global money, only a tightly constrained, focused view can prevail as launching a system mimicking a Swiss bank in your pocket requires this level of carefulness. If indeed blockchains represent a major evolution in computing, those systems may follow an evolving philosophy closer to a traditional software release cycle with constantly iterated release cycles.

These debates will be reminisced upon like early internet debates about the ideal protocol standard or intranets and the Internet (earlier generations' blockchains v. bitcoin) or debates even further back about the viability of inferior monetary metals to gold. Ultimately, winners will emerge out of today's conflicting visions invoking "how did we not see that coming?" commentary in the process.

For now, the future remains to be built.

Links

- https://en.wikipedia.org/wiki/A_Conflict_of_Visions
- https://en.wikipedia.org/wiki/The_Vision_of_the_Anointed
- <https://www.tsowell.com/>
- https://en.wikipedia.org/wiki/Invisible_hand
- https://en.wikipedia.org/wiki/Spontaneous_order
- https://www.conservapedia.com/Galt%27s_Gulch
- <http://radicalmarkets.com/>
- https://medium.com/@nic_carter/visions-of-bitcoin-4b7b7cbcd24c
- <https://tokeneconomy.co/visions-of-ether-590858bf848e>
- <https://www.tokendaily.co/blog/money-crypto-vs-tech-crypto>
- <https://medium.com/@hasufly/bitcoins-social-contract1f8b05ee24a9?sk=27e8cf65d45c46ffae1466ce2ac31b48>
- https://medium.com/@pierre_rochard/bitcoin-governance-37e86299470f
- <https://twitter.com/ali01/status/1073005172949843968>
- <https://jessewalden.com/4-eras-of-blockchain-computing-degrees-of-composability/>
- <https://medium.com/@jimmysong/why-blockchain-is-hard-60416ea4c5c>
- <https://twitter.com/naval/status/877467629308395521>

- <https://medium.com/@PanteraCapital/a-crypto-thesis-47eaacf861ca>
- <https://denisnazarov.com/what-comes-after-open-source/>
- <https://twitter.com/VitalikButerin/status/875191751752826880>
- <https://twitter.com/bitstein/status/993819747623096320>
- <https://twitter.com/VitalikButerin/status/993679744393732097>
- https://en.m.wikipedia.org/wiki/Nirvana_fallacy
- <https://news.earn.com/quantifying-decentralization-e39db233c28e>
- <https://twitter.com/ummjackson/status/1053122713848569857>
- <https://twitter.com/ferdousbhai/status/1087596119138287617>
- <https://twitter.com/Nouriel/status/1049092516233064451>
- <https://blog.picks.co/bitcoins-distribution-was-fair-e2ef7bbbc892>
- <http://unenumerated.blogspot.com/2006/11/wet-code-and-dry.html>
- <http://bluematt.bitcoin.ninja/2017/02/28/bitcoin-trustlessness/>
- <http://unenumerated.blogspot.com/2017/02/money-blockchains-and-social-scalability.html>
- <https://twitter.com/el33th4xor/status/1055513144838238208>
- <https://twitter.com/martinvars/status/936654528736366594?lang=en>
- <https://twitter.com/el33th4xor/status/1045115535254540288>
- <https://twitter.com/el33th4xor/status/1046133563584909313>
- <https://medium.com/orbs-network/on-stake-and-consensus-a05e52daa496>
- <https://twitter.com/hugohanoi/status/1046100388133449728>
- <http://www.truthcoin.info/blog/pow-and-mining/>
- <https://twitter.com/naval/status/935878356507258880>

Why Blockchain Differs From Traditional Technology Life Cycles

Why another bubble is likely and what the blockchain space should focus on now

By [Daniel Heyman](#)

Posted February 1, 2019

In the aftermath of the 2001 internet bubble, Carlota Perez published her influential book [Technological Revolutions and Financial Capital](#). This seminal work provides a framework for how new technologies create both opportunity and turmoil in society. I originally learned about Perez's work through venture capitalist Fred Wilson, who credits it as a key intellectual underpinning of his investment theses.

In the wake of the 2018 ICO bubble and with the purported potential of blockchain, many people have drawn parallels to the 2001 bubble. I recently reread Perez's work to think through if there are any lessons for the world of blockchain, and to understand the parallels and differences between then and now. As Mark Twain may or may not have said, "History doesn't repeat itself, but it does rhyme."

Framework Overview

In *Technological Revolutions and Financial Capital*, Carlota Perez analyzes five "surges of development" that have occurred over the last 250 years, each through the diffusion of a new technology and associated way of doing business. These surges are still household names hundreds of years later: the Industrial Revolution, the railway boom, the age of steel, the age of mass production and, of course, the information age. Each one created a burst of development, new ways of doing business, and generated a new class of successful entrepreneurs (from Carnegie to Ford to Jobs). Each one created an economic common sense and set of business models that supported the new technology, which Perez calls a 'techno-economic paradigm'. Each surge also displaced old industries, drove bubbles to burst, and led to significant social turmoil.

Technology Life cycles

Perez provides a framework for how new technologies first take hold in society and then transform society. She calls the initial phase of this phenomenon "installation." During installation, technologies demonstrate new ways of doing business and achieving financial gains. This usually creates a frenzy of investment in the new

technology which drives a bubble and also intense experimentation in the technology. When the bubble bursts, the subsequent recession (or depression) is a turning point to implement social and regulatory changes to take advantage of the infrastructure created during the frenzy. If changes are made, a “golden age” typically follows as the new technology is productively deployed. If not, a “gilded age” follows where only the rich benefit. In either case, the technology eventually reaches maturity and additional avenues for investment and returns in the new technology dwindle. At this point, the opportunity for a new technology to irrupt onto the scene emerges.

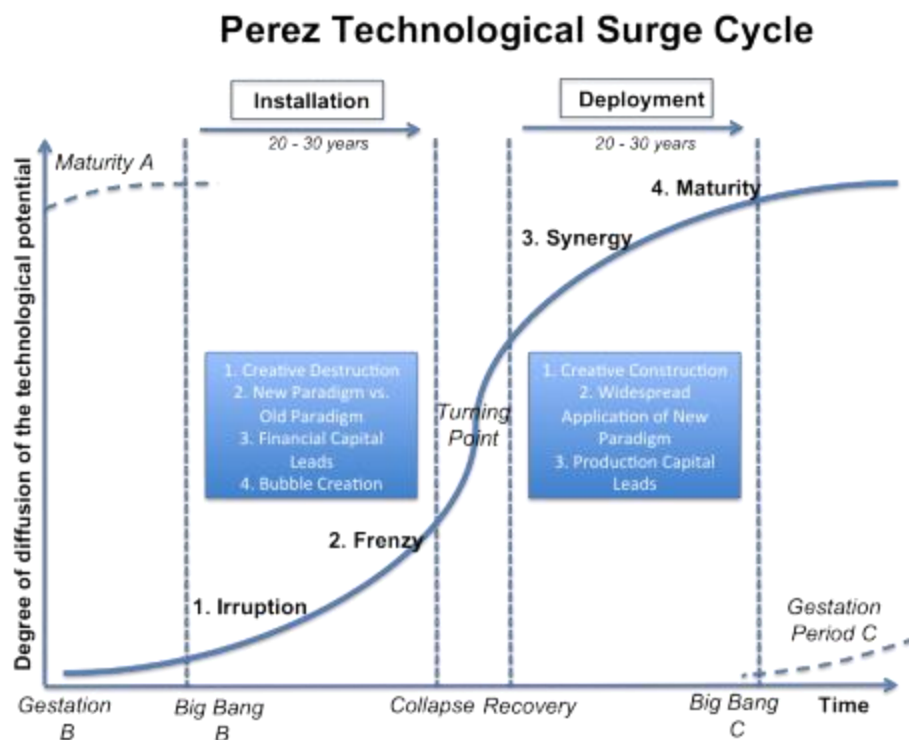


Image from *Technology Revolutions and Financial Capital*

Inclusion-Exclusion

Within Perez’s framework, new techno-economic paradigms both encourage and discourage innovation, through an *inclusion-exclusion process*. This means that as new techno-economic paradigms are being deployed, they provide opportunities for entrepreneurs to mobilize and new modes of business to create growth, and at the same time, they exclude alternative technologies because entrepreneurs and capital are following the newly proven path provided by the techno-economic paradigm. When an existing technology reaches maturity and investment opportunities diminish, capital and talent go in search of new technologies and techno-economic paradigms.

Technologies Combine

One new technology isn't enough for a new techno-economic paradigm. The age of mass production was created by combining oil and the combustion engine. Railways required the steam engine. The information age required the microprocessor, the internet, and much more. Often, a technology will, as Perez says, "gestate" as a small improvement to the existing techno-paradigm, until complementary technologies are created and the exclusion process of the old paradigm ends. Technologies can exist in this gestation period for quite sometime until the technologies and opportunities are aligned for the installation period to begin.

Frenzies and Bubbles

In many ways, the bubbles created by the frenzy in the installation phase makes it possible for the new technology to succeed. The bubble creates a burst of (over-)investment in the infrastructure of the new technology (railways, canals, fiber optic cables, etc.). This infrastructure makes it possible for the technology to successfully deploy after the bubble bursts. The bubbles also encourage a spate of experimentation with new business models and new approaches to the technologies, enabling future entrepreneurs to follow proven paths and avoid common pitfalls. While the bubble creates a lot of financial losses and economic pain, it can be crucial in the adoption of new technologies.

Connecting the Dots

A quick look at Perez's framework would leave one to assume that 2018 was the blockchain frenzy and bubble, so we must be entering blockchain's "turning point." This would be a mistake.

My analysis of Perez's framework suggests that blockchain is actually still in the gestation period, in the early days of a technology life cycle before the installation period. 2018 was not a Perez-style frenzy and bubble because it did not include key outcomes that are necessary to reach a turning point: significant infrastructure improvements and replicable business models that can serve as a roadmap during the deployment period. The bubble came early because blockchain technology enabled liquidity earlier in its life cycle.

There are three main implications of remaining in the gestation period. First, another blockchain-based frenzy and bubble is likely to come before the technology matures. In fact, multiple bubbles may be ahead of us. Second, the best path to success is to work *through*, rather than *against*, the existing technology paradigm. Third, the ecosystem needs to heavily invest in infrastructure for a new blockchain-based paradigm to emerge.

The ICO Bubble Doesn't Match Up

2018 did show many of the signs of a Perez-style 'frenzy period' entering into a turning point. The best way (and ultimately the worst way) to make money was speculation. 'Fundamentals' of projects rarely mattered in their valuations or growth. Wealth was celebrated and individual prophets gained recognition. Expectations went through the roof. Scams and fraud were prevalent. Retail investors piled in for fear of missing out. The frenzy had all the tell-tale signs of a classic bubble.

Although there are no "good bubbles," bubbles can have good side effects. During Canal Mania and Railway Mania, canals and railways were built that had little hope of ever being profitable. Investors lost money, but after the bubble, these canals and railways were still there. This new infrastructure made future endeavors cheaper and easier. After the internet bubble burst in 2001, fiber optic cables were selling for pennies on the dollar. Investors did terribly, but the fiber optics infrastructure created value for consumers and made it possible for the next generation of companies to be built. This over-investment in infrastructure is often necessary for the successful deployment of new technologies.

The ICO bubble, however, did not have the good side effects of a Perez-style bubble. It didn't produce nearly enough infrastructure to help the blockchain ecosystem move forward.

Compared to previous bubbles, the cryptosphere's investment in infrastructure was minimal and likely to be obsolete very soon. The physical infrastructure—in mining operations, for example—is unlikely to be useful. Additional mining power on a blockchain has significantly decreasing marginal returns and different characteristics to traditional infrastructure. Unlike a city getting a new fiber optic cable or a new canal, new people do not gain access to blockchain because of additional miners. Additionally, proof of work mining is unlikely to be the path blockchain takes moving forward.

The non-physical infrastructure was also minimal. The tools that can be best described as "core blockchain infrastructure" did not have easy access to the ICO market. Dev tools, wallets, software clients, user-friendly smart contract languages, and cloud services (to name a few) are the infrastructure that will drive blockchain technology toward maturity and full deployment. The cheap capital provided through ICOs primarily flowed to the application layer (even though the whole house has been built on an immature foundation). This created incentives for people to focus on what was easily fundable rather than most needed. These perverse incentives may have actually hurt the development of key infrastructure and splintered the ecosystem.

I don't want to despair about the state of the ecosystem. Some good things came out of the ICO bubble. Talent has flooded the field. Startups have been experimenting with different use cases to see what sticks. New blockchains were launched incorporating a wide range of new technologies and approaches. New technologies have come to market. Many core infrastructure projects raised capital and made significant technical progress. Enterprises have created their blockchain strategies. Some very successful companies were born, which will continue to fund innovation in the space. The ecosystem as a whole continues to evolve at breakneck speed. As a whole, however, the bubble did not leave in its wake the infrastructure one would expect after a Perez-style bubble.

Liquidity Came Early

The 2018 ICO bubble happened early in blockchain technology's life-cycle, during its gestation period, which is much earlier than Perez's framework would predict. This is because the technology itself enabled liquidity earlier in the life-cycle. The financial assets became liquid before the underlying technology matured.

In the internet bubble, it took companies many years to go public, and as such there was some quality threshold and some reporting required. This process enabled the technology to iterate and improve before the liquidity arrived. Because blockchain enabled liquid tokens that were virtually free to issue, the rush was on to create valuable tokens rather than valuable companies or technologies. You could create a liquid asset without any work on the underlying technology. The financial layer jumped straight into a liquid state while the technology was left behind. The resulting tokens existed in very thin markets that were highly driven by momentum.

Because of the early liquidity, the dynamics of a bubble were able to start early for the space in relationship to the technology. After all, this was not the first blockchain bubble (bitcoin already has a rich history of bubbles and crashes). The thin markets in which these assets existed likely accelerated the dynamics of the bubble.

What the Blockchain Space Needs to Focus on now

In the fallout of a bubble, Perez outlines two necessary components to successfully deploy new and lasting technologies: proven, replicable business models and easy-to-use infrastructure. Blockchain hasn't hit these targets yet, and so it's a pretty obvious conclusion that blockchain is not yet at a "turning point."

While protocol development is happening at a rapid clip, blockchain is not yet ready for mass deployment into a new techno-economic paradigm. We don't have the proven, replicable business models that can expand industry to industry. Exchanges and mining companies, the main success stories of blockchain, are not replicable business models and do not cross industries. We don't yet have the infrastructure for

mass adoption. Moreover, the use cases that are gaining traction are mostly in support of the existing economic system. Komgo is using blockchain to improve an incredibly antiquated industry (trade finance) but it is still operating within the legacy economic paradigm.

Blockchain, therefore, is still in the “gestation period.” Before most technologies could enter the irruption phase and transform the economy, they were used to augment the existing economy. In blockchain, this looks like private and consortium chain solutions.

Some people in blockchain see this as a bad result. I see it as absolutely crucial. Without these experiments, blockchain risks fading out as a technological movement before its given the chance to mature and develop. In fact, one area where ConsenSys is not given the credit I believe it deserves is in bringing enterprises into the Ethereum blockchain space. This enterprise interest brings in more talent, lays the seeds for additional infrastructure, and adds credibility to the space. I am more excited by enterprise usage of blockchain today than any other short-term developments.

The Future of Blockchain Frenzy

This was not the first blockchain bubble. I don’t expect it to be the last (though hopefully some lessons will be learned from the last 12 months). Perez’s framework predicts that when the replicable business model is found in blockchain, another period of frenzied investment will occur, likely leading to a bubble. As Fred Wilson writes, “Carlota Perez [shows] ‘nothing important happens without crashes.’” Given the amount of capital available, I think this is a highly likely outcome. Given the massive potential of blockchain technology, the bubble is likely to involve more capital at risk than the 2018 one.

This next frenzy will have the same telltale signs of the previous one. Fundamentals will decrease in importance; retail investors will enter the market for fear of missing out; fraud will increase; and so on.

Lessons for Blockchain Businesses

Perez’s framework offers two direct strategic lessons for PegaSys and for any serious protocol development project in the blockchain space. First, we should continue to work with traditional enterprises. Working with enterprises will enable the technology to evolve and will power some experimentation of business models. This is a key component of the technology life-cycle and the best bet to help the ecosystem iterate.

Second, we must continue investing in infrastructure and diverse technologies for the ecosystem to succeed. This might sound obvious at first, but the point is that we will miss out on the new techno-economic paradigm if we only focus on the opportunities that are commercially viable today. Our efforts in Ethereum 1.x and 2.0 are directly born from our goal of helping the ecosystem mature and evolve. The work other groups in Ethereum and across blockchain are doing also drives towards this goal. We are deeply committed to the Ethereum roadmap and at the same time recognize the value that innovations outside Ethereum bring to the space. Ethereum's roadmap has learned lessons from other blockchains, just as those chains have been inspired by Ethereum. This is how technologies evolve and improve.

Links

- https://hackernoon.com/@HeymanDaniel?source=post_header_lockup
- <https://hackernoon.com/@HeymanDaniel>
- <https://www.amazon.com/Technological-Revolutions-Financial-Capital-Dynamics/dp/1843763311>

Blockchain Privacy: Equal Parts Theory and Theater

Satoshi Has No Clothes

By [Ian Miers](#)

Posted February 1, 2019

The cryptocurrency community has done a poor job of evaluating privacy. We are even worse at explaining the tradeoffs of different implementations to regular users. Improvement is necessary and it needs to happen now. Many of these protocols aspire to be the future of payments – one of them may win. By the time that happens, it'll be too late to get the design right.

In 2011, when I started working on privacy in cryptocurrencies, it was commonly thought that Bitcoin was private. WikiLeaks solicited “anonymous Bitcoin donations” on Twitter, which is somewhat tragic; we can confidently guess that a few WikiLeaks donors were in sensitive positions, at least.

Now we're aware that Bitcoin is nowhere close to anonymous. A [number](#) of [academic](#) papers [have shown](#) that you can link pseudonymous transactions together and thereby track what someone is doing across a blockchain. In addition, companies like Chainalysis are in the business of discovering and surfacing such analytics.

Bitcoin is Twitter for your bank account. Anyone can see what you're doing. That includes your family members, friends, current and former romantic partners, business associates, competitors, all the way up to government agencies. Even people who are government decision-makers themselves should remember that other governments – the ones they don't like – will delve into the details of their finances.

It's common to say that “privacy is dead,” suggesting that it's hopeless to protect your privacy. The idea is that someone – the government, Google, a mysterious bogeyman – will always know things about you. But there's a difference between one person knowing your deepest, darkest secrets, and everyone knowing them. Just because Google knows your browsing history doesn't mean that you want it to be public.

During the past seven or eight years, we've seen many proposals to add privacy to cryptocurrencies. The techniques range from simple things, like avoiding address reuse, to complex cryptographic protocols. Measuring the privacy afforded by a certain implementation is tricky.

Right now, we can't resort to empirical methods. It would be akin to evaluating internet privacy in 1992, when the only websites were ones at CERN. That was before targeted ads, and tracking cookies; Google AdWords didn't launch until 2000. Richard Stallman was considered an alarmist crank. It was before we really used the web for anything where it would be worth tracking people.

In the current cryptocurrency ecosystem, you cannot look at people's usage and then produce an authoritative estimate of whether (or which!) privacy techniques are effective. The necessary data isn't there. Today nearly all transactions are speculative, which illustrates the privacy needs of risk-loving investors, but leaves aside everyone else.

We don't have the rich tapestry of structure that results when you pay for your train trip, walk to the local market to buy a sandwich, then mail a package at the post office, then buy something at the vending machine. That kind of behavior, and the data generated by it, is not evident among the vast majority of cryptocurrency users.

As a researcher, even if this data existed, I couldn't use it. I have limited access to data due to cost concerns, and I and other academic researchers have ethical limitations imposed by the Institutional Review Board. Our adversaries do not.

The upshot is that an empirical evaluation of future privacy is impossible. Instead of relying on data, we must resort to thought experiments. We need to think through the usage of our systems in the coming decades and consider how that will play out. One viable approach is to look at the problems in related domains.

Real-World Privacy Threats

The most common threat that people bring up is governments and law enforcement leveraging blockchain data. As with the privacy needs of speculators, that is one threat, but it's not the only one. Nor is it the threat most likely to affect the public at large. (That said, we should not dismiss the concerns of activists and dissidents.)

Looking beyond cryptocurrencies, we recently learned that [Google has been collecting offline payment data from Visa and MasterCard](#) and using it to build up profiles for targeted advertising. You may think that Google does a good job and institutes reasonable security controls, or you may not. Regardless, it's a worrying trend (and not a new one). If Google is doing it, so are people and entities that are less scrupulous. You've never heard of them and you have no idea how they're using information about your transactions.

Similarly, we know that companies want to build up rich profiles of their customers' behavior. There are numerous sources of data for them to compile — for example, usage of loyalty cards and coupons. Retailers can track and analyze this information,

to the extent that they're able to guess when customers are pregnant, since pregnant customers exhibit certain purchasing patterns. Other medical conditions likely fall in the same boat.

News reports have indicated that retailers aim to discover these things before you even know yourself... or at least before the other people in your family know. In 2012, Charles Duhigg wrote a [feature for the New York Times Magazine](#) that contained this anecdote:

"About a year after [Target data scientist Andrew Pole] created his pregnancy-prediction model, a man walked into a Target outside Minneapolis and demanded to see the manager. He was clutching coupons that had been sent to his daughter, and he was angry, according to an employee who participated in the conversation. "My daughter got this in the mail!" he said. "She's still in high school, and you're sending her coupons for baby clothes and cribs? Are you trying to encourage her to get pregnant?" The manager didn't have any idea what the man was talking about. He looked at the mailer. Sure enough, it was addressed to the man's daughter and contained advertisements for maternity clothing, nursery furniture and pictures of smiling infants. The manager apologized and then called a few days later to apologize again."

"On the phone, though, the father was somewhat abashed. "I had a talk with my daughter," he said. "It turns out there's been some activities in my house I haven't been completely aware of. She's due in August. I owe you an apology." There are serious privacy problems with data about what people buy. It's plausible that sexual orientation could be targeted in the same way. These examples are more fine-grained than you might be able to extract from a blockchain, but nonetheless the issue manifests in a system like Bitcoin."

A more on-the-nose example is Venmo. For those of you who don't know, Venmo is a service primarily used for payments between friends, to pay for a bar tab or split a restaurant check. By default, [Venmo has a public feed](#) of every transaction that its users make. It includes your name, the recipient's name, and a memo field describing why you paid them. That is pretty close to the data on the Bitcoin blockchain.

We've seen the failure cases of Venmo's public feed, including small-time pot dealers being arrested and supposedly lighthearted guides to stalking your ex-boyfriend. That's playful in theory, but actually no, it's creepy and abusive. People should not be okay with any system having these features.

Another threat that's more well-known to the cryptocurrency community, where issues are even cropping up today, is fungibility. We know that for certain cryptocurrencies, freshly mined coins sell for a premium. Exchanges sometimes block customers based on their transaction history; where they've sent their money in the past.

It's important to note that exchanges are powerful. We can't think of them as merely third-party observers. They know more about you than just the transaction graph. Frequently they conduct transactions on behalf of their users. The privacy problem here is akin to trying to maintain privacy from Google while using Gmail and Google Maps on an Android phone. At some level, you're embodying your adversary.

Remember, Bitcoin is Twitter for your bank account. And not the kind of Twitter where you choose what tweets to write and publish. Bitcoin is more like a creepy alternate-universe Twitter that automatically transmits all of your thoughts.

Defenses and Failures

What are the viable defenses?

In a world of massive data collection and machine learning, plausible deniability doesn't work. Typically when I talk about this, someone comes up to me and says, "What if I tell the police, 'Hey, you can't prove it's me!'" That is naivete, insufficient for the real world. The algorithms being deployed don't care about plausible deniability; they operate on probabilities. And when the probability is high enough, that holds up for law enforcement purposes as much as advertising.

Blockchain privacy is not intuitive. Typically people tend to think of passive third-party observers as the main threat. But it's crucial to consider active attackers who can send payments to you, receive payments from you, and interact with third parties. Obvious examples of such attacks are merchants or cartels of merchants who keep track of customers, people who try to identify a payment recipient's real identity, and exchanges that also want to track you. (I'll address these scenarios momentarily.)

The range of supposed solutions to privacy problems is huge, so I won't review all of them individually. However, we can look at the approaches broadly in terms of three different kinds of systems.

First, some systems look like vanilla Bitcoin, where you explicitly identify the origin of your payment. The only protection here is that there are no real names. The base layer doesn't even attempt to obfuscate transaction data, which is now widely understood in cryptocurrency circles. (The general public could still use education on the issue.) Another approach is what I'm going to call decoy-based systems, where you hide

what's going on in a given transaction by selecting a certain number of possible payment origins. The strongest approaches are Zerocoin and Zerocash, where no origin at all is identified.

In decoy-based systems — CoinJoin, Monero's RingCT, and others — you are required to explicitly verify the source of your funds, but you try to hide it by including a handful of decoys that aren't your real source. Theoretically, anyone looking at the transaction cannot tell which is which. The actual origin is obfuscated by adding noise.

And again, in systems using the principles of Zerocash, you don't have any identifiers whatsoever.

My position is that we haven't properly examined the downsides of decoy-based systems. It is a significant oversight, because much of the cryptocurrency community is turning to decoys as a source of scalable privacy. Decoy-based systems do not provide the robust, attack-resistant privacy that people assume.

Decoy-Based Deanonimization

Let's say that you're sending a decoy-obfuscated transaction. The protocol identifies the possible source of the funds, along with a handful of decoys. Now an observer or attacker has access to a tree of possibly associated payments that go back in history. They can't pinpoint quite what happened, since it's like a fuzzy family tree, but they can extrapolate some notion of what's going on based on this single transaction. That family tree — what I will call a taint tree — also works going forward.

Overseer Attack

Let's say that your transaction was a payment to a merchant. Where does the money go next? Attackers cannot know precisely because of the systemic use of decoys. But they will be able to trace a finite number of possibilities in terms of where the money might have gone. Next, they can start a process of elimination.

The taint tree gives an attacker a lot of power, especially when tracking analysis is repeated over multiple transactions. One thing you can do if you're a merchant, or a set of colluding merchants, is track customers across repeated payments.

Hypothetically, I'm going into Target on a daily basis and making cash purchases. There should be no way of tracing me — beyond arduous methods like dusting for fingerprints or DNA, which requires already having those biometrics, or knowing in advance the serial numbers of the bills I'm going to use.

What if I start using a cryptocurrency to buy things at Target? (No, large retailers don't accept cryptocurrencies yet, but that's the endgame of these technologies.) Ideally I could make three separate purchases and there would be no way to link them together. A cryptocurrency with true privacy would achieve that.

If you look at decoy-based systems superficially, it seems like that do achieve that. None of these transactions appear to be linked together:



It gets worse. Again, let's consider multiple payments that I've made to one merchant. I don't want them to know that I'm the same person, but in a decoy-based system you have taint trees of possible ancestors. Well, what happens if they have a common origin? I went to Coinbase or whatever exchange, and I bought a bunch of cryptocurrency, then I loaded it onto the blockchain.

There's going to be one source of those funds. If you trace back the taint trees, you can look at the intersections and pinpoint the person making these transaction. That method works not just for one merchant, but also for groups of merchants — or other entities that receive payments. They can collude to figure out who you are, which is a problem when the goal is privacy.

Flashlight Attack

Let's suppose I want to accept payments online, anonymously. For example, I'm a dissident in an authoritarian country who needs to accept donations, but I cannot reveal my real identity; my life is at risk in the country where I do my activism. But I need to be able to fund my work. Of course, the government of that locale is trying to identify me. They have intel agencies and secret police at their disposal.

If I'm using a privacy-preserving cryptocurrency, it should be safe for me to deposit the donated funds at a local exchange. Even if that exchange is controlled by the

government! Ideally the data that could be used to identify me — probabilistically or otherwise — is simply not available. I should be safe regardless of whether the exchange is hacked, corrupt, subpoenaed or otherwise infiltrated. What I'm describing is how it *should* work, not how it actually works.

If the government wants to identify me, they have my cryptocurrency addresses because I've exposed them in order to accept donations. Maybe my website is only accessible over Tor; maybe I even use a unique address per donation. And of course I'm relying on a decoy-based cryptocurrency.

The government realizes that they can send tracking payments to an address of mine. Three of them, perhaps, or 20, or 100. The payments can be very small; size is irrelevant. At some point I'm going to deposit the funds from those payments.

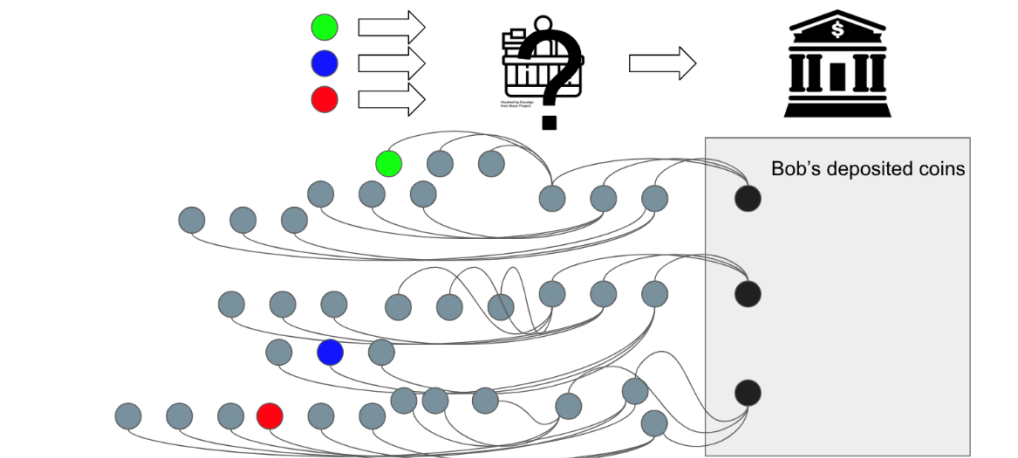
Now I've got a big problem. Anybody who can access the exchange's records is now able to test whether the depositor is the same person as the democracy activist. They can examine the set of coins that I've deposited and reconstruct the taint tree, the possible sets of origins.

For any random person, it would be unremarkable that their deposits involved tainted payments. Decoys are picked at random, so by happenstance, one of the tainted payments could make its way into their deposits. On the other hand, the probability of that happening multiple times is quite low. It's vanishingly unlikely to happen with all of the funds from 100 tainted payments that were sent to this one democracy activist.

The government can look through all of my deposits, and see that my taint tree contains all of the tracking payments that they sent. That evidence links my legal identity to my democracy activism with overwhelming probability.

As you can see, taint trees are viable for deanonymization, and thus decoy-based systems violate people's notions of how privacy should (or does) work in cryptocurrencies. Taint trees allow privacy to be ripped apart in a way that would shock and concern many users.

Flashlight attack: identifying anonymous merchants



This is probably the easiest to execute and most immediately troubling attack on decoy based systems.

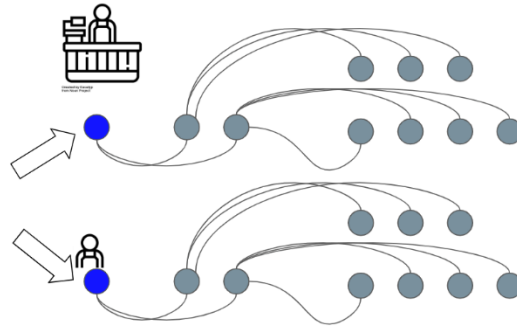
The takeaway is that repeated interactions with a malicious sender or recipient are dangerous. But it keeps getting worse!

Tainted Dust Attack

Remember when I mentioned that taint trees can be used to trace money going forward? After you make a payment, there's an uncertain cloud of possible transactions that could involve those funds. That can also be abused. For example, an attacker could find out where a friend – or family member, or ex-lover, or anyone else they know a bit about – is spending their money.

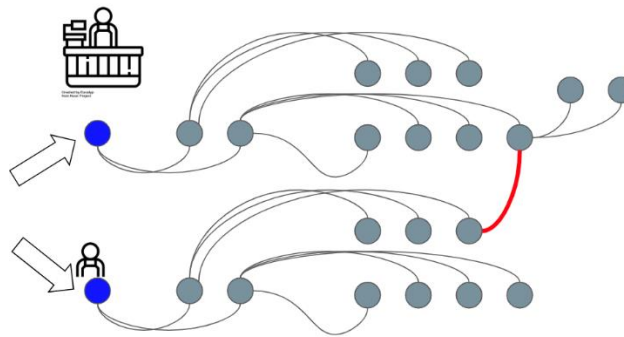
Let's say the attacker makes a small payment. It could even be a dust transaction. They make a payment to some merchant, and then to their victim. They keep watching as the taint tree grows out, as possible spends happen.

Tainted dust attack: seeing where money is spent



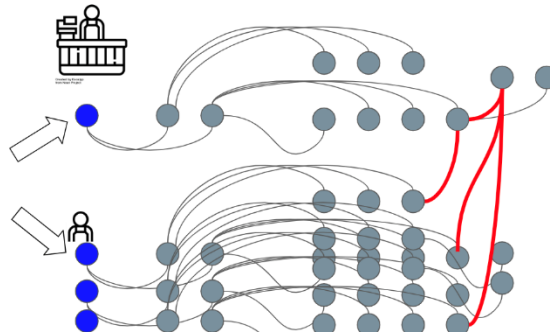
At some point, there's an interesting crossover. The attacker notices a transaction that seems to involve both the funds they sent to the merchant and the funds they sent to their victim.

Tainted dust attack: seeing where money is spent



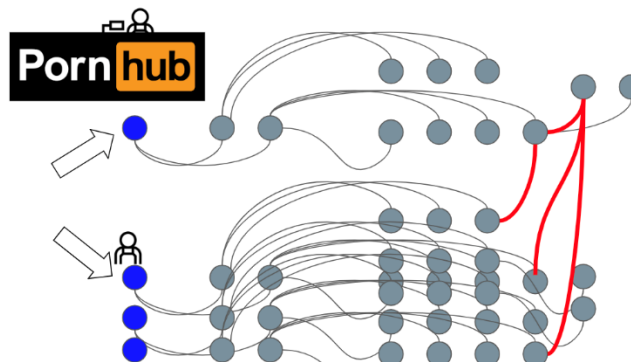
Many plausible explanations exist. The crossover could result from random decoys. Or perhaps the victim who received the attacker's transaction was spending money with the merchant in question. What the attacker now sees is the merchant moving funds out of a hot wallet, or spending them to pay bills, or whatever else. Again, any one instance is not definitive. But if the pattern repeats several times, then you have strong probabilistic evidence that your friend is making recurring payments to this merchant.

Tainted dust attack: seeing where money is spent



Law enforcement could use an analysis along these lines to validate that a particular person does indeed use a particular supplier. Or you could identify that your friend makes purchases on Pornhub. Which would be incredibly embarrassing for them, not because they're paying for porn, but because they're probably doing it using Verge.

Tainted dust attack: seeing where money is spent



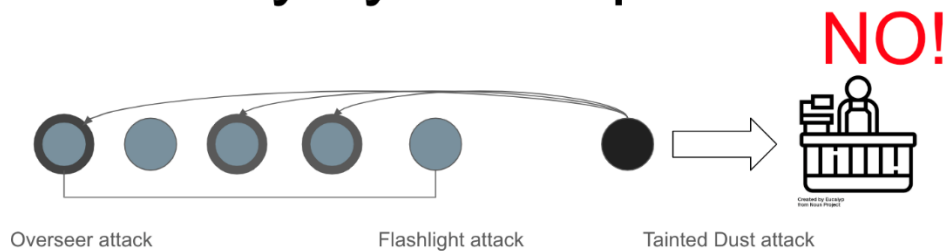
In summary, the limitations of decoy-based privacy systems are readily apparent once you threat model how attackers might approach them. You must consider what people can actively do, what they can't, and what goals they're likely to have. Various privacy proposals need this kind of rigorous evaluation or they can't be expected to stand up against clever adversaries (especially well-resourced ones). Cryptocurrency designers have to ask themselves, "If I were going to identify someone via this system, how would I go about it?"

The democracy activist taking donations over Tor might think, "I'm safe, I'm behind seven proxies!" But with a decoy-based system that isn't true. The moment someone

can start sending you tracking payments, and then get data from an exchange, you lose any and all privacy.

Solving Decoy Problems

Are decoy systems private?



The common perception of these various techniques seems to be, “Well, Bitcoin may not be private, but anything above-and-beyond Bitcoin will add meaningful privacy.” The reality is that specific techniques and implementations matter. The details are crucial. Users need to understand the tradeoffs afforded by the specific system they’re using. Buying modafinil has a different threat model from protesting an authoritarian regime.

I’m not saying that it’s impossible for decoy-based systems to provide meaningful privacy. If your decoy set is very large — think five million possible origins to identify, rather than five — that changes the probabilistic evidence that attackers can uncover. On top of that, the decoy sets would have to substantially overlap across all recent transactions. Otherwise you will still see repeated common origins when making multiple purchases with a merchant and so on.

Finally, it’s important to sample the decoys carefully. I won’t go into it here, but a [couple](#) of [papers](#) have shown that the distribution from which Monero sampled their decoys didn’t line up with the distribution of people’s transactions. There was a gap. In previous versions of Monero — this is now somewhat fixed — the last transaction in the decoy set was actually the real transaction, with overwhelming probability, because of recency preferences.

Most decoy-based systems are intended to be practical. In order to get substantial decoy sets, you can’t have systems that scale linearly in the number of decoys. Using

Monero and bulletproofs as an example, each additional decoy costs you 1-2 kilobytes in transaction size. It should be very clear, with linear scaling, that you're not going to have a transaction with 100 decoys in it, or 500, or a thousand. Proof generation and verification scale equivalently, which ruins the practicality.

What you need is logarithmic size. The transaction size should be logarithmic in your decoy set, and transaction generation and verification time should be at least logarithmic if not constant.

Zero-Knowledge Approach

I'm a little biased, but in my view the solution is a Zerocash-style protocol. Transaction outputs are commitments to the value in the recipient address, and you generate a Merkle tree over some fraction of the UTXO set, whatever you can afford computationally. A zero-knowledge proof is used to show that the origin of your payment exists in the UTXO Merkle tree. It can be verified without revealing the UTXO in question. This is where the privacy comes from. That's the basic approach of Zerocash, where the entire UTXO set is included in the Merkle tree.

How do you make that scalable? You have to pick a zk-proof technology that you like, and by "like" I mean: You think the cryptography is secure, you think that the assumptions are warranted, and the setup properties work for whatever operational requirements you have. It might be SNARKs, or STARKs, or bulletproofs. After choosing a zk-proof, you can tinker with scalability.

The scheme and parameters have been selected, so now you turn to efficiency. Start benchmarking. As the Merkle tree gets longer the transactions are going to get bigger and the verification times are going to slow down if your not using QAP-based zk-SNARKs like in Zcash.. The goal is finding a depth where efficiency meets your performance requirements. Maybe it's $d=32$, which Zcash Sapling uses. Maybe $d=4$, maybe 8, it doesn't really matter. Whatever you do, your decoy set is now 2^d , which exceeds most decoy-based approaches.

I should briefly note that the state of the art for these techniques is improving. With respect to zk-SNARKs, it's gone from taking ~40 seconds to like two seconds to generate a transaction. Huge amounts of memory used to be required, in excess of three gigabytes, and now it's 40 megabytes. Similarly, bulletproofs keep getting faster and faster.

Conclusion

We need to deeply consider our approaches to privacy. Cryptocurrencies should be built with robust, attack-resistance solutions for protecting financial information. That may happen on-chain, but it's not a given. The current mantra is that privacy will

be ensured off-chain. That's fine and I hope it works, but it doesn't absolve you from assessing the default weaknesses of your system. Merely because it's off-chain doesn't mean that information doesn't leak.

It's been interesting to observe the reactions to my talks at Scaling Bitcoin and Devcon. Some projects care giving their users accurate expectations. For example, the Grin project has [written up the state of its privacy protections](#). That's exactly what cryptocurrency developers should do, and the document is excellent. Grin's team took a very conservative position, talking about the privacy that is available now — not hypotheticals or privacy theater. My only concern is that Grin underplays the risks with leaking the transaction graph (what they call "inputs and outputs linking"). But all in all, the "Grin Privacy Primer" is very good, and I wish more groups would strive for equivalent clarity.

Unfortunately, many others have responded with the exact kind of privacy theater that I featured in my talk. It is irresponsible to claim that CT, stealth addresses, or Dandelion provide comprehensive or perfect privacy. None of those technologies address the issues that I've raised. None of them stop the flashlight attack that would allow governments to identify someone's legal identity by interacting with a dark-web site that accepts payments. It is a major concern for some users today, but privacy theater distracts from the real risks.

Finally, a number of people have noted that some of the attacks I mentioned may be hard to mount in practice, because of noise and large volumes of transactions. For the tainted dust attack, that's absolutely true. But it's not true at all for the flashlight attack or the overseer attack.

In general, the attacks that I described are thought experiments. The goal is to make you realize that many systems aren't as private as people think they are, and to guide explorations of the practical levels of privacy. It may be the case that with enough traffic and sufficiently large decoy set, you get viable privacy. However, barring an analysis proving that, we have to think about which implementations pass a basic smell test. Moreover, my examples are the basic attacks that come up when thinking through real-world cryptocurrency usage. Adversaries are clever, creative, and diligent.

Remember, passive third parties are not the only attackers. That's not the main threat that people face with existing technologies on the internet today. It's being tracked by companies, or malicious ex-lovers, or oppressive governments. Also remember that attacks only get better. We are in the early days of cryptocurrency functioning and usage. Compared to the internet or other older systems, we have very little experience with building or protecting cryptocurrencies.

By all means, choose to prioritize scaling over privacy. That is a reasonable choice to make as developers and as a community. But when you do that, understand what you're giving up in terms of privacy, and be transparent about it. Don't pick any random approach and say, "It adds some privacy, ergo the thing is completely private." That's not true; adding some privacy doesn't make a protocol private in totality, and users will still be vulnerable.

It took, what, 20 years for us to understand how bad the privacy problems with the internet were? Progress has accelerated, but a couple of years will not be enough. Five years, or 10, maybe. It's important to lay the groundwork for privacy now.

Why Monetary Maximalism could fall short of expectations

By [Su Zhu](#) and [Hasu](#)

Posted February 2, 2019

Monetary maximalism is the idea that in a free market for money one big winner will emerge and that the "soundest" money is in the best position to do so.

In a previous post I [wrote that](#) "every token competes in one massive power law distribution for the title of dominant non-sovereign monetary store of value. If it does not win this rat race (or comes to a close second or third place), its market share will, effectively, be zero."

The most popular argument for why that should be the case is that it already happened once – with gold.

There are two big assumptions baked into the grand narrative of monetary maximalism today. First, that the world will gravitate towards the soundest monetary-policy coin. And second, that gold-analogies are apt in describing Bitcoin.

We would argue that this is reasoning by analogy, and that the analogy is not self-evident even for many people inside crypto, let alone outside. We should steer clear of suggesting that we can use logic to determine how this will all play out.

Instead, we should realize that for Bitcoin to become what most of the community wishes it to be, there are multiple challenges to overcome that work as counterforces to the consolidation into one money. These counterforces are:

Misalignment of incentives with crypto companies

Crypto companies are funded with the goal to capture value – especially value that can weather both bull and bear markets. The result is a value capture layer on top of

Bitcoin with actors that over time evolve their own opinions that ultimately become social attacks on Bitcoin.

Many of these companies would lose if bitcoin was to become a mature store-of-value tomorrow and since they respond to their shareholders and not the Bitcoin community, it's in their best interest to prevent that.

The biggest “attack” on Bitcoin is the existence of altcoins. Investors and VCs are incentivized to push for a multicoin future because they can be paid for finding the next Bitcoin. Monetary maximalism ascending necessarily implies that this paradigm of crypto-as-tech would come to an end.

Exchanges like Coinbase are also incentivized to push for a multicoin future, as they benefit from people trading back and forth between different assets. Consolidation into one money would mean a massive decline in cross-currency trading. As an exchange, they love drama and volatility in the markets to attract traders. Their support for past contentious Bitcoin forks as an attempt to shape the protocol to suit the needs of their business and later pushing for a world where Bitcoin is just one of many assets have been entirely rational.

Miners can also decide to attack Bitcoin, with Bitmain as a prominent example. When they disliked the direction protocol development was going, possibly because they were afraid that a layered scaling approach would hurt their bottom line, they launched a social attack in the form of Bitcoin Cash. Even though the attack ultimately failed, the fork diluted Bitcoin's supply in the eyes of the public as well as its brand value.

If we look at who is actually incentivized to help Bitcoin become a mature SoV, in terms of crypto businesses there are shockingly few. A mature Bitcoin would force many of them out of business. And yet we find that Bitcoiners are constantly surprised by the so-called impure behavior of companies in this space.

Culture clash between different currencies

Because of crypto's unique nature of a [social layer and technical implementation](#) reinforcing each other, all networks are highly cultural in nature.

All coins get their properties from the shared beliefs of their holders. A strong culture has to be enforced so they can retain these properties against change.



Image

Source: [Unpacking Bitcoin's Social Contract](#)

Arjun Balaji and Yassine Elmandrja have recently [laid out](#) how almost all fundamental disagreements in crypto are not about details of implementation, but about the fundamental values that each project enshrines in their social layer.

The result is competing frameworks like “[Vision of the Constrained vs Unconstrained](#)”, “[Money crypto vs tech crypto](#)” or “[Autonomous](#) vs [Governed](#)”, proving that there is a lot to disagree about when it comes to culture.

Just as the world is unlikely to converge to a single culture, whether we are talking about politics, art, music, language or food, so too can crypto exist for a long time as a pluralistic collection of different cultures.

If we assume there are irreconcilable disagreements on the social layer between projects and that the value of each token is agreed upon at the social layer, then the logical conclusion is that people with different cultures will prefer – and hence monetize – different coins.

We claim Bitcoin is apolitical maximalist money, but in practice the political philosophy views of bitcoiners are homogenous, especially with regards to libertarianism, and distinct from other crypto communities (which your authors [have previously argued](#) is a dangerous mismatch).

Bitcoiners tend to be [objectivists](#) – they believe there is such a thing as objective moral truths. But let us not mistake strongly held opinions for provable truths. We can neither prove that global money will evolve through soft forks rather than hard forks, nor can we prove that a premine is worse than no premine.

We can only show that the tradeoffs are such that we believe certain approaches are more promising than others. But if people disagree with us and these projects don't actually implode as we predict, then this market can well stay fragmented forever.

Appealing to human biases

Beyond basic preferences that are the result of a different culture, there are some biases inherent to our thinking that can draw people away from Bitcoin's monetary maximalism and towards other forms of money.

The most familiar example is probably the unit bias. When faced with a selection of coins most people intuitively compare the price of one unit, without regard for the number of total units outstanding. As a result, they falsely assume the cheapest unit is underpriced relative to the others and buy it.

Then there are people who have a bias in favor of innovation and tend to promote the new over the old without really looking at its limitations or weaknesses. Pro-innovation bias could play a big role in Bitcoin's future as the incentives of this market (see earlier) are aligned in such a way that crypto companies and investors collectively benefit from a steady flow of new competitors.

The most important bias working against Bitcoin, however, might be the "anti-waste" or "anti-PoW" bias. Already today there are many who categorically refuse to use any currency that uses proof-of-work for security, claiming that it is extremely wasteful and hence dangerous to our environment.

You can expect Bitcoin competitors like Ethereum to lean even more on this bias once they have completed their switch to proof-of-stake.

It's hard to imagine that people with a strong ideological dislike for proof-of-work can be convinced by economic arguments to turn around and embrace it. We find it more likely that this particular bias will continue to appeal to many people in the same way that [easy answers to hard questions](#) have always appealed to humans throughout history.

Conclusion

While we don't fundamentally disagree with the idea that a big winner could emerge from the battle of monies in the ultra-long run, there are also significant counterforces at work to prevent Bitcoin from being that winner.

The counterforces presented today all assume that the market structure itself is uncompromised, i.e. a free market for money exists. In practice, this assumption is hopelessly optimistic. Governments will continue to shape our economic realities as

people in the Liberal West will not risk their lives to use one money over another for ideological reasons.

Most Bitcoiners are gleefully unaware of how few companies in this space actually have an incentive to help Bitcoin succeed, especially those who own the customer relationship and onboard all the new people into this space.

Bitcoiners should stop expecting companies, miners, etc. to virtue signal to them and instead [start taking ownership](#) of the means of production by building their own exchanges, nodes, wallets, custody, and education.

All cryptos are highly cultural. They need to be because they derive their properties from the shared beliefs of all users. This is a major differentiation from gold. The idea of Bitcoin monetary maximalism would require Bitcoin to transcend culture itself if it wants to appeal to people versus other cryptocurrencies.

Many people are questioning the “top-down” analogies used by bitcoiners today. Even many Austrian economists are not buying into Bitcoin [as sound money](#).

So instead of mapping the history of gold over the future of bitcoin, we should look where we are today, where we want to be tomorrow, and how we can get there.

Links

- <https://uncommoncore.co/a-deductive-valuation-framework-for-cryptocurrencies/>
- <http://artodyssey1.blogspot.com/2011/09/vytautas-laisonas.html>
- <https://uncommoncore.co/unpacking-bitcoins-social-contract/>
- <https://medium.com/@yelmanjraark/a-conflict-of-crypto-visions-160dbfc33bfa>
- <https://www.tokendaily.co/blog/money-crypto-vs-tech-crypto>
- <http://unenumerated.blogspot.com/2017/02/money-blockchains-and-social-scalability.html>
- <https://medium.com/cryptolawreview/against-szabos-law-for-a-new-crypto-legal-system-d00d0f3d3827>
- <https://uncommoncore.co/evangelizing-bitcoin/>
- [https://en.wikipedia.org/wiki/Objectivity_\(philosophy\)](https://en.wikipedia.org/wiki/Objectivity_(philosophy))
- <https://www.artstation.com/artwork/the-man-of-armadon-ebb515a7-7168-44da-a605-21baa34d1c71>
- <https://news.gallup.com/poll/240725/democrats-positive-socialism-capitalism.aspx>
- <https://www.artstation.com/artwork/k4Eqr2%EF%BB%BF>
- <https://en.wikipedia.org/wiki/Anarcho-communism>

- <https://mises.org/wire/why-cryptocurrencies-will-never-be-safe-havens>

Politics, Power & Protocols

Insights from (available) on-chain governance data

By [Meltem Demirors](#)

Posted February 5, 2019

Ah, humans. What wonderful and mysterious beings we are. Millennia of human history have shown us that the systems we create, especially our systems of politics, are inherently fragile and often extremely flawed.

As you consider the following discourse — please remember:

1. We are complex creatures who are **predictably irrational** in our behavior; we often build rules to protect us, from us.
2. The pursuit of an ***optimal structure for governance has plagued every ‘tribe’*** (society and organization) since human consciousness; and is ***still an unproven experiment (outcome TBD)***. Look no further than the fragility of our existing ‘democratic structures’ for evidence.
3. Governance occurs ***both within and between*** the institutions and entities that make up a system. Despite popular belief— ***it is not a static and fixed process***. It is ***largely dynamic and evolutionary***; dependent on interactions of actors in systems.

Governance for the sake of this conversation, is broadly defined as the set of processes that comprise how a state, market or system ‘makes rules’.

The familiar mechanisms of governance include: ***laws; cultural and social norms; language***.

Historically speaking, these are administered via both soft and hard expressions of power through ***violence, coercion, collusion***; and other more subtle mechanisms like ***social signaling*** and ***virtue signaling, appeals to authority***, and the like.

Collectively, the whole of these make up the nebulous idea of “governance.”

Sidebar: Much pontification has been done about the nature of on-chain and off-chain governance, as well as formal and informal governance mechanisms. Instead of providing a thorough review of this literature here, I will simply state that there are as many opinions as there are individuals expressing these. As you’ll likely agree, the optimal form of governance for each of us is that which serves our individual preferences and benefit, regardless of how deeply and

ardently we justify and rationalize these arguments. I am frequently confronted with my own biases and rationalizations for these, and must confess, I often question my own incentives in engaging in these debates.

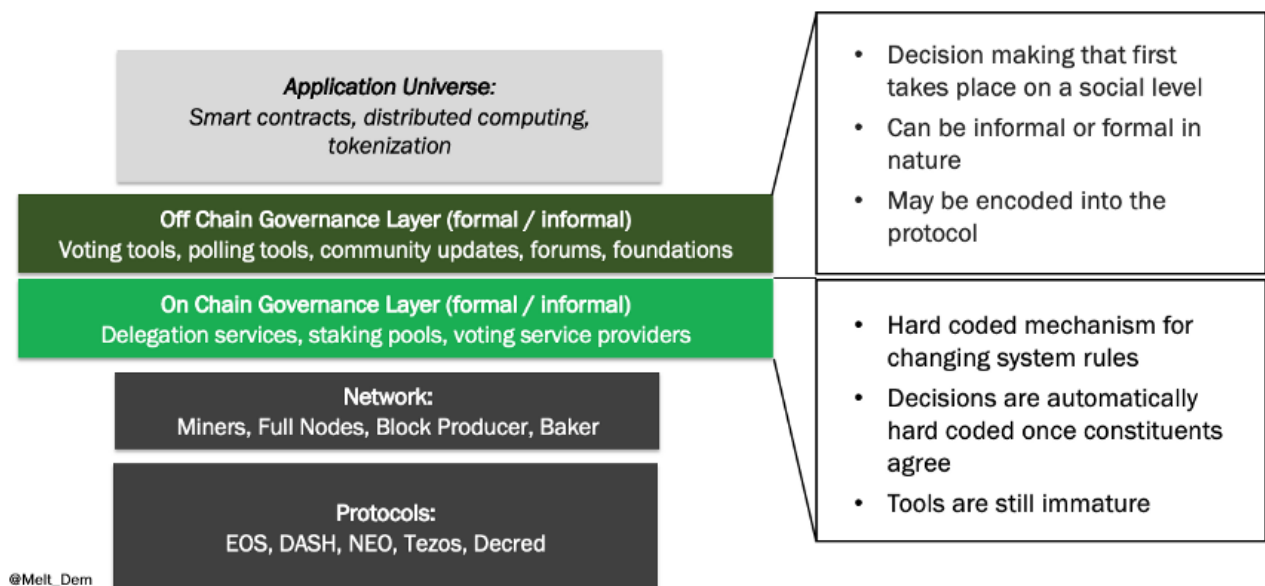
One of the pursuits of blockchain-based systems is the attempt to express governance at the 'protocol level' by codifying it into the function of the network itself—this post represents a summary of my current thinking on crypto governance experiments as they currently stand:

...Remember, Governance of human systems, organizations, and networks is still an unproven experiment (outcome TBD). Look no further than the fragility of our existing 'democratic structures' for evidence...

It turns out that translating or iterating on these historical analogs in 'blockchain land' often leads to similar results.

Let's take a look—in my view, current expressions of blockchain governance look like this:

GOVERNANCE IS AN EXPERIMENT



When the Aragon team asked me if I'd like to speak at [their conference](#), it became a great forcing function to summarize my

current thinking on crypto governance experiments as they currently stand...

I by no means believe my thoughts are unique or authoritative, and the process of informing my thinking by using data—as shared in the graphics that follow—was a hard fought battle indeed. More on this at the end.

Politics and power motivated my [writing on Tezos](#) over the summer—and this topic continues to fascinate me because the dynamics of most crypto protocols still revolve around quasi-political influencers who battle one another for influence and authority in the no-(wo)man’s land known as ‘Crypto Twitter.’

So, let’s begin with the most basic question.

Who Has The Right to Govern?

For the purposes of this piece, I decided to focus on the five largest networks deploying on-chain governance today, since this would give us some empirical evidence, however imperfect.

Here is a brief summary of these five networks, who has the right to govern each, and how participation varies based on these dynamics.

One More Side bar (I promise): I want to be careful not to conflate Proof of Stake, which is a consensus mechanism for securing the network, with governance—which is the process of decision making about changes to the network and how to utilize resources dedicated to the network. There is an emerging trend within protocols of using the same “Proof of Stake” tokens to vote, but there is a difference in function here, just using the same tokens (as opposed to systems like Aragon which have their own second, independent token dedicated to “voting.”) For the purposes of this post, I am talking about using tokens for governance, not security and sybil-resistance.

CURRENT ON-CHAIN GOVERNANCE PROJECTS

	CONSENSUS	AGE	PARTICIPATION	PARTIES	RISK MODEL
EOS	DPoS	<1 year	48% staked, 25% voted on BPs	21 BPs 100 SPs	No risk to vote for BPs
DASH	PoW + Proof of Service	5 years	55% in masternodes	4,662 active masternodes	No risk using masternode key
NEO	DBFT	2 years	Unclear	Foundation holds 50% of votes	No risk to vote for consensus nodes
Tezos	DPoS	<1 year	78% delegated	479 bakers	Delegate (no risk) Bake (risk)
Decred	Hybrid PoW PoS	3 years	48% staked for voting	23 VSPs hold 50% of tickets	Buy "tickets" to vote, pay txn fee

Sources: Tezos Foundation, Tr5can.io, DASH website, StakingRewards.com, EOS Authority voting statistics, Decred website and dcrstats.com, Cryptoslate, NEO.edu, Coinmonks
@Melt_Dem

These 5 networks represent roughly \$4B of market value
(as of 1/30/2019)

Disclosure: I participate in Tezos governance via Tezzigator, a baker and delegation service. You can see all of my investments and token holdings [here](#).

Three takeaways from this grid —

1. Each network has its own, nuanced mechanism for governance and these slight nuances make "participating" in each network incredibly time consuming.
2. The risks associated with "participating" in governance in each of these networks is also vastly different, and therefore, any wise participant would carefully weigh the potential risk and reward of their participation in on-chain governance before proceeding.
3. There are a number of additional risks that are difficult to capture succinctly, but it suffices to say, in **all** of these networks, active participation in governance is time consuming and requires a non-negligible investment of time and energy.

So let's take a look at the risks (and rewards):

RISK AND REWARD MATTER

	GOVERNANCE	SET UP	THREAT MODEL	ROI
EOS	Token holders vote for block producers	BPs \$100k+ to run, voting costs nothing	No risk to voters, may get paid by BP	n/a
DASH	Masternodes vote on governance decisions	1k DASH (\$67k) collateral	No risk using masternode key	7 – 10%
NEO	7 Consensus nodes, voted for by NEO holders	1000 GAS (2 nd token) needed to create vote	Low risk - time lock tokens in election	n/a
Tezos	Bakers vote in Amendment Process	Pay ~15% to delegate 10k XTZ (\$4k) to bake	Delegate (no risk) Bake (risk)	5 – 15%
Decred	Token holders buy tickets to "vote"	111 DCR (\$1.7k) per ticket, 1 – 5% to VSP	Time lock DCR to vote or use VSP	1% on avg but varies

Sources: Tezos Foundation, TzScan.io, DASH website, StakingRewards.com, EOS Authority voting statistics, Decred website and decrstats.com, Cryptoslate, NEO.edu, Coinmonks @Melt_Dem

The risks and rewards of participating in governance can be confusing

Looking at this very basic risk reward analysis, we can quickly start to determine where participation is profitable and where it is not, which might inform why we see certain networks gravitating toward more or less competitive dynamics in governance.

This leads me to my second, likely more accurate, question...

Demystifying Blockchain Not Bitcoin

By [David Nage](#)

Posted February 9, 2019

This is a conversation that needs to happen now. As many know, I have been part of the family office community for the last decade and have been working to educate my peers on crypto for the last two years. This article comes on the heels of two private luncheons this week, where we discussed crypto amongst other investment themes. The popular, but incorrect catch phrase, “blockchain, not bitcoin” came up several times and I attempt to identify several drivers of this narrative.

Some of you will read that catch phrase and be filled with 3 emotions: rage and disgust followed by annoyance. Others will think this is a logical separation, and...more importantly, will be more inclined to put their chips down on the Blockchain island.

Non-crypto focused investors hear about IBM and their work with Hyperledger; they hear about JP Morgan and Quorum. These are brand names no different than Nike, Pepsi and Ford; they’ve been comfortable with them for a long time—but in essence they don’t understand the fundamental differences in what IBM and other corporate entities are building (a permissioned DLT) versus what Bitcoin, Ethereum and other protocols are building.

Why does this divide exist? How did we get here?

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they’ll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

As Garrick Hileman writes:

“The 2008 financial crisis reached its nadir with the collapse of Lehman Brothers on September 15, just six weeks before Satoshi Nakamoto published the bitcoin paper”

This is what was given to the world after the financial crisis—a purely peer-to-peer version of electronic cash allowing online payments to be sent directly from one party to another without going through a financial institution.

Innovation and adaptation has occurred during the last decade, as observed with every other technology society has bore witness to. In addition to Bitcoin we’ve seen other protocols leveraging the proof-of-work consensus algorithms and we’ve seen other consensus algorithms be created, such as proof-of-stake.

This discussion is NOT going to delve into which is the best and why, etc. However, at the very core, there is a fundamental lack of understanding from the perspective of the Institutional Investor on several main tenets which need to be illuminated:

1. Difference in Distributed, Centralized and Decentralized Systems;
2. Why we (as a society) need them;
3. Contributor (node) and Incentive models and;
4. Why it can’t be in the form of fiat/USD.

Distributed Systems

The work done by Stanislav Kozlovski: “[A Thorough Introduction to Distributed Systems](#)” provides color on this; as stated:

A distributed system in its most simplest definition is a group of computers working together as to appear as a single computer to the end-user.

These machines have a shared state, operate concurrently and can fail independently without affecting the whole system’s uptime.

Distributed But Centralized

As [Julia Poenitzsch](#) writes:

A distributed, but centralized system may sound contradictory but consider a cloud service provider offering a data storage service. Physically, your data could be shared and replicated on different machines according to resource availability and resiliency(distributed). However, wherever the machines and data storage facilities happen to be, the cloud service provider still controls them all (centralized).

Distributed systems and ledgers can be either decentralized, granting equal rights within the protocol to all participants or centralized, designating certain users particular rights.

Decentralized Systems

Decentralized and distributed systems, such as Bitcoin, cannot be altered by any one entity. It also runs as a **peer-to-peer network** of independent computers spread across the globe.

In conversations with Institutional Investors they understand concepts associated with Distributed Systems but this shift from centrally controlled distributed systems to a P2P network of “**independent**” computers/nodes is where the confusion comes in.

Why We Need Them

Decentralized, distributed systems offer advantages to their legacy centralized systems. Two of the more pronounced arguments in favor of these new systems that may resonate with traditional, non-crypto investors are:

1. **Fault Tolerance:** Because they rely on many separate components, decentralized systems are less likely to fail accidentally. The recent [Wells Fargo](#) outage serves as evidence of legacy systems failing.
2. **Attack resistance:** Due to the presence of a lot of players, decentralized systems lack central points of failure; there's no one point of attack that would disarm the entire system. This makes it more expensive and less viable to destroy these systems. This [infographic](#) is very useful to explain the significant amounts of data hacks we as a society have fallen victim to over the last decade and a half.

Incentive Models

Cathy Barrera discusses how incentive models help crypto: “[Blockchain Incentive Structures: What they are and why they matter](#)”

As Cathy notes:

An incentive is any design element of a system that influences the behavior of system participants by changing the relative costs and benefits of choices those participants may make.

Incentives include pay-for-performance reward systems that compensate individuals with money and they also include systems that incorporate no financial rewards at all.

Economics of Bitcoin

As Bitcoin.org states:

Bitcoins have value because they are useful as a form of money. Bitcoin has the characteristics of money (durability, portability, fungibility, scarcity, divisibility, and recognizability) based on the properties of mathematics rather than relying on physical properties (like gold and silver) or trust in central authorities (like fiat currencies). In short, Bitcoin is backed by mathematics. With these attributes, all that is required for a form of money to hold value is trust and adoption. In the case of Bitcoin, this can be measured by its growing base of users, merchants, and startups. As with all currency, bitcoin's value comes only and directly from people willing to accept them as payment.

This is a fundamentally misunderstood concept; more and more I hear “why can’t a bitcoin/blockchain miner be paid in USD/fiat”. This sounds ridiculous to people who’ve been in the ecosystem for years, but this phrase comes from multiple conversations with HNW/Family Office investors. Investors need more education on this topic because it is essential that they understand it.

Conclusion

Bitcoin, blockchain and the phrase “crypto” are part of the conversation among Institutional Investors these days; education from crypto investors, researchers and builders has significantly improved over the last year but there continues to be significant deficits in understanding the fundamental roots of the technology. Conversations with investors should focus on the four areas highlighted in this article; especially during the elongated “crypto winter” so they better understand the massive tectonic shift that is underway.

Who Has the Will to Govern?

Given that it's so time consuming to follow all of these protocols, to know the main actors and main influencers, to track development updates, to track network evolution and growth, and to track the flow of money—it's beginning to become clear that there are really two, perhaps three, key motivations for those who participate in governance.

1. Money
2. Power
3. Curiosity / Masochism / Insanity (*Perhaps*)

It's no real surprise that money and power dominate the conversation when it comes to governance. People were outraged when I suggested as much in my thinking around [Tezos](#), but as more proof of stake protocols emerge, I imagine we'll start to see the beginnings of crusades and ideological wars between the entities below.

THE DYNAMICS OF POWER

EXCHANGE USERS	FUNDS / VCs	FOUNDATION	PROJECT TEAM
			
• Users have no control over keys or assets • Limited ability to stake or delegate tokens will on exchange • Some exchanges may delegate tokens for profit without informing users	• Vested interest in specific outcomes • Heavily pursued by "service providers" who charge 10%+ • Sometimes collude to run their own pools for staking	• Typically do not have the right to participate in governance / vote • Often receive a reward from voting or can be granted more capital • May support research into governance tools	• Limited clarity as to how many tokens teams received and if they are staking / participating • Limited disclosure around conflicts

@Melt_Dem

Collusion, coercion, manipulation, lobbying, bribing, and gerrymandering are part and parcel to the processes of modern democracies.

It would be foolish to believe that crypto governance would be absent these forces, and many systems, while they may be technically robust, are susceptible to social engineering.

We already see coercion and collusion for instance, in EOS, where there have been numerous accusations and in-depth investigations of collusion and cartel-like behavior amongst exchanges, investors, and the Block.one team.

DIFFICULT TO UNTANGLE INCENTIVES

	EXCHANGES	INVESTORS	FOUNDATION	TEAM
EOS	Bitfinex and others enable voting	>70% of EOS held by 100 addresses	Block.one controls 10% of voting power	Unknown how much EOS team owns
DASH	Must run own masternode	Most masternodes run by investors	Sell memberships, receive 10% of BR	Unknown
NEO	Unclear	Unclear	Foundation holds 50% of votes	Team holds 10% of foundation tokens
Tezos	Run own baker or delegate for users	Investors running own bakers	Foundations holds 10% of tokens	Founders got 8.5% of tokens
Decred	Must buy tickets outside exchange	Running staking operations	10% of tokens go to foundation for "dev"	8% dev subsidy, 9% dev pre-mine

Sources: Tezos Foundation, TzScan.io, DASH website, StakingRewards.com, EOS Authority voting statistics, Decred website and dorstats.com, Cryptoslate, NEO.edu, Coinmonks

@Melt_Dem

It's very difficult to find reliable information about stakeholders and their participation in formal, on-chain governance, as well as their motivations

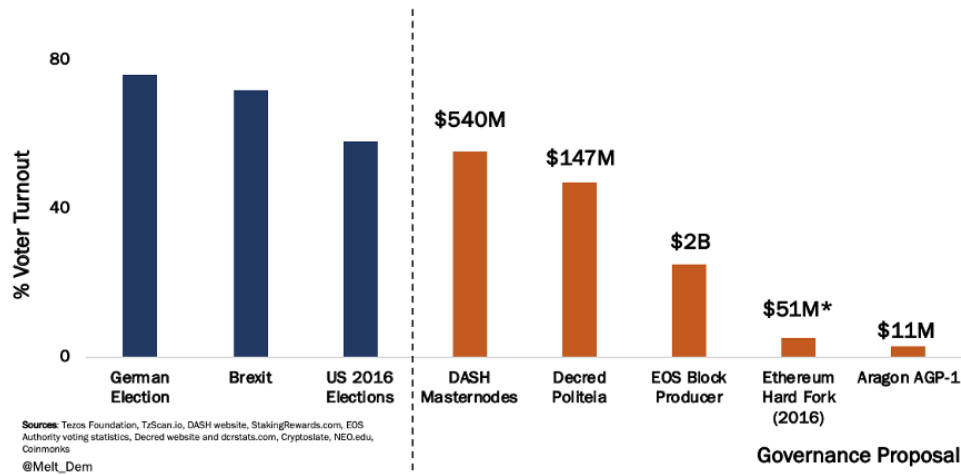
In fact, as I was writing this, the Cosmos team [merged a change](#) to remove a cartel with 53% of voting power from "Game of Stakes"—their testnet.

Looking at the five protocols I analyzed, it's easy to see the balance of power amongst network participants.

How Is [Exertion of] Power Measured In This Model

Perhaps the best way to measure the ability for participants in a system to express their will is to look at the turnout rate for votes.

TURNOUT DEPENDS ON STAKES

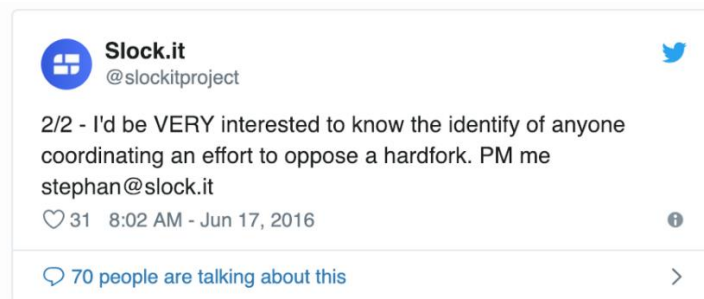


As we can see, participation in each protocol is challenging to measure, and I fully agree (with you, the reader yelling at the screen) that the above is an imperfect measure.

However, it's a starting point, and highlights a few key issues at play here:

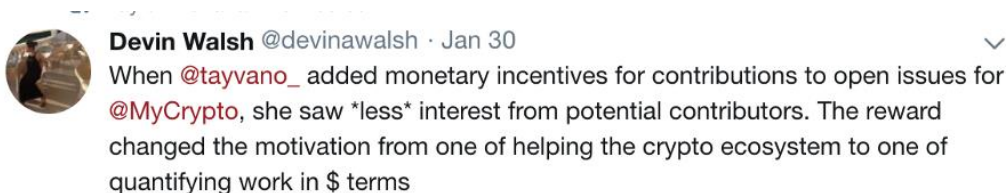
- **Ease of Voting:** If voting is difficult, whether it be technically difficult (e.g. needing specialized hardware or specialized technical competence) or physically difficult (e.g. needing to travel somewhere or have robust connectivity to a network) turnout is likely to be lower. Today, most blockchain-based voting mechanisms feel clunky to users, and therefore casual users are unlikely to invest the time and energy to participate in voting if it requires using new software or paying for tickets, etc. This is why increasingly, funds with numerous token holdings are relying on staking-as-a-service providers to offer their specialized expertise, as these funds don't have the time to manage the mechanics of five, let alone fifty protocols. ***Specialization will inherently emerge as these systems grow in complexity.***
- **Importance of Voting Issue:** Depending on the issue at hand, voters may turn out in higher or lower numbers. I've attempted to capture the "magnitude" of each crypto governance vote in the graphic above, but again, the true stakes of these votes are difficult to identify. What we do see is when issues really matter, whether ideologically, socially, or financially, voters turn up. For example, very few EOS holders vote for block producers because they feel their vote doesn't really matter. Some EOS holders I polled said they feel the BP selection process is so heavily dominated by large EOS holders like exchanges, EOS founders, and early EOS investors, that it isn't worth their time and energy to participate. Perhaps these users feel the way a democratic voter feels in a republican state during US elections...

- **Risk of Voting:** If voting represents potential risks, either social (reputation damage or privacy loss); financial (capital loss); or physical (violence) then turnout is likely to be lower. In most current systems, voters are compensated for taking risk by putting their assets “on chain” or in escrow by getting a direct vote, while those who don’t get little say. However, one of the aspects that hasn’t been covered as widely is ‘reputational risk’ and privacy. For voting to be effective, privacy is tantamount. ***Should it be possible for participants to express unpopular opinions without feeling like they’ll be ostracized*** by the hordes on crypto twitter? I believe yes, but others (see below) may not share that sentiment. We’ll also cover this later under the topic of “ochlocracy” or rule by mob.



Source: Peter Todd's writing on the Ethereum hard fork ([link](#))

- **Personal Gain:** The most important factor of all is how much someone stands to gain by participating in governance via voting. ***In my view, what on-chain governance has done most effectively is put a price on network participation.*** This is a rather contrarian view, but I believe networks that provide a financial reward for ‘politicking’ will become over-run with the types of people attracted to these schemes. As someone who spends most of her time in bitcoin, where there isn’t a direct link between participation and compensation, and everyone is a volunteer, I wonder if we lose some of the magic of “community” when we ‘financial-ize’ participation.

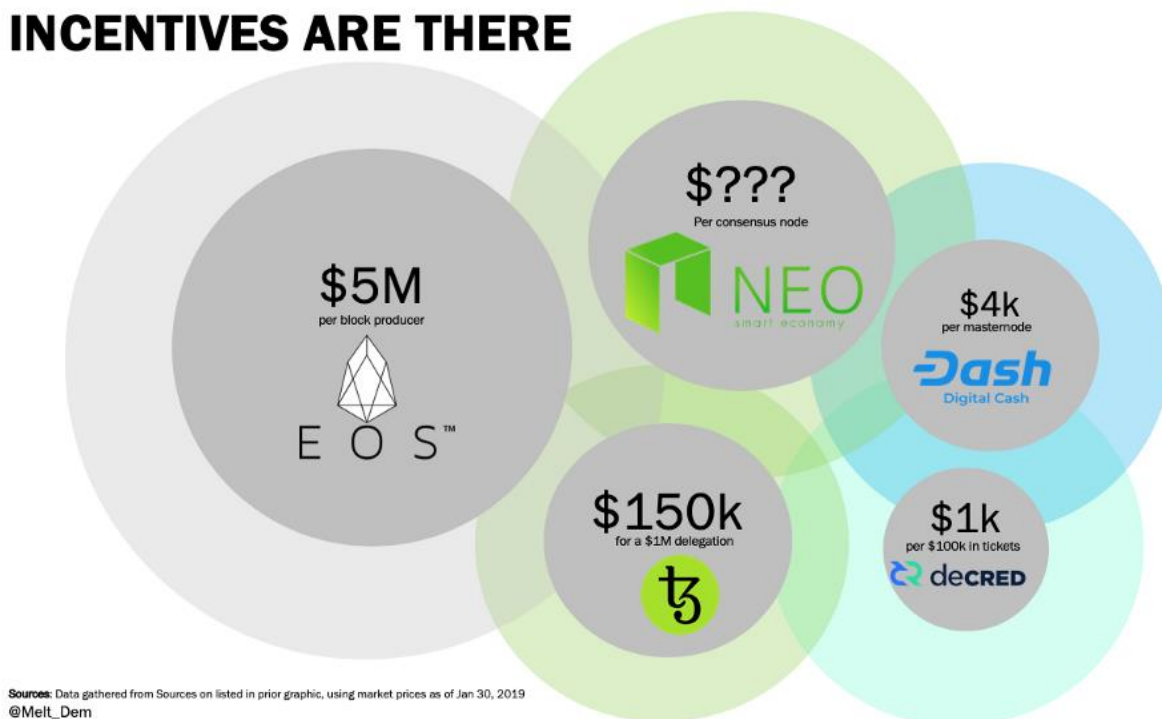


Similar observations in [another conversation](#) at AraCon2019 — by [Taylor Monahan](#) via [Devin Walsh](#)

A Rising Tide Lifts All Boats (Stakes)

The stakes in these games of governance will only continue to grow. The below graph represents the financial incentives at play in each of these protocols. The financial incentives will only grow as the value of these networks grow, and as the stakes continue to increase, I expect increasingly sophisticated players to enter the market for governance.

INCENTIVES ARE THERE



Not my best bubble chart, so don't come @ me — I know the sizes are not to scale :D

We also can't ignore the unquantifiable “path dependency” stakes in these protocols, which we saw play out in bitcoin's political landscape over the last three years.

Many people building businesses on top of these networks are dependent on certain changes being implemented. Make no mistake, the ability to influence and control the future development of the network—what changes get merged, how governance itself evolves—in the right hands, can be priceless.

The Future of On-Chain Governance

So where does this leave us? While I'd love to imagine a world where governance is perfectly competitive and many service providers emerge to offer users practical

tools, I believe the current state of on-chain governance is trending more towards oligopolies.

Each protocol has its own ruling party and its own oligarchs, some better known than others, and these parties will collaborate to maximize outcomes in their own favor.

Mind you, those outcomes might also happen to be optimal for all network participants; **negative externalities do not have to manifest as a result.**

PUTTING IT ALL TOGETHER



Explicit or implicit agreements to collude to maximize profits can take the form of joint ventures, mergers, partnerships, and cartels

@Melt_Dem

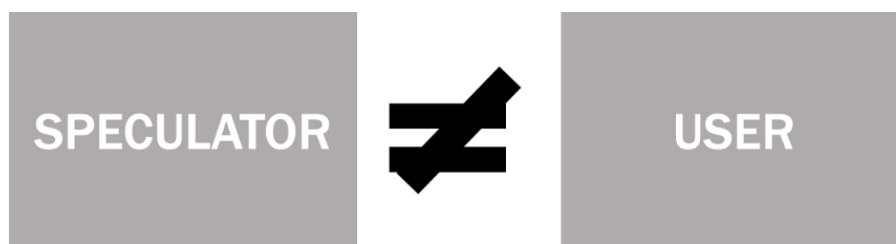
I do believe certain exchanges, investors and individuals will align themselves with specific protocols where they can “govern” or exert control more effectively; and play a more active role in shaping the future.

We already see this already, in the form of services like [Staked](#) and [Battlestar Capital](#)*, which support crypto funds by “compounding” their crypto and taking advantage of the opportunity to earn financial returns via staking.

It’s odd to me that the politics of staking-as-a-service providers haven’t been discussed, but it doesn’t take a leap of the imagination to see that large service providers could effectively become “cartels-in-a-box” for large investors.

You may balk at the use of the word ‘cartel,’ as it brings to mind images of drug kingpins and oil-rich kleptocracies...calm your imagination... cartels have a rich history in emerging markets, particularly in new industries, where economics dictate that collusion is more profitable than no collusion, and consumers have few alternatives.

While to date, the incentives of investors (speculators) and networks have been largely aligned, I would not expect that to be the case in the future.



When will we learn?

I know I keep belaboring the point, but remember that speculators, i.e. investors with fiduciary obligations, are **not users.**

Therefore, I'm extremely wary of projects where speculative investors control more than 50% of the tokens, and therefore, 50% of the votes.

Some investors may convince you they are there to do what is best for the protocol, and I do believe that many investors provide positive contributions to the crypto community.

Of course, I am myself an investor, and therefore fall into this same camp. I have no illusions about the conflicts of interest here.

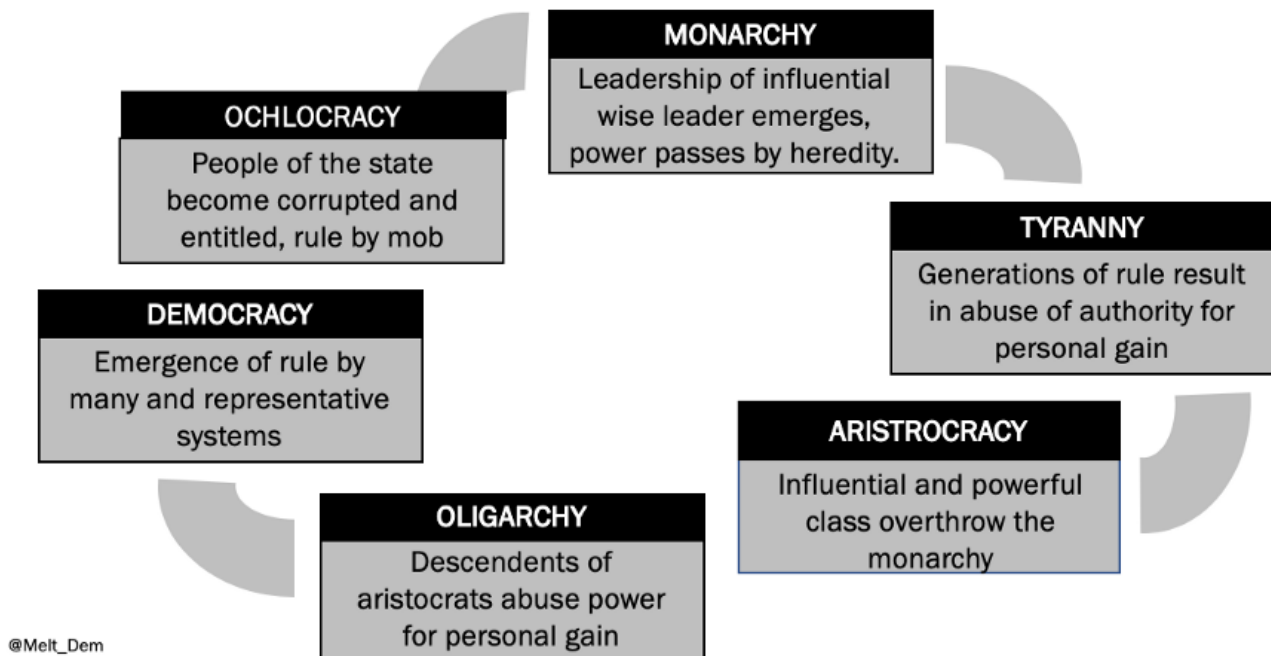
The “cartel of good intentions” (see this [Foreign Policy article](#) which helpfully [introduces and defines the phrase](#)) ultimately is all about charting a course which maximizes profit.

While we may all have the best of intentions, ultimately, tools are neither inherently good or bad, just or unjust. It is in their use, by humans, that these tools can take on this character.

The phrase “absolute power corrupts absolutely” is perhaps a fitting reminder of what happens when we couple power with politics in protocols. Perhaps borrowing from history would be most appropriate here.

Most forms of governance begin as “benign” in nature—whether it be monarchy, aristocracy, or democracy. Over time, these benign and weak forms of governance are abused and become malignant, devolving into tyranny, oligarchy, and ochlocracy. Eventually, those subject to malignant rule overthrow it in favor of a more benign form of rule, and the cycle begins a new.

POLYBIUS' SEQUENCE



This pattern, called [anacyclosis](#) or Kyklos, features heavily in the writing of Aristotle and Plato

One needs only glance at the world of cryptocurrencies to see these patterns play out repeatedly:

Arguably, the emergence of governance oriented protocols was a direct response to the perceived tyranny of bitcoin. But as these protocols are implemented and their governance mechanisms activated, we see them, in turn, plagued by their own unique forms of dysfunction.

Perhaps the ultimate fate of many of these systems is rule by mob, where we all scream at one another on crypto twitter, until we see a wise ruler emerge (via Medium post, of course) who tames us all and decrees how it *shall* be going forward.

Perhaps, history can inform us as to the mistakes of the past and what has been learned from these. Again, Polybius, in his eternal wisdom, has some key lessons to impart (*which I've commented on in italics*)

- **Tenure of rulers must be kept short to prevent them becoming despots**
(Many networks rely on benevolent dictators, and I continue to believe one of the brilliant aspects of bitcoin's design is Satoshi's disappearance. Likewise,

Charlie Lee stepping away from Litecoin and Ricardo Spagni (fluffypony) stepping away from Monero could be interpreted similarly.)

- **External threats, whether real or imagined, preserve internal peace** *(We see this play out with many protocols, and its what makes the phrase “short the bankers, long bitcoin” and others like it so appealing. Rallying cries like these provide social unity and justify many forms of behavior in defense of a common good. See “The Banality of Evil” for further reading on this.)*
- **If any one individual gains too much power—whether it be monetary, political, or military—banish them** *(We have seen this play out, and perhaps the Bitcoin forks are a great example of people choosing to banish themselves.)*
- **Decision makers and governance bodies must never accept money to make decisions** *(This is in direct conflict with the idea of staking for return, and lobbying will inevitably become part of the industry as the size of these networks and the money and influence at stake continues to grow. Perhaps blockchains will change this, but I find it doubtful, because human nature, ya know.)*
- **The middle class must be large** *(This topic is controversial, but in my view, the initial distribution of wealth ie tokens matters greatly to future decision making. Balaji Srinivasan did some [helpful writing](#) on this topic, I discussed it at the [World Economic Forum](#) last year, and there is a lot of discussion around what is and isn't fair initial distribution, and whether or not it matters. Hopefully by this point, I've been able to demonstrate why in protocols with on-chain governance, initial asset distribution matters greatly.)*
- **If all citizens are aware of law, history, and constitution, they will endeavor to maintain “good” governance** *(Perhaps this is my greatest takeaway of all. Much of crypto governance tends to veer into the territory of ideas that have already been implemented or tried before, without an active acknowledgement of the failures and dangers of these designs. If nothing else, this post hopefully helps provide some context on how we might at least begin to understand our role in on-chain governance systems and what we may do to make them more likely to succeed at their stated intent.)*

Who knows how the future will unfold.

I have some ideas, some of which are shared above, but nothing is certain.

Part of the fun here is watching these ideas unfold in real time. As more and more Proof of Stake networks go live, it will be fascinating to see how these new networks evolve and grow to maneuver around the risks outlined above.

I am particularly intrigued by Cosmos, given its attempts to actively remove cartels from the system, and if and how that will prompt cries of “de-platforming” from those who happen to run these cartels. After all, the beauty of blockchain networks is

their un-censorable nature, which means intent in design becomes all the more important. If abuse is possible in your design, then is it the fault of the abuser or the designer? Arguably, using the rules to play the game in a manner different than which it was designed for isn't a crime.

In the meantime, I continue to actively track the economics of staking, and to date, have chosen to focus primarily on Tezos to further my learning and my experimentation with proof of stake and on-chain governance. However, over time, this may change, and I look forward to sharing what I learn with the community.

A Few Final Comments

1. **Tracking the Data:** Gathering data for this piece was challenging, to say the least. A special thanks to [TzScan](#), [Eos Authority](#), [DCR Stats](#), and [StakingRewards.com](#), just to name a few of the sources I relied on heavily. I'd like to see protocol teams or foundations *themselves* also start to adopt, implement, and track more robust frameworks to track, analyze, and socialize key data points around their governance schemes. ***Maybe this is a gap Messari* will fill (cc: TwoBitIdiot)***
2. **Slides:** You can see and download the slides from this talk here [Speakerdeck](#), and see other slides I've published [here](#) (not always up to date, but I try). Feel free to borrow and use as you like, but please attribute when and where appropriate.
3. **Notes and Disclosures:** *The Battlestar Capital team works out of our NY office, and we engage in a lot of lively debates around the economics and politics of staking, so it could be argued that I'm biased here. *I'm an investor in Messari.

Links

- <https://www.youtube.com/watch?v=wfcro5iM5vw>
- <https://aracon.one/>
- https://medium.com/@Melt_Dem/the-tezos-experiment-b97e124e5b38
- <https://www.meltemdemirors.com/disclosure>
- <https://github.com/cosmos/game-of-stakes/pull/263>
- <https://petertodd.org/2016/ethereum-dao-bailout-vote>
- <https://twitter.com/devinawalsh/status/1090553366218969093>
- <https://medium.com/@tayvano>
- <https://medium.com/@devinwalsh>
- <https://staked.us/>
- <https://battlestarcap.com/>
- <https://foreignpolicy.com/2009/11/11/the-cartel-of-good-intentions/>
- <https://en.wikipedia.org/wiki/Anacyclosis>
- <https://news.earn.com/quantifying-decentralization-e39db233c28e>

- <https://www.youtube.com/watch?v=fQ0YkPCdxZ8>
- <https://tzscan.io/>
- <https://eosauthority.com/voting>
- <https://dcrstats.com/>
- <https://stakingrewards.com/>
- <https://messari.io/>
- <https://medium.com/@twobitidiot>
- <https://speakerdeck.com/meltdem/power-by-proxy-the-case-for-crypto-cartels>
- <https://www.meltemdemirors.com/content>

Bitcoin is a hedge against the cashless society

By [Su Zhu](#) and [Hasu](#)

Posted February 12, 2019

When cash is gone, where will you turn to transact with a basic level of privacy? What money do you hold when negative interest rates start eating away at your bank account?

The rise of digital payments and the move towards a cashless society are often seen as the same, but there is an important difference between them.

Digital payments like Paypal, Venmo, domestic-, and international bank transfers are convenient for people and businesses to transact with. They represent fintech innovation to consumers by the market. Faster, cheaper, and more efficient forms of digital payments are uncontroversial and largely an engineering and marketing challenge.

They don't however, remove every need for cash. Cash [has unique properties](#) that digital payments have not. As physical coins and notes, it can be exchanged peer-to-peer without a middleman. Its ownership is transferred simply by handing it over. The absence of an intermediary ensures that transfers are permissionless, censorship-resistant and, most importantly, private.

Digital payments solutions do not utilize physical cash but also do not prevent anyone from continuing to use cash if they want. It is an alternative payment method to cash but is not antithetical to it. Indeed, in almost all modern societies, there coexists both a large digital economy and a large cash economy.

We will argue that the elimination of cash, even if most payments are already digital, will make society more vulnerable to surveillance, financial control, and authoritarianism.

Why do countries go cashless?

In a cashless society, the government seeks to discourage or even criminalize the holding and using of cash itself. In [Sweden](#), it happened largely without coercion. In [India](#), the government demonetized the 500 and 1,000 Rupee denominations of notes.

Different countries can have different incentives to push for a cashless society. In China, digital payments are primarily a tool of social control and serve as a backbone

for China's social credit system. And they are making progress on it: 96% of cash payments in 2012 have turned into only 15% in 2019.

Over in Europe, central bankers are enthralled by the idea of negative interest rates. A recent IMF report [states that](#):

“Severe recessions have historically required 3–6 percentage points cut in policy rates. If another crisis happens, few countries would have that kind of room for monetary policy to respond.”

Negative interest rates were traditionally hard to implement because cash served as a lower bound. In a cashless society, this lower bound would disappear. In a severe recession, the CB could drop the policy rate to, say, -4% to make consumption and investment more attractive relative to saving.

Recently, central banks have started to brush everyone who prefers cash with the label of a criminal. They do that by separating the uses of cash into [legitimate and illegitimate](#). People “abroad” can hold cash “legitimately” to replace an unstable or inflationary currency. Now domestically, the only beneficiaries of an anonymity-providing currency are

“those engaged in tax evasion, money laundering and the financing of terrorism, and those wishing to store the proceeds from crime and the means to commit further crimes.”

Indeed, the use of cash in larger denominations has become so stigmatized in the US and Europe that withdrawing or carrying above a certain amount requires explicit government permission.

Problems of the cashless society

A society without cash has no ability to transact value without the omnipresence of government actors. By going cashless, societies double down on the properties of digital payments but lose all access to the unique properties of cash.

If every payment is intermediated, it becomes impossible to pay someone for anything without there being a record somewhere. It eliminates privacy and places the government as the third party in every financial event.

Governments claim that a cashless society enables them to protect citizens from criminals. The specters of terrorism and organized crime are often cited at this point. But this makes the naive assumption that governments itself can never become evil.

Because all transactions require the consent of an intermediary, they can easily be censored and funds confiscated. It might not be happening right now, but a good monetary system should be robust to changes in political moods. A cashless monetary system is less resistant to both the tyranny of the majority and shifts towards authoritarianism.

Cash may not be the right tool for the majority of transactions, but the elimination of it removes an important choice, and safeguard against government abuse, for the people.

Bitcoin as a hedge against the cashless society

When cash is gone, where will you turn to transact with a basic level of privacy? What money do you hold when negative interest rates start eating away at your bank account?

Traditionally, it has been impossible for the private market to come up with solutions for these basic human demands. The state doesn't like competition to their own fiat currency and made sure to quickly shut down all attempts of other monies to enter the market.

Bitcoin could change that. Decentralized and digital in nature, it no longer has the central point of failure that made previous "private monies" vulnerable. And it is modeled to marry the two forms of money – physical cash and digital payments – into an entirely new breed: digital cash. It can be transacted peer-to-peer, is permissionless, does not censor people or transactions, and has a reasonable level of privacy (if one knows how to use it).

We are still early into the Bitcoin-experiment, but with the cashless society looming on the horizon, we more than ever need it to succeed. Its fixed monetary policy already makes it a hedge against high inflation (that is increasingly used in places with collapsing fiat currencies [like Venezuela](#)). But, equally importantly, Bitcoin is a hedge against the demonetization of cash and the rise of the cashless society.

Links

- <https://coincenter.org/files/2019-02/the-case-for-electronic-cash-coin-center.pdf>
- <https://www.weforum.org/agenda/2018/11/sweden-cashless-society-is-no-longer-a-utopia/>
- https://en.wikipedia.org/wiki/2016_Indian_banknote_demonetisation
- <https://blogs.imf.org/2019/02/05/cashing-in-how-to-make-negative-interest-rates-work/>
- <https://www.nber.org/papers/w15118.pdf>

- <https://medium.com/@mattahlborg/nuanced-analysis-of-localbitcoins-data-suggests-bitcoin-is-working-as-satoshi-intended-d8b04d3ac7b2>

Security Budget in the Long Run

By [Paul Sztorc](#)

Posted February 12, 2019

“A discussion of Bitcoin’s ability to resist 51% attacks (ie, its “security budget”). Competition makes it difficult for one network to collect enough fees – instead, we should try to collect fees from all networks.”

This post is a somewhat more-empirical sequel to [“Two Types of Blockspace Demand”](#). And to my [Building-on-Bitcoin](#) talk.

1. The “Security Budget”

Bitcoin’s [“security budget”](#) is the total amount of money we pay to miners (or, if you prefer, the total amount spent on mining – they are the same thing). When this value is low, 51% attacks are cheap. In 2018, BTC’s security budget was [about \\$7 million per day](#). So, the suppression of BTC (via a never-ending campaign of 51% attacks) would cost –at most– \$2.6 billion per year.

\$2.6 B is pretty low – by comparison, the 2017 annual US Military Budget was \$590 billion, and the [FED’s annual operating expenses](#) totaled \$5.7 billion.

2. The Block Subsidy

Fortunately, we can expect the *block subsidy* to give us more security in the future. Even though it “halves” once every four years (effectively falling by a factor of 0.84 per year), it hits for full force no matter how high the BTC exchange rate climbs. As long as annual appreciation 19%+, it fully compensates for the PP lost to the halvening. Historically, the rate has been *much* higher than 19% (more like 70%+), and so the security budget has increased substantially over time, and will continue to do so for a while.

Of course, eventually the exchange rate must stop appreciating. Even [if Bitcoin is outrageously successful](#), it will apparently reach a point where it simply cannot grow faster than 1.077 per year¹, as this is apparently the growth in the nominal value of all the world’s money.

Here I show the growth, and ultimate decline of the security budget:

Security Budget over next 40 yrs, if Fees are Zero						
Year	Subsidy	Exchange Rate (theoretical maximum)	Exchange Rate (market-imputed)	BTC Security Budget (billions per year)	USA Defense Spending (billions per year)	Safety Ratio
	from protocol	x_2017 = \$11.22M, growth = 1.077	x_2016 = \$700, growth = 1.6265; blended with maximum	= Subsidy * Exchange Rate (m.l.) * 6 * 24 * 365 * (1/1e9)	x_2015 = 637, growth = 1.047	Security B. / Defense B.
2008	50	\$2,725,960	\$0	\$0.00	\$461.76	0.000
2012	25	\$3,671,828	\$100	\$0.13	\$554.95	0.000
2016	12.5	\$4,945,897	\$700	\$0.46	\$666.96	0.001
2020	6.25	\$6,662,050	\$4,900	\$1.61	\$801.57	0.002
2024	3.125	\$8,973,683	\$75,000	\$12.32	\$963.36	0.013
2028	1.5625	\$12,087,419	\$800,000	\$65.70	\$1,157.79	0.057
2032	0.78125	\$16,281,574	\$15,000,000	\$615.94	\$1,391.47	0.443
2036	3.9E-01	\$21,931,039	\$21,931,039	\$450.27	\$1,672.32	0.269
2040	2.0E-01	\$29,540,785	\$29,540,785	\$303.25	\$2,009.85	0.151
2044	9.8E-02	\$39,790,999	\$39,790,999	\$204.24	\$2,415.50	0.085
2048	4.9E-02	\$53,597,887	\$53,597,887	\$137.55	\$2,903.02	0.047
2052	2.4E-02	\$72,195,560	\$72,195,560	\$92.64	\$3,488.94	0.027
2056	1.2E-02	\$97,246,350	\$97,246,350	\$62.39	\$4,193.13	0.015

Above: Bitcoin's security budget over time. Each row refers to a different year. Theoretical max exchange rate from the [Game and Watch paper](#). Imputed exchange rate is historical rates and growth factors, with some manual "blending in" so as to more rapidly approach the theoretical maximum. Defense budget extrapolated from [wikipedia data](#). "Safety Ratio" is the percentage of military budget that would be needed to disable Bitcoin. All numbers are in nominal dollars.

The "indifference" epoch is one where Bitcoin is vulnerable, but few adversaries squander their opportunity to attack because they are not paying attention. The "healthy" epoch is one where BTC should be able to deter 51% attacks even from ultra-wealthy motivated adversaries. But the "decline" epoch shows us a bleak future, in which 51% attacks on Bitcoin are easy again.

3. Transaction Fees

i. The Desired "Fee Pressure"

As is commonly known, *transaction fees* are expected to come to the rescue. As [Greg Maxwell remarked](#):

"fee pressure is an intentional part of the system design and to the best of the current understanding essential for the system's long term survival"

He [later famously wrote](#):

"Personally, I'm pulling out the champaign that market behaviour is indeed producing activity levels that can pay for security without inflation."

This view, (of a needed “fee pressure”), is common. Roger Ver has [compiled similar quotes](#) from other Bitcoin intelligentsia. Roger did this in order to discredit them politically, but the quotes are nonetheless accurate.

ii. The Dual Nature

The **dual nature** of Bitcoin (as both a money-unit, and a payment-rail) has confused people since Bitcoin was first invented.

In general, monetary theorists and economics ignored the payment-rail (and dismissed Bitcoin as supposedly having “no intrinsic value”). Businessmen and bankers ignored the money-unit (and regarded purchases of *BTC* as hopelessly naive), and instead tried hopelessly to rip-off the “blockchain technology”.

The confusion persists today in the “scaling debate”, in the form of a discussion over whether or not the “medium of exchange” use-cases are more valuable than the “store of value” use-cases.

And I think it persists in long-run security budget analysis, as well. Consider the following table:

Revenue Source	Block Subsidy (12.5 BTC)	Transaction Fees
Market's Units	...of BTC	...of block space
Price Units	... \$ (PPP) per BTC	\$ (PPP) per byte
If BTC price = moon...	...SB Goes Up	...SB <i>Unaffected</i>
Meme	Store of Value	Medium of Exchange
Slogan	“Digital Gold”	“P2P Electronic Cash”

While the two are mixed into the same “security budget”, the **block subsidy and txn-fees are utterly and completely different**. They are as different from each other, as “VISA’s total profits in 2017” are from the “total increase in [M2](#) in 2017”.

VISA’s profits are a function of how cost-effectively VISA provides value to its customers, relative to its competitors (MasterCard, ACH, WesternUnion, etc). Changes in M2 are a function of other things entirely, such as: election outcomes, public opinion, business cycles, and FED decisions. There is some sense in which M2 “competes” with the Japanese Yen, but there are really no senses in which it competes with MasterCard.

iii. Are fees truly paid “in BTC”?

Transaction fees are explicitly priced in BTC. But, unlike the block reward, they *do* react to changes in the exchange rate. As the exchange rate rises, a given satoshi/byte fee rate becomes more onerous, and people shy away from paying it.

And so tx-fees are not really “priced in BTC”, despite the protocol’s attempt to mislead us into thinking that they are. They are actually priced in [purchasing power](#), which –these days (pre-hyper-bitcoinization)– is best expressed in US Dollars.

So, it is entirely appropriate [to say](#), for example, that “in Dec 2017, BTC had tx-fees as high as *twenty-eight dollars*”. And it would be inappropriate to say that the tx-fees were “as high as .0015,0000 BTC”. For if the BTC price had been 10x higher², the tx-fees would have only reached .0001,5000 BTC.

iv. Stimulating Production

Whenever prices rise, entrepreneurs are induced to produce. (Owners are also induced to sell, but we are not interested in that right now.)

The supply of BTC is famously capped at 21 million. The *produced* supply (aka the “new” supply) is currently capped at 12.5 BTC per block, until the next halving.

The supply of a completely different good, “btc-block-bytes”, is also capped. It was first (in)famously capped at 1 MB per block, and now is capped at [something-like](#) 2.3 MB per block.

As was just said: whenever blocks become more valuable, entrepreneurs search for ways to produce more of them.

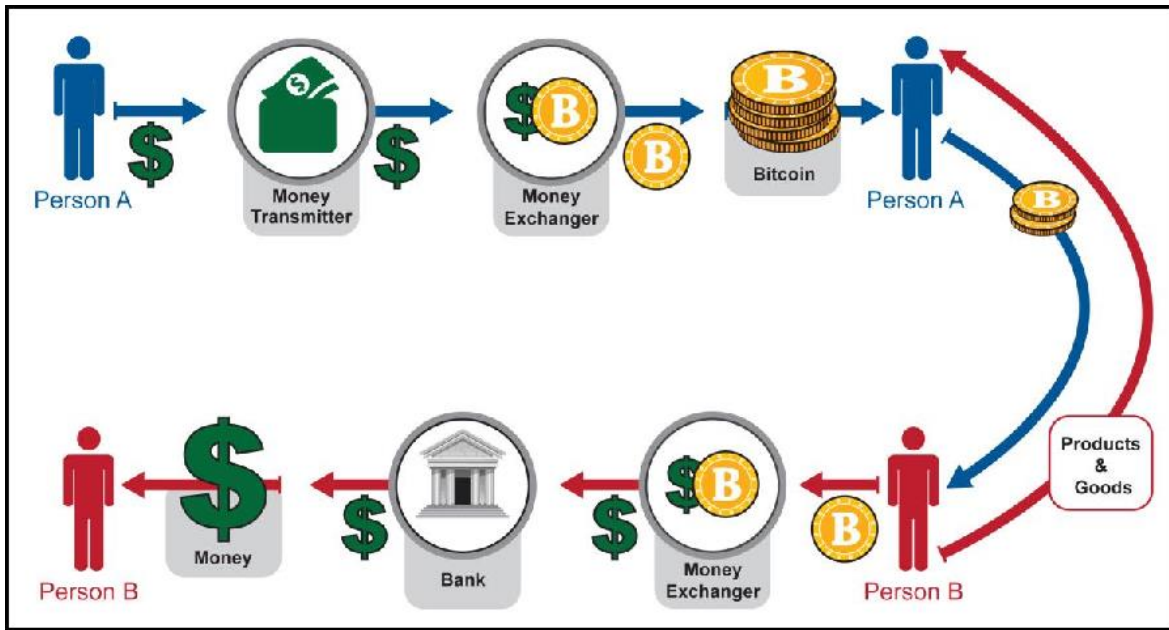
One way is to reactivate older, marginally unprofitable mining hardware. Production then hastens...temporarily. Of course, after the next difficulty adjustment, block-production will return to its equilibrium rate (of 1 block per 10 minutes).

Alternatively, entrepreneurs can create, and mine, Altcoins.

v. Altcoins as Substitute Goods

Alt-“coins” are *very poor* substitutes for Bit-“coins”. Each form of money, is necessarily in competition with all other forms: money has strong network effects; the recognizability property has super-linear returns to scale; exchange rates are transaction frictions that are inconvenient; etc. What people wanted was a BTC. They wanted to *get rid of* all their other forms of money!

But it is the reverse when we consider transaction fees and “btc-block-bytes”: Altcoin-blockspace is a pretty good substitute for Bitcoin-blockspace. Remember that this type of demand has *nothing to do* with obtaining BTC. Users merely wish to buy something using the Bitcoin payment-rail. This image from [2013 FINCEN Congressional testimony](#) hopefully makes it clear:



Since the amount of coin sent in a blockchain payment is always configurable, it will always be possible to send someone “twenty dollars” worth of LTC; or “one BTC” worth of DOGE; or “one sandwich” worth of EOS. All of this is made much easier by the “exchangers” (ie: Coinbase, ShapeShift, SideShift, BitPay, LocalBitcoins, multi-currency wallets, CC ATMs, etc) which now take numerous forms and are easy to use.

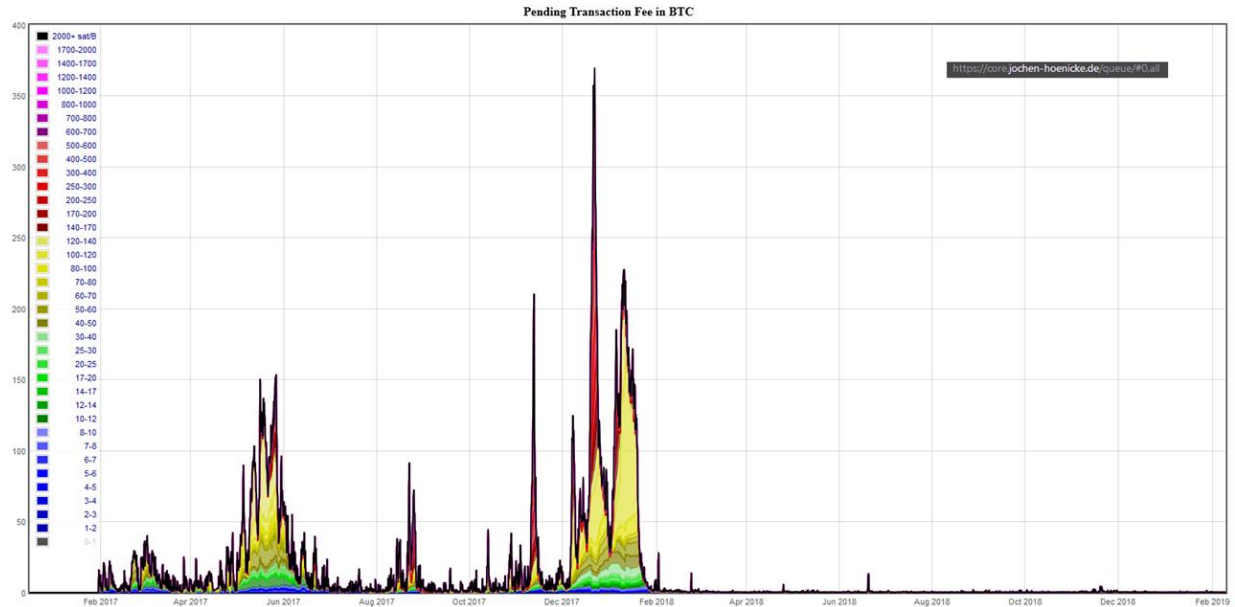
Furthermore, this (true) premise –that Altcoin-payments are indeed substitutes for Bitcoin-payments– is occasionally explicitly admitted³, even by hardcore maximalists. Especially during the last fee run-up in late 2017:

- [Samson Mao](#)
- [Francis Pouliot](#)
- [“The digital currency for payments”](#)

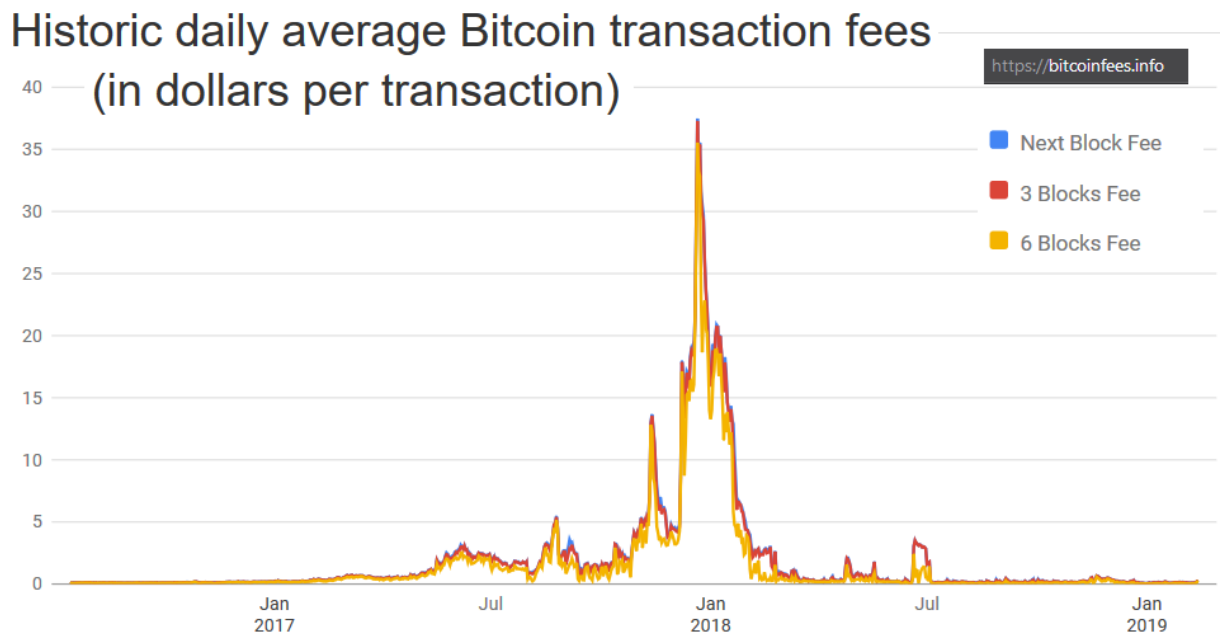
vi. Competitive Demand for the Payment Rail

The supposedly-essential “fee pressure” has, for the moment, deserted us.

See this graph (from [this page](#)) for BTC-priced fees:

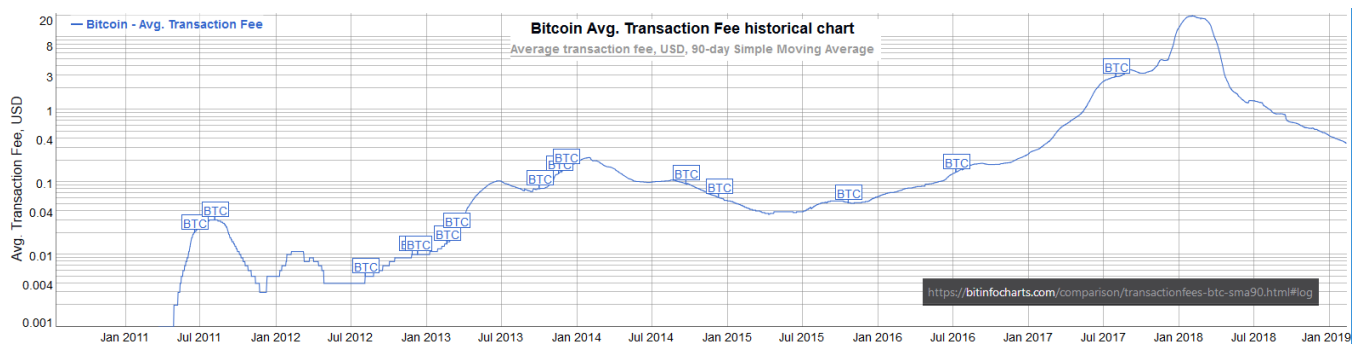


And this graph (from [this page](#)) for USD-priced fees:

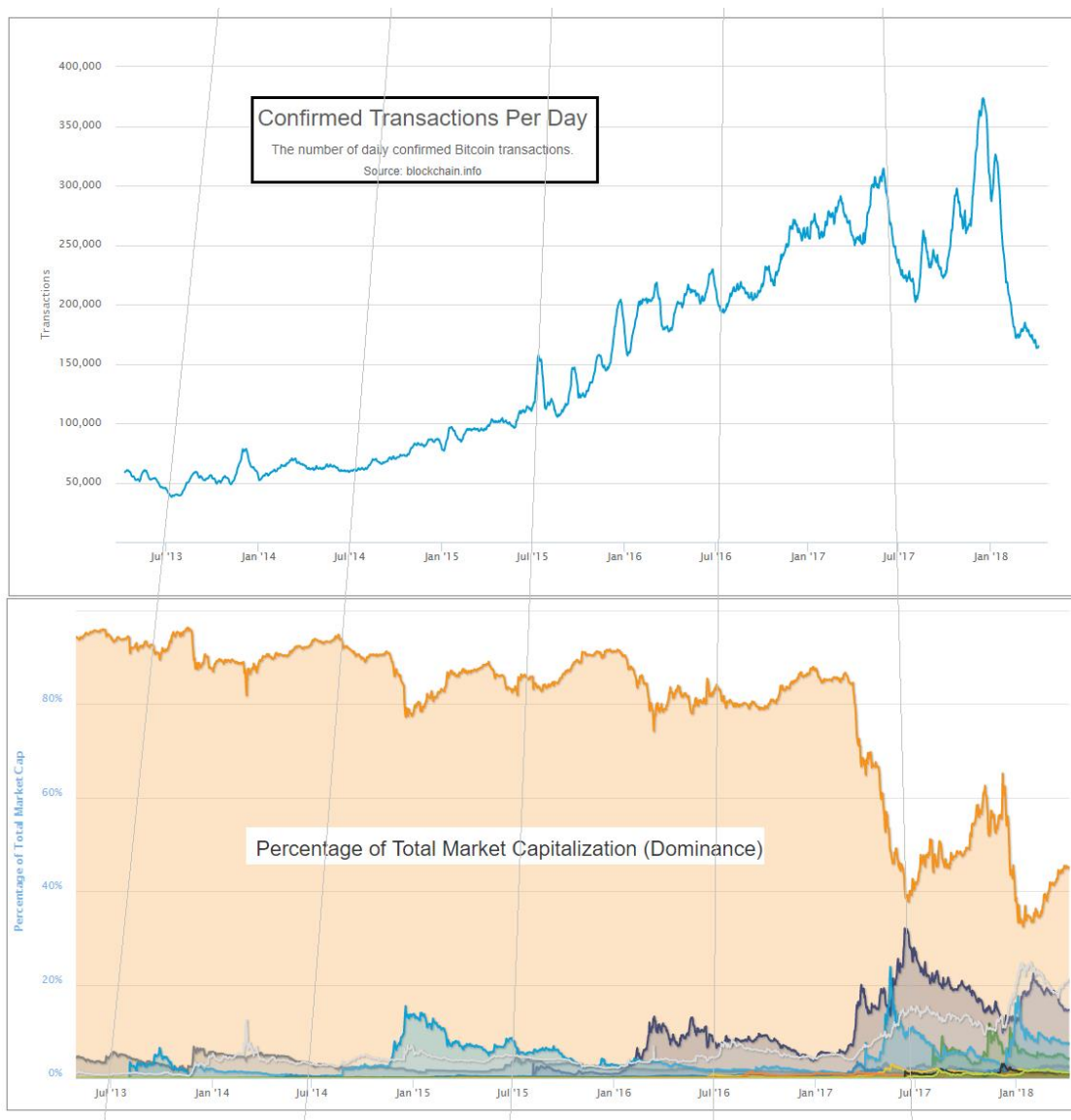


We see that fee pressure has crumbled. Today, [a typical transaction will cost](#) 30-40 cents – much cheaper than a VISA txn.

Compare the [historical data, given in 90-day moving-average...](#)



...to the two graphs below:



We see that BTC's crossing of the "1 USD per transaction line", in May of 2017, coincides with the rise of Altcoins. We also see that the "pressure" of late 2017 quickly

canceled itself out, and then some. Finally, we see that this release-of-pressure coincided with a sudden (and unprecedented) decline in BTC-transactions.

To me, this data refutes the theory that users will pay high BTC fees willingly. In fact, they seem to have only ever paid high fees *unwillingly* – during a brief “bubble” time (of relative panic and FOMO).

If that theory is indeed false, then total fees will not be any higher –in USD terms– than they are today.

According to blockchain.info, fees in the last 12 months totaled \$70 million. (In the 12 months before *that*, they were \$770 million).

Revisit the [chart above](#), and you will see that this barely registers. After all, when \$70 M is priced in the units of the chart (billions), it is just \$0.07.

If the consumer is cost-conscious, and will only pay the lowest tx-fees, then how can we get those numbers up?

vii. Alternative Fee-Sources

a. Lightning Network

The Lightning Network (if successful) will allow very many “real-life transactions” to be fit into just two on-chain txns.

The immediate effect of this, is to *lower* on-chain transaction fees; but the ultimate effect is increase them. LN boosts on-chain fees by increasing the utility of each on-chain txn (by allowing each to do the work of many txns), and by therefore making high on-chain fees more tolerable to the end user.

Exactly how much will LN boost fees?

At this point – it is anyone’s guess. But *my* guess is that they cannot realistically increase by more than two orders of magnitude.

First, on-chain txns are needed to create, and periodically maintain, the LN. So LN-users will still be paying on-chain fees; and will still prefer to minimize these costs. Meanwhile, Altcoins will have their own Lightning Network (they will copy LN, just as they’ve copied everything else). All of these LNs will compete with each other, the same way that different blockchains compete with each other.

Keep in mind, that the fees paid to LN-hubs⁴ will, by definition, *not* be paid to miners. So, there is no sense in which LN-fees “accumulate” into one big on-chain txn-fee (in

contrast to how *the economic effect* of each LN-txn does accumulate into a single net on-chain txn).

Second, the LN user-experience will probably always be worse than the on-chain user-experience. LN is *interactive*, meaning that users must be online, and do something [sign a transaction] in order to receive money. It also means that your LN-counterparties can inconvenience you (for example if they stop replying, or if their computers catch fire) or outright harass you. LN also comes with new risks – the LN-design is very clever at minimizing these risks, but they are still there and will still be annoying to users. Users will prefer not to put up with them. So they will tend to prefer an Altcoin on-chain-txn over a mainchain-LN-txn.

b. Merged Mining Sidechains

Merged-Mined Sidechains do whatever Altcoins can do, but without the need to purchase a new token. So they have infinitely lower exchange rate risk, and are more convenient for users.

On top of that, MM SCs send all txn-fees they collect to Bitcoin miners. Under [Blind Merged Mining](#), they do this without requiring any users or miners to run the sidechain node software.

A set of [largeblock sidechains](#) could process very many transactions. In the next section, I will assume that the total Sidechain Network replaces VISA, (and VISA alone), and captures all of its transaction fee revenues. VISA is only a small percentage of the total payments market (which includes checks, WesternUnion, ApplePay, etc), but it is a good first look.

viii. VISA's Transaction Fee Revenues

Contrary to what I believed just moments before looking this up, VISA does not earn any money off of the interest that it charges its customers.

Observe page 40 of [their most recent annual report](#):

Our operating revenues are primarily generated from payments volume on Visa products for purchased goods and services, as well as the number of transactions processed on our network. We do not earn revenues from, or bear credit risk with respect to, interest or fees paid by account holders on Visa products.

Instead VISA's revenue comes from transaction fees. This perfectly facilitates our comparison.

Total revenues were 18,538 \$M in 2017, up from 11,778 \$M in 2013. This corresponds to quite an annual growth rate – 12% per year.

If we assume that current trends holds, we get the following:

Security Budget over next 40 yrs (assuming VISA-level fee-revenues)								
Year	Subsidy	Exchange Rate	Exchange Rate (market-imputed)	Block Subsidy (billions per year)	VISA Tx-Fee Revenues (billions per year)	Total Security Budget (billions per year)	USA Defense Spending (billions per year)	Safety Ratio
	from protocol	$x_{2017} = 7 = 1.6265$	$x_{2016} = \$700$, growth = 1.6265; blended with maximum	$= \text{Subsidy} * \text{Exchange Rate (m.l.)} * 6 * 24 * 365 * (1/1e9)$	$x_{2017} = 18.538$, growth = 1.120	$\text{sum}(\text{block\_subsidy} + \text{VISA\_fees})$	$x_{2015} = 637$, growth = 1.047	Security B. / Defense B.
2008	50	####	\$0	\$0.00	\$6.68	\$6.68	\$461.76	0.014
2012	25	####	\$100	\$0.13	\$10.52	\$10.65	\$554.95	0.019
2016	12.5	####	\$700	\$0.46	\$16.55	\$17.01	\$666.96	0.026
2020	6.25	####	\$4,900	\$1.61	\$26.05	\$27.66	\$801.57	0.035
2024	3.125	####	\$75,000	\$12.32	\$41.00	\$53.32	\$963.36	0.055
2028	1.5625	####	\$800,000	\$65.70	\$64.53	\$130.23	\$1,157.79	0.112
2032	0.78125	####	\$15,000,000	\$615.94	\$101.57	\$717.51	\$1,391.47	0.516
2036	3.9E-01	####	\$21,931,039	\$450.27	\$159.87	\$610.14	\$1,672.32	0.365
2040	2.0E-01	####	\$29,540,785	\$303.25	\$251.63	\$554.88	\$2,009.85	0.276
2044	9.8E-02	####	\$39,790,999	\$204.24	\$396.05	\$600.29	\$2,415.50	0.249
2048	4.9E-02	####	\$53,597,887	\$137.55	\$623.37	\$760.92	\$2,903.02	0.262
2052	2.4E-02	####	\$72,195,560	\$92.64	\$981.15	\$1,073.80	\$3,488.94	0.308
2056	1.2E-02	####	\$97,246,350	\$62.39	\$1,544.29	\$1,606.68	\$4,193.13	0.383

[Link to Excel sheet.](#)

Above: The ‘security budget table’ from earlier in this post, plus a new column: VISA transaction fees. These fees are added to the base block subsidy amounts, to get a new total security budget.

This security budget *does* seem to be much safer in the long run, and safer in general.

Conclusion

To deter 51% attacks, Bitcoin needs a high “security budget”. Today’s tx-fee revenues are not high enough; we must ensure that they are “boosted” in the future.

Higher prices (ie, higher satoshi/byte fee-rates) are one way of boosting revenue. Unfortunately, competition from rival chains acts to suppress the market-clearing fee-rate.

A better way, is to attempt to devour the entire payments market, and claim all of its fee revenues. This can be done using Merge Mined Sidechains, without any decentralization loss.

Footnotes

2. The math is that $1.077 = (25.94/5.85)^{(1/20)}$. And note that 1.077 is below the required “stasis rate” of 1.19. [↗](#)
3. I mean that if the USD/BTC price had been 10x higher, throughout the “bubble” of late-2017. In other words, if Bitcoin had started Jan 2017 at around 9,000 USD/BTC and then risen to 190,000 USD/BTC. [↗](#)
4. I do remember there being much more of this, but I could only find a few examples (before giving up). Please message me if you can find/remember any other examples. I guess I will eventually remove this paragraph if I never find any more. [↗](#)
5. By “fees paid to LN-hubs”, I mean the fees that you would pay, (off chain), to any Lightning Node that your LN-payment routes through. [↗](#)

Links

- <http://www.truthcoin.info/blog/blockspace-demand/>
- <http://www.drivechain.info/literature/index.html#bob>
- <https://medium.com/coinmonks/bitcoin-security-in-one-chart-694ee3ed8c2d>
- <https://www.blockchain.com/charts/miners-revenue?timespan=2years&daysAverageString=7>
- <https://www.federalreserve.gov/publications/2017-ar-federal-system-budgets.htm>
- <https://coinjournal.net/research-paper-makes-case-5-8-million-bitcoin-price/>
- <http://www.truthcoin.info/blog/security-budget/#fn:1>
- https://en.wikipedia.org/wiki/Military_budget_of_the_United_States
- <https://web.archive.org/web/20171207201015/https://botbot.me/freenode/bitcoin-wizards/2016-01-17/?msg=58099943&page=1>
- <https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2017-December/015455.html>
- <https://www.docdroid.net/NG1sbVq/pantera-march-2017.pdf>
- <https://www.investopedia.com/terms/m/m2.asp>
- <http://www.truthcoin.info/images/true-money/>
- <https://www.cnn.com/2017/12/19/big-transactions-fees-are-a-problem-for-bitcoin.html>
- <http://www.truthcoin.info/blog/security-budget/#fn:2>
- https://en.bitcoinwiki.org/wiki/Block_weight#Conversion_to_real_sizes
- <https://www.fincen.gov/news/testimony/statement-jennifer-shasky-calvery-director-financial-crimes-enforcement-network-0>
- <http://www.truthcoin.info/blog/security-budget/#fn:3>
- <https://twitter.com/Excellion/status/926908067521761280>

- <https://twitter.com/mikeinspace/status/1078546356476628992>
- <https://litecoin-foundation.org/product/understanding-litecoin-the-digital-currency-for-payments/>
- <https://core.jochen-hoenicke.de/queue/#0,all>
- <https://bitcoinfees.info/>
- <https://www.buybitcoinworldwide.com/fee-calculator/>
- <https://bitinfocharts.com/comparison/transactionfees-btc-sma90.html#log>
- <https://www.blockchain.com/charts/transaction-fees-usd?timespan=2years>
- <http://www.truthcoin.info/blog/security-budget/www.truthcoin.info/blog/security-budget#2-the-block-subsidy>
- <http://www.truthcoin.info/blog/security-budget/#fn:n>
- <http://www.truthcoin.info/blog/blind-merged-mining/>
- <http://www.truthcoin.info/blog/gigachain/>
- http://www.annualreports.com/HostedData/AnnualReports/PDF/NYSE_V_2017.pdf
- <http://www.truthcoin.info/images/long-run-security-budget.xlsx>

Why Crypto is the Future and How it is Essential to us All

By [Chris Herd](#)

Posted February 13, 2019

What people fail to realize when correlating crypto prices with Fiat is that there is far less certainty in government-controlled currency than you imagine.

Since USD value was divorced from the Gold standard by Nixon in 1971, because of his perception of the weakening of the Dollar in comparison to companies that were not tied to the price of gold, its underpinning is less certain. People often imagine that the value of money is tied to a physical commodity but this is no longer true.

Money might not quite be the intellectual construct that Cryptocurrency is, but it is careless and irresponsible to assume it is any less dependent on the faith of the people for its value to remain.

People imagine that because a government stands behind it that there is more control or safety measures—and there obviously are—but the distance between the two is closer than you would initially think. The overall value of fiat is contingent on the whims, fluctuations, and successes of a country. Supply can be manipulated through arbitrary decisions by a central bank who can print money as monetary policy significantly affecting inflation

Effectively what this means is that a government can unilaterally decide to devalue everything in a country overnight. Think of quantitative easing as a stock split where instead of receiving two for one, the government splits your stock and keeps half.

That is what effectively occurred following the 2008 financial collapse and there was nothing to stop it or nothing we could do about it. The argument that it prevented deeper financial issues was irrelevant to normal people—they didn't cause the problem! They might have been dependent on the pensions accrued from the companies that were failing but their blame started and finished with the rules and practices of the banking profession.

Crypto began its rise to prominence at a similar time, coincidence?

I don't think so. Crypto is controlled by a decentralized, distributed network of users who exert equal control. Progress is controlled by consensus—that is a key innovation. There aren't elected representative that make decisions on our behalf, we row our own boat.

Today's pronouncement that the dollar won't be affected by the volatility of Crypto is true. The dollar doesn't depend on it. Crypto, on the other hand, thrives in the face of government corruption or idiocy. That is where it's grown from. Crypto offers an alternative to faith in those who have not acted in our collective interest. Looking at what is happening in Venezuela—where government eradicates equitable financial access—individuals can voluntarily opt out!

Citizens control their fate in a world where an alternative exists.

Prior to Bitcoin, there was no alternative. You could purchase stocks but where was the liquidity? Same with physical goods or livestock. Individuals require their money quickly, but the hyperinflation in the country meant they could not keep their earning in the national currency.

Crypto enables individual fiduciary responsibility for yourself

It breaks your reliance on the government you inherit in your local geographic location. It democratizes your ability to persist and subsist. That is why Crypto is important. Current prices might well be a bubble—most likely they are. But the bursting of the .com bubble didn't kill the internet, it gave birth to perhaps the greatest period of consumer innovation in history!

And Cryptocurrency and blockchain will do the same.

Bitcoin might be Pets.com, Ethereum might be MySpace, but Facebooks, Amazons, Googles and Apples of this space will emerge—probably from a dorm room in China.

And that is what needs to be understood. This is a nascent industry, of which the use case isn't entirely clear. But every major technological innovation experiences this stage. There's an initial burst, a short and a long boom

The boom is characterized by a maturing of technology through an understanding of capability—we are nowhere near this yet. Use cases are still being explored—look at Cryptocats—and there will be significant failures encountered along the way

Speculators will most likely lose their coat, just look at what has happened to BitConnect today, but the use case for Cryptocurrency is just beginning to be explored.

Web 1.0 gave rise to internet

Web 2.0 gave rise to the giants who dominate it

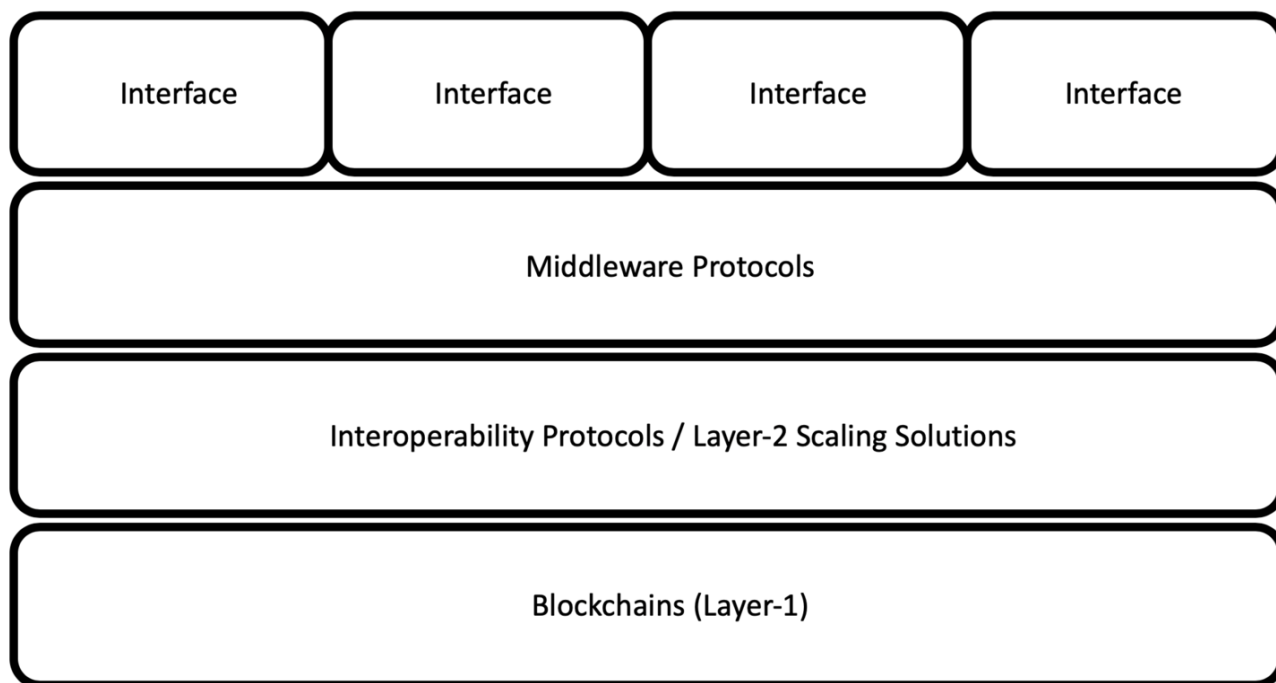
Web 3.0 will give rise to distributed networks that take it back

The Defensibility of Middleware Protocols

By [Chris Burniske](#)

Posted February 14, 2019

Interoperability of state and value is likely to place downward price pressure on layer-1 blockchains that have no monetary premium, while enabling strong [middleware protocols](#) to achieve cross-chain, winner-takes-most dominance in their respective services. While not a perfect mapping to traditional use of the term *middleware*, these protocols can be thought of as anything sitting just below the interface layer (i.e., the applications the end user interacts with), but leveraging the lower-level functionality provided by layer-1 blockchains and interoperability protocols.



Others have called these service-layer protocols, as they focus on providing a specific service to the interface layer, be they financial, social, technological, etc. Financial services include things like exchange, lending, and risk-management; social services offer functionality like voting structures, arbitration, or legal-contract management; technological services include components like caching, storage, location, and maybe the granddaddy of them all, a unified OS for protocol services to be neatly bundled to the interface layer.

Financial-service protocols that [Placeholder has invested in](#) include Ox, Erasure, MakerDAO, and UMA, while Aragon is our main social-service protocol to date, and

technological-service protocols that we work with include CacheCash, Filecoin, FOAM, and Zeppelin. All of these protocols have originated on Ethereum, but we believe interoperability of state and value—the promise of a Cosmos, Polkadot, and Ethereum 2.0 future—will allow these protocols to become horizontally defensible starting from Ethereum’s base.

Take MakerDAO, for example. Its token, MKR, [can be thought of as an insurance pool for secured loans](#) originated through the platform. The larger the overall value of MKR, the greater the insurance and therefore lower the risk for all users of the system. Let’s say FakerDAO pops up on Tron, providing the exact same service, but with its own native governance asset, FKR. Right now, it would be hard for the Maker team to leverage the value in MKR to secure a parallel system on Tron, but with interoperability of state and value it would become considerably easier.

Assuming the Maker team can build out for Tron before FKR gets to a similar value as MKR, then they should be able to deploy on Tron and provide a lower risk service than FakerDAO can, insured by the much larger pool of value stored in MKR. With two communities driving utility through MakerDAO, MKR’s pooled value is then likely to significantly outpace FKR’s, further widening the risk and quality of service-gap (Whether MKR holders would want to underwrite the risk of operating on another chain like Tron is a separate question).

We believe similar dynamics will play out for many other middleware protocols, though in different ways depending on the cryptoeconomic [1] and governance design of the system. Protocols whose reliability, security, speed, liquidity, or coverage scales with the size of the asset base and nodes supporting it, stand to do well in an interoperable world.

Footnotes:

[1] Most middleware protocols are likely to employ some variant of a capital asset as their cryptoeconomic model, where supply-siders must stake the asset to provide the service, giving them access to value-flows for so doing.

Sidenote: After viewing what we hold, some have asked why ether isn’t included. While we are fans of the Ethereum team, and think that people underestimate the soft-network effects of the system, we don’t hold ether (or any layer-1 smart contract blockchain) in part for the above reasons. We believe the middleware protocols we’ve invested in give us upside exposure to ether (if ETH appreciates in fiat terms then the *quality* assets that ride atop it tend to also appreciate in fiat terms, holding their value relative to ETH), while also protecting us from the downside exposure should more dominant layer-1 smart contract blockchains, or interoperability protocols, start to steal from ether’s value.

Links

- <https://twitter.com/cburniske/status/1022140822165352448>
- <https://www.placeholder.vc/about>
- <https://www.placeholder.vc/blog/2019/1/23/maker-investment-thesis>

Bitcoin Delta Capitalization

A New View of BTC Long-Term Valuation

By [David Puell](#)

Posted on February 14

Disclaimer: Nothing contained in this article should be considered as investment or trading advice.

As a follow-up to [Willy Woo's](#) recently-introduced [Bitcoin Valuations live chart](#), this article aims to present delta cap with the goal of answering two of the most pressing questions in speculators' minds at the present moment:

Where is the bottom?

When is the next bull run coming along?

Something's Amiss

Two sets of items originated the search for what later became delta cap:

[Awe and Wonder's studies on Bitcoin's logarithmic regression](#) and [Plan B's studies on Bitcoin's power regression](#) (R^2 of 0.93 and 0.95 respectively), which seem to suggest that the BTC trend is increasing at a decreasing rate.

[Murad Mahmudov's exploration of historical moving averages](#), expressing a dissatisfaction with any particular SMA or EMA as definitive enough to "catch the bottom" in every bear cycle.

This initiated the search for a metric that both adapted to Bitcoin's rapid, high-velocity parabolic moves and accounted for its overall trend decay over time. Two other valuation models seemed to provide a tentative answer: realized cap for the former and average cap for the latter.

Delta Capitalization

Delta cap is, as seen next, a hybrid of sorts—half "fundamental," half "technical." It is calculated through the following formula, measuring the difference between two long-term Bitcoin moving averages:

$$\textit{DeltaCap} = \textit{RealizedCap} - \textit{AverageCap}$$

For the purposes of this piece, let's review these definitions:

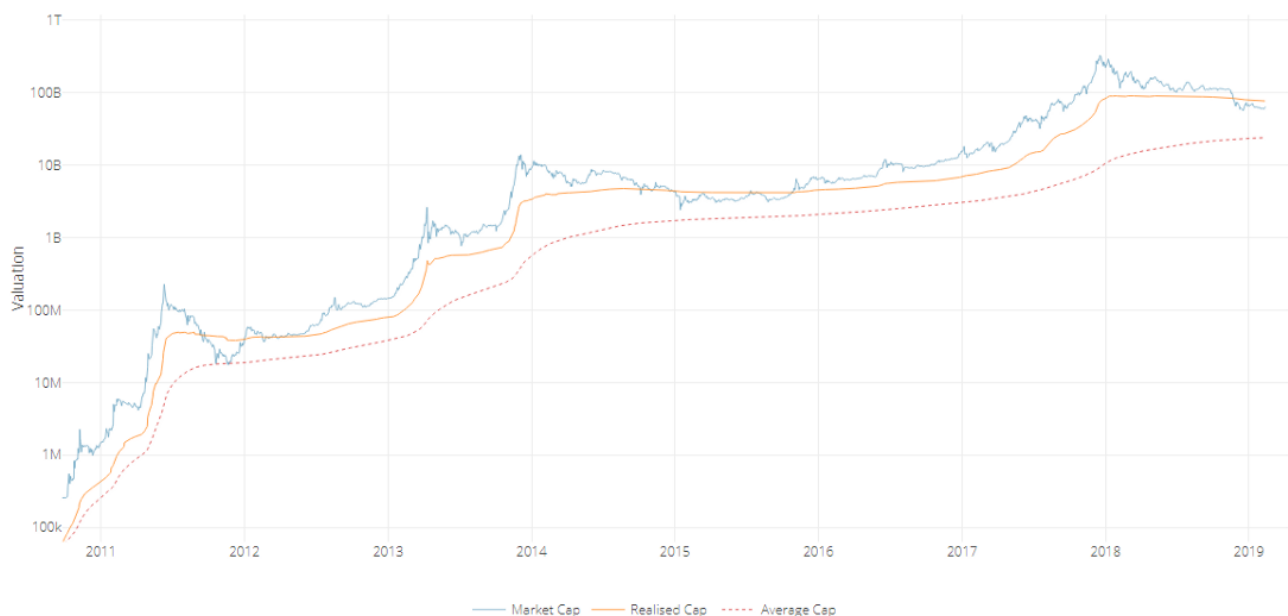
Realized capitalization

[Invented and presented by the brilliant team at Coinmetrics](#), instead of counting all of the mined coins at current price, the coins are counted at the price when they last moved through the blockchain. This approximates the USD value paid for all the bitcoins in circulation. Best put by its co-creator [Nic Carter](#), it can be described as an on-chain volume-weighted average price (VWAP) of BTC.

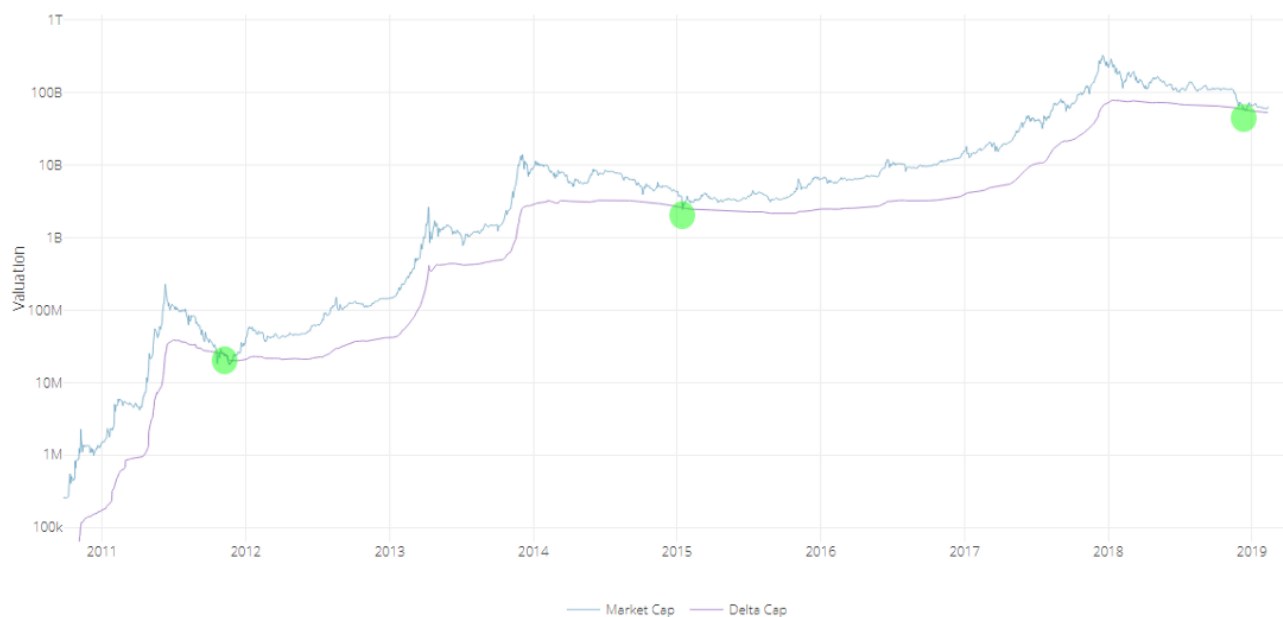
Average capitalization

Instead of setting a fixed period for calculating a moving average (e.g., a 200-day MA), this is a life-to-date, cumulative simple moving average that serves as the true mean of the whole history of market cap. Due to its “laggy” nature, it is the perfect mechanism to help decay the upward speed of delta cap over time. Shoutout to [Renato Shirakashi](#) for first pointing out this average.

Below, a view of both lines, courtesy of Willy Woo:



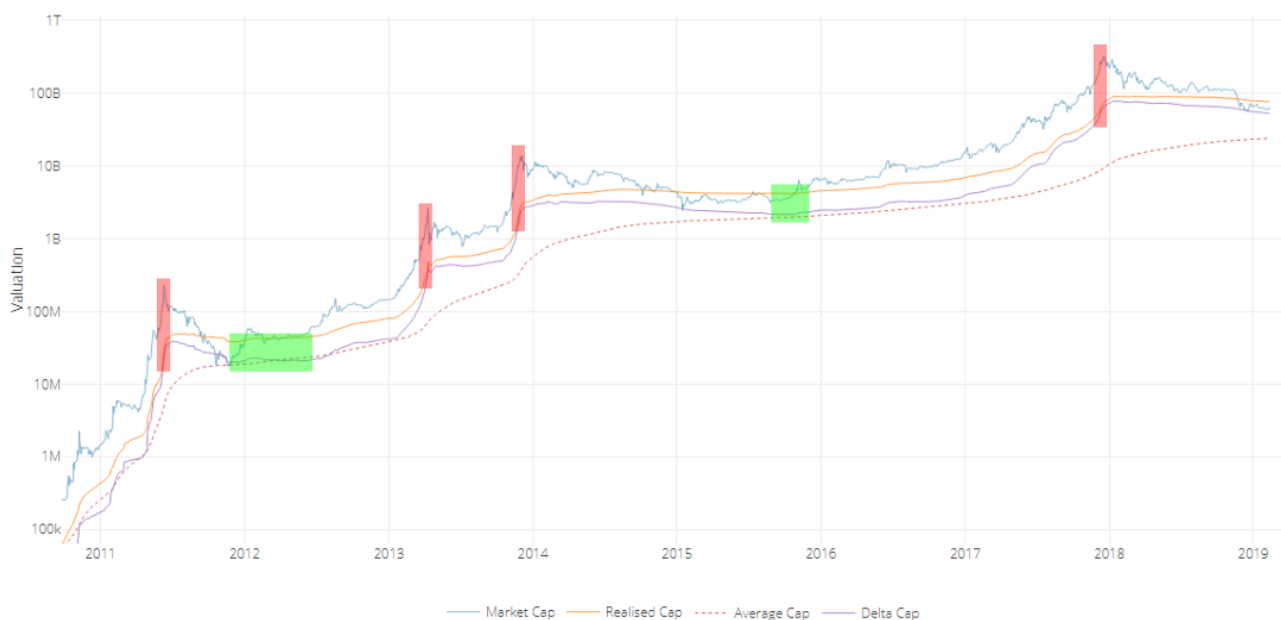
The aforementioned subtraction of the two in turn provides the following delta cap line, both reactive locally and decaying globally:



As seen at first glance, delta cap provides an excellent framework for catching global bottoms—or at the very least bottoms near the floor of the bear cycle. Please see the caveats of this indicator below to have a more nuanced view of the current state of affairs, since *having just touched delta cap does not guarantee that we have bottomed*.

Time Analysis

Another interesting (and still experimental) exploration of delta cap emerges when comparing it to its parent inputs through a logarithmic view, as follows:



We can easily gauge periods where delta approaches realized cap during the bubble tops, and then evermore slowly descends to almost touching the average cap during the phases of breakout price behavior, signaling the inauguration of the new bull run.

The good news? If this pattern continues, people will have lots of time to buy up. The bad news? This bear-to-sideways market may last for an unprecedented while, going as far as projecting a post-accumulation breakout as late as Q2, 2020—the moment when it could be expected for delta cap to get nearest to average cap if the extension of these lines continues as-is. Bear in mind that this is all pending on the overall rate of drop of realized cap and the rate of rise of average cap—local price action, velocity, and dormancy are all in play. Time domain here is still a broad estimate.

It goes without saying that we lack enough bottom samples to claim this as a certainty, but long-term investors must stay mentally prepared for this possible delay. It is further evidence that suggests Bitcoin's cycles are elongating.

Yes, Another Ratio: MVDV

Since most will be curious about how the Market-Value-to-Delta-Value (MVDV) Ratio looks like, here it goes:



A few notes on it:

Just as seen on [MVRV Ratio](#) and the [Mayer Multiple](#), MVDV seems to indicate that each of Bitcoin's blow-off tops is losing momentum. This is not necessarily bearish, as I believe it merely implies that each bubble is becoming less exuberant and getting closer to the mean.

Major bearish divergences seem to announce global tops (red circles) while differentiating them from previous local tops of the same cycle.

The bottoms seem to maintain a steadier horizontal longitudinal threshold at 1 (green line). If market cap were to revisit delta cap today at a lower low, the oscillator would present this event as a double bottom.

Caveats

Having touched delta cap recently does not imply a global bottom: One must remember that delta cap is currently sloping down—and it will continue to do so for several months—so the likelihood of market cap revisiting it is not out of the question. Add to that the fact that the NVT tools are still just slowly trending into normal historical conditions and velocity remains weak. Touching delta cap on a lower low in the following months is still a likely possibility. Every penetration of market cap into delta cap should be best used as one component of an averaging-in strategy over a prolonged period of time.

Despite timeboxed halving days, the Bitcoin cycle seems to be elongating: This makes perfect sense, since larger bull runs require larger liquidity. The experiment here is to continue evaluating delta cap as a mean that keeps adjusting to Bitcoin's

curved trend. That being said, the time analysis section of this article remains highly speculative, especially for signaling the breakout events, so let's take it one day at a time.

The market currently holds a major dissonance: That of delta cap providing a good “baseline” for a relatively optimistic market floor, versus the current state of velocity as seen on [NVT Ratio](#), [Network Momentum](#), and [NVT Caps](#)— on life support relative to price.

Delta cap remains experimental: Just as with most technical and on-chain tools, these indicators should be used with prudence and in the company of other trading mechanisms and a sound risk management strategy. Past events don't reflect future outcomes.

Acknowledgements

Many thanks to the following individuals:

[Willy Woo](#), for the beautiful charts and valuable feedback.

[Murad Mahmudov](#), [Phil Bonello](#), [Hans Hauge](#), [PositiveCrypto](#), and [Plan B](#), whose comments helped perfect this article.

Sources

[Woobull.com](#): Charts and early market cap data archeology.

[Coinmetrics.io](#): Realized cap data.

[Blockchain.com](#): Market cap data.

Author

[David Puell](#), Partner and Head of Research @ [Adaptive Capital](#)

Links

- https://medium.com/@kenoshaking?source=post_header_lockup
- <https://medium.com/@kenoshaking>
- <https://twitter.com/woonomic>
- <https://twitter.com/woonomic/status/1096103959897489413>
- https://twitter.com/Awe_andWonder/status/1053408719063707648
- <https://twitter.com/100trillionUSD/status/1092771532231897088>
- <https://twitter.com/MustStopMurad/status/1090762552102084614>
- <https://coinmetrics.io/realized-capitalization/>
- https://twitter.com/nic_carter

- https://twitter.com/renato_shira
- <http://charts.woobull.com/bitcoin-mvrv-ratio/>
- <http://charts.woobull.com/bitcoin-mayer-multiple/>
- <http://charts.woobull.com/bitcoin-nvt-ratio/>
- <http://charts.woobull.com/bitcoin-network-momentum/>
- <http://charts.woobull.com/bitcoin-valuations/>
- <https://twitter.com/MustStopMurad>
- <https://twitter.com/PhilJBonello>
- <https://twitter.com/hansthered>
- <https://twitter.com/PositiveCrypto>
- <https://twitter.com/100trillionUSD>
- <http://charts.woobull.com/>
- <https://coinmetrics.io/charts/>
- <https://www.blockchain.com/en/charts/>
- <https://twitter.com/kenoshaking>
- <mailto:info@adaptivecapital.co>

Rehypothecation: BTC's path to becoming king of collateral

By [Patrick Dugan](#)

Poster February 15, 2019

Quick Take

- Concerns about rehypothecation in layer 2 protocols for Bitcoin are overblown, we just need to accurately price its risk premiums
- In the default model of the Lightning Network, lots of BTC is needed in a fully-collateralized fashion to facilitate payments, earning a low yield from routing fees of generally under 1% per annum
- There's a strong argument to be made that historically, when people were allowed to create currency, e.g. credit instruments, to facilitate trade, prosperity rose
- Power money that is more scarce in supply becomes useful as a market referent and collateral base when it has the lowest perceived counterparty risk on the planet
- The path to BTC becoming king of collateral will require forms of rehypothecation

Concerns about rehypothecation in layer 2 protocols for Bitcoin are [overblown](#). We don't need to fear rehypothecation, we just need to accurately price its risk premiums. There's inflationary and deflationary forms of derivative open interest. The deflationary version comes in the form of fully-backed synthetic cash positions, which fuels Bitcoin Dollarization and gives a sensible valuation-growth model for Bitcoin. To understand these nuances, we have to understand bank credit.

If your collateral is so good, why not use it like any other collateral?

What is fiat? Fiat is a b-side currency note, a form of immediate-term debt, it's an asset, but only because of its legal connection to the amortization of debts. It is an anti-liability, but mathematically, by the transitive property – that's an asset!

To restore some sanity, we call these “financial assets”, derivatives are also financial assets, that's why you can be short them. For every \$1 in someone's pocket, which they are “long”, the Central Bank or Commercial Banks are short \$1.

A real asset would be, for example, some Caterpillar machinery purchased with a secured loan. To buy real assets, people accept shorting units of fiat that they borrow, then spend. You get this phenomenon of “fiat” – let it be – the “creation” of new money in the form of credit. The difference between a licensed bank, and a pool of

investors funding loans on LendingClub with full capital paid, or a bond investor, is that the bank has essentially a portfolio margin license from the government. You don't have to fund loans with cash, you can fund them with credit. Your bank's credit. Also, the checking account deposits everyone depends on to survive are a junior, most-subordinated liability of the bank — thanks for looking out for us.

In essence, a lender is making a hypothesis that the borrower will pay them back. In the hypothetical scenario of a default, XYZ can be triggered (e.g. going and taking assets to settle the loan). So to hypothecate something, you just have to lend it.

To rehypothecate something then, you just... lend it again! Currency units issued by a bank as consideration for a new debt note, which may cycle back to that same bank and generally these days the value stays in the banking system, and around and around it goes. One man's leveraged capex is another man's revenue is another bank account's deposit. You get the money multiplier effect.

People who are Pro-Bitcoin generally hate the Federal Reserve, inflation, and fractional reserve banking. This is because many of us came of age at a time where all of these institutions were called into question, amidst great cataclysm unleashed through corruption of the highest halls of capitalism, and also we saw this movie called *Zeitgeist* and watched Ron Paul run for president. We read Baby Boomers' rants about gold manipulation on ZeroHedge, and then we found BTC. Murray Rothbard, Hayek, and the general school of Austrian economics figured in, but people who consider themselves a priori, categorically, it's gotta be Austrian, Austrians, are not necessarily representative of the majority of Pro-Bitcoin people.

Rehypothecation can fuel Lightning

In the default model of the Lightning Network, lots of BTC is needed in a fully-collateralized fashion to facilitate payments, earning a low yield from routing fees of generally under 1 percent per annum (what Nik Bhatia calls the "Lightning Network Reference Rate"). The presumption here, was that LN is necessarily going to be used in that way, that BTC would necessarily dominate liquidity in an environment of cross-chain asset swaps, and that nobody would use BTC/LN in a way that would contravene these Austrian economics tenants of strictly deflationary currency — which by the way, aren't strictly speaking representative of pre-Bitcoin Austrian economics, perhaps better described as Quebecois Economics, after its two most prolific proponents, Francis Pouliot and Pierre Rochard. Much respect.

However, one of the greatest things about Bitcoin is that nobody can censor usage of it. The only thing you can do to discourage certain kinds of usage is, either get mass consensus for a soft fork, changing around parameters that make it more difficult to

relay “spam”, or have it be generally uneconomical. But if it’s economical, enough clients will relay it, and a single block-winning miner will include it, it can get in. Lightning Network is also a client-agnostic network in the sense that it has no global consensus state or specific blockchain. So it reasons, LN clients that run a bit differently could be pretty amazing for getting yield on BTC. For those who know what they are doing, there’s nothing that can be done to stop that, and it will have some degree of synthetic dilutive effect on BTC in the Lightning Network.

Rehypothecation of BTC across Lightning Nodes, creating some sort of money multiplier, is possible if channels are constructed that operate based on un-collateralized trades. Finance has given us solid math describing the adequate pricing, at least to the extent that major bank trading desks are able to stay in business, for trades both involving collateral and without. For those without, they price a sort of Credit-Default-Swap-like option premium, called a Counterparty Value Adjustment, in order to compensate the optionality of having some time window to deliver on a trade.

In the context of Lightning Network HTLC-like trades with a time-based escrow, someone can underwrite those failures to deliver as an income business, in a manner similar to a bail bondsman; think of it as collating the default risk of all those option-writes into a big secured loan that aggregates however many writes a party wishes to make. Those writes come with risk of default, but if there are recoverability mechanisms with a high efficacy rate, the business can end up looking like covered writes rather than risky, uncovered writes, and the premiums can get pretty cheap. Instead of stacking lots of BTC for a low yield, smaller sums of BTC can underwrite throughput for a higher yield and slightly higher risk, making loose trading more cost effective. Cheaper premiums allow people to trade up a storm, which creates derivatives of open interest (basically rehypothecated BTC). Time horizon is a major limiter to how much this sort of synthetic inflation can actually scale.

Bakkt to the future

With Baakt, they start with a 1 Day contract, the community doesn’t cry fowl, they bridge the old money to the new, fees akimbo, great. That open interest is unlikely to become substantially larger than their daily volume, more likely the open interest will be a fraction of daily volume. They then position themselves to the retail public as anti-rehypothecation, but most likely with success on the 1 Day they’ll consider quarterlies and monthlies, and we’d quickly see open interest expansion. However, there are many spread positions in derivatives. Calendar spreads are an example, people trying to milk out a living at the edge of market efficiency, that expansion of open interest is inflationary to some extent and is rehypothecation-like, but it’s still healthy for market liquidity. What we’d like to see is the equivalent of the CME’s

Commitment of Traders report for bitcoin derivatives, breaking down hedgers vs. speculators, and ideally, to separate the inflationary OI from the deflationary.

A loan default is deflationary. The money goes out of existence, it's balanced, and it's why the Fed has done okay manipulating interest rates for the last 40 years. Derivatives portfolios are similarly limited. For swaps and futures open interest, scarcity in the cash-collateral is needed to capture the "risk-free" return of swap payments or futures premium; this creates demand in spot markets, soaks up supply, and puts BTC to work as collateral on higher time horizons.

But if Baakt, or even enterprising traders, are willing to adapt the horizon of Wall St. derivatives practice to loosening the margin requirements of Lightning-type DEX environments, we could end up with a situation where 1 BTC in margin can be used to portfolio-margin a lot of spreads in CVA options vs. BTC settled options that reference some price. We could then have those under-writers hedge by using graph default swaps, the equivalent of Credit Default Swaps but for sets of networked counterparties. These GDS price the risk of different sets of channels operating by different margin rules, and perhaps also with detectable capitalization levels that indicate greater risk, it will be possible to trade these GDS instruments effectively in dynamic, data-informed strategies.

Imagine a CDS on BitMex's contracts: the CDS pays you whatever percent of open interest is experienced as a shortfall on BitMex due to margin calls that are unfilled by a fast-moving market. BitMex has an insurance fund and a lot of revenue to replenish it, but let's say it didn't, such a CDS might be relevant to some traders, and provide a seemingly "free money" yield to those willing to take the other side. Now imagine the same for a decentralized BitMex based on LN. The nuanced degree of how much a contract shortfall can amount to makes these GDS potentially much more efficient to trade than traditional CDS, which deal in tail risks, usually involving extreme binary events. Sometimes corporates go bankrupt and semi-senior notes recover at some rate, or sovereigns default and try to force a restructure, but the percentages involved are usually greater than 50 percent of face value, rather than the 2-25 percent range that a volatility-stricken decentralized contract might suffer margin short-falls.

There are two strong attractors: the higher time-value based return of deploying BTC in the LN to channels operating along CVA-type margining, and the demand for leverage which keeps those premiums enticing. It's a bilateral way of doing leverage in the Lightning Network between chains, in the form of options, which could complement more "traditional" perpetual swaps (less than three years old, BitMex launched XBTUSD perpetual swap in April 2016) that settle on LN just in BTC or LTC. **All these forms of leverage create, temporarily, and against risk, some inflation in the trade-able supply of these coins. That's just a fact of life.**

Gold as an analog only goes so far

If we look at what happened to the gold market, prior to China's buy-out plans, the lending of gold allowed banks to lend more gold on-paper than they had sitting in a vault. Gold banking, in other words. Before anyone turned in their tallysticks to buy shares in the Bank of England, gold receipt issuance was a source of fiat inflation. In the London/New York gold market structure, both spot and derivatives markets were saturated with multipliers. These were not transparent systems, LN counterparties are probably much more auditable. It's arguable that 200x open interest to warehouse inventory ratios, or having less detectable dilution of supply through rehypothecation of gold was bad for the gold market, and made some ideological investors pretty upset. But let me ask you: if your collateral is so good, why should it not be utilized like any other collateral? **The main issuing is one of auditing transparency so that extreme financial practices don't create moral hazards, systemic risks and information asymmetry.**

There's a strong argument to be made that historically, when people were allowed to create currency, e.g. credit instruments, to facilitate trade, prosperity rose. See the late Stephen Belgin and Bernard Lietaer's book *New Money For A New World* for more color on that. It's probably not so simple as, fixed supply good, expanding supply bad. Elastic supply that is intelligently allocated, not by a single intelligent planner but by many people lending, trading, working, building and so forth in the economy, based on value production, not political graft, that is what seems to make a currency most dynamic and valuable. See also Niall Ferguson's chapters in *The Ascent of Money* regarding the fortunes of the gold-hungry Spanish vs. the debt-happy Italians, it's like night and day.

Power money that is more scarce in supply becomes useful as a market referent and collateral base that has the lowest perceived counterparty risk on the planet, which then evolves a complementary market mechanism. As with interest rates, a balance is achieved through price discovery, between inflation and deflation.

Bitcoin is valuable because it serves a purpose in that market mechanism, but with the added hyperfungibility of information; it's globally transversable, melting capital controls like the invisible, imaginary boundaries they are. So it's got an uptrend. It's got time value as collateral. It's got other derivative time-value returns that can be obtained at times, by using it to hedge, shorting those derivatives. These things have so far reinforced each other, with other key metrics like the thickness of Bitcoin's mining moat being positively correlated.

King of collateral

This is how BTC becomes king collateral for the world:

1. Lightning Network Swap Dex's
2. Inter-chain Counterparty Value Adjustment Options Exchanges
3. Reinsurance-like market for Graph Default Swaps that create side-bets, mostly for hedging purposes we assume, on the credit risk of different galaxies of the LN.
4. Now with the ability to have yielding synthetic cash, leveraged bets, options markets, the works, and leading the way in new derivatives frontiers that attract the brightest quantitative traders to seek fortunes in a new wild west of risk hedging, we finally show the legacy financial system what a parallel, independent, systemic risk-quantified financial system can look like.

Whereas banks currently employ quants crunching simulations of graph triangle-counters to try and process nettings of various derivatives counterparties (we're talking about hundreds of thousands of big to medium sized bank counterparties), we can do this on the scale of hundreds of thousands of LN nodes. The utility in UXTO money is increased significantly.

In conclusion, I think the fear of rehypothecation may be overstated, but it's indeed possible, and BTC scalability will depend on the influence of fiat-liquidity into the system, seeking a USD-benchmarked return, which will to some extent dilute supply through leverage. But on the other hand, safe-returns-seeking capital will tend to do the opposite, put on a 1:1 fully collateralized position, and ride it for the USD interest rate, which is very bullish for the supply and demand dynamics of any commodity money that becomes a popular synthetic-USD base.

I think most likely, the most extreme leverage, with the most survivability, will be with the most professional risk managers who can crunch the math on these derivatives and start making markets. Maybe not the 90 percent quoting-time market makers, but those who take smart views to trade mis-priced hedges, who take a market view, who lean into LN constellations with the best margin rules, or who exploit convexity between different instruments.

And that means most of the leverage dilution in imminent supply will be a boon to liquidity, and the sort of leverage that gets people rekt will remain a modest component of overall supply and demand. This will make Lightning many times more capital efficient, maybe not 10x like the typical fractional reserve banking money multiplier, but enough to create convex liquidity aggregation benefits in the LN in general.

Nik Bhatia's counterparty risk spectrum fits into this. He cited cold storage as near-zero counterparty risk (there's still operational risk of physical attack vectors and the credit risk of the underlying blockchain, small though it may be) and the average optimized return for routing fees a bit further up that scale, because you have to be

in a live hot wallet perpetually to operate for that revenue. Then, off-chain lending was this example of a riskier thing yet, which veers into the realm of counterparty risk. But HTLCs used for margining general derivative contracts with BTC also come with counterparty risk that must be priced to make HTLC's incentive-aligned enough that those trading mechanisms actually work. We're probably going to need to evaluate Schnorr-based discrete log contracts or some modification on the HTLC-based cross-chain atomic swap model, such that one party clearly holds the option, and the other party is short it. Having either side be equally able to jerk out of the trade is too problematic to be priced and functional.

It's not just about 2:2 locked channels, hashed timelocks, or 2:3 watchtowers. There's also 2:3 of M multisigs, where M is the number of signers, being used as a state channel for Byzantine Fault Tolerant staked sidechains. These create more decentralized watchtowers, allow for instant-finality of signed transactions, and facilitate state references to co-ordinate LN DEX contract settlements, especially once the migration to stealthy transactions with Schnorr/Taproot/unicast begins.

BFT Sidechains are going to figure into solving some of the technical weak spots in the Lightning Network settlement model. It bears considering, when I use portfolio margin on Deribit, ultimately Deribit is assuming underlying clearing risk for me blowing up my account. Perish the thought, but let's say I was a sloppy options trader and I sold 10x the number of naked calls as my equity, Deribit would end up on the hook after that sudden \$500 snap rally that you know can happen any day. Who takes the role of Deribit to enable more sophisticated margining? It would have to be the sidechain, with collateralized validators checking up on state, taking small fees, another layer of income and risk removed.

Turns out this risk spectrum goes in deep if you zoom in on the middle. It's probably the next big thing in derivatives, fueled perhaps by hyper-bitcoin-dollarization, a process of mainstream finance replacing the Eurodollar model with a bitcoin-backed dollars model. If you look into how much time and money is spent on Wall Street trying to deal with collateralization and counterparty risks, you could see how with just the right amount of momentum, just the right amount of debt supercycle unwinding, macro tail-winds, pricing in every inch of a vast semi-decentralized network of dealers, could become quite interesting for Wall Street. They need this financial system, it will eventually save them so much money vs. the old, not because "blockchain technology reduces overhead on back-office auditing and compliance tasks – for the enterprise." But rather because the collateral discounting rates will precipitously favor it. Time value of money is the crux of the whole banking business and they will follow the value in time.

Thanks to Nik Bhatia for providing good feedback on how to reposition the key themes of the essay front and center. Also to Dan Goldman for technical feedback.

Tweetstorm: Power and Money

By [Saifedean Ammous](#)

Posted February 17, 2019

Fiat money allows wars with no real cost to governments, which makes detestable bloodthirsty chickenhawk scum like [@MaxBoot](#) & [@BillKristol](#), who've never faced costs for their warmongering, the perfect "foreign policy experts".

Why Are These Professional War Peddlers Still Around? Pundits like Max Boot and Bill Kristol got everything after 9/11 wrong but are still considered "experts." <https://www.theamericanconservative.com/articles/why-are-these-professional-war-peddlers-still-around-tucker-carlson-max-boot-bill-kristol/>

In 2003 Wolfowitz told Congress the Iraq war would be practically costless. It turned out to cost more than \$2Trillion.

With hard money Wolfowitz would have had to raise the \$2T BEFORE war.

With easy money, he can get his carnage on & leave taxpayers footing the bill for decades

Wolfowitz was not alone. Richard Perle, Lawrence Lindsay, Kenneth Pollack, Glenn Hubbard, Ari Fleischer, Donald Rumsfeld, & Mitchell Daniels all lied about the expected cost of war. They all got paid handsomely for it; never had to pay back a dime.

Who Said the War Would Pay for Itself? They Did! Unwise words from the "experts" who promised a cost-free war. <https://www.thenation.com/article/who-said-war-would-pay-itself-they-did/>

Modern "intellectuals", who are government propaganda parrots, think this is just how war works. I urge you to read Hoppe's Democracy The God That Failed for an explanation of how war functioned under governments forced to be responsible by hard money:

riosmauricio.com/wp-content/upl...

Under hard money, governments had to finance their operations from their citizens, which made wars possible when necessary but bankrupted governments that engaged in unnecessary war. War was limited & contained to expensive armies kings were careful to not decimate needlessly.

Under hard money, governments fought till they ran out of their own money.

Under easy money, governments can fight until they completely consume the value

of all the money held by their people.

This is why the century of central banking was the century of total war.

Whatever you think of the retarded Keynesian economics used to justify government control of money, you need to come to terms with the fact that the most horrific criminals of history have all operated with easy government-controlled money, as discussed in The Bitcoin Standard:

It is no coincidence that when recounting the most horrific tyrants of history, one finds that every single one of them operated a system of government-issued money which was constantly inflated to finance government operation. There is a very good reason that Vladimir Lenin, Joseph Stalin, Mao Ze Dong, Adolf Hitler, Maximilien Robespierre, Pol Pot, Benito Mussolini, Kim Jong Il, and many other notorious criminals all ruled in periods of unsound government-issued money which they could print at will to finance their genocidal and totalitarian megalomania. It is the same reason that the same societies which birthed these mass murderers did not produce anyone close to their level of criminality when living under sound monetary systems which required governments to tax before they spent. None of these monsters ever repealed sound money in order to fund their mass murder. The destruction of sound money had come before, hailed with wonderful feel-good stories involving children, education, worker liberation, and national pride. But once sound money was destroyed, it became very easy for these criminals to take over power and take command of all of their society's resources by increasing the supply of unsound money.

This is why bitcoin matters, and this is of course the point that critics of bitcoin miss. What better technology do you have for castrating scum like Kristol & Wolfowitz & preventing their sociopathic minds from capturing government money & causing millions of deaths?

Bitcoin's real cost is in hardware & electricity needed to run the network. Fiat's real cost is the hundreds of millions of deaths financed by government made omnipotent by inflation.

Which do you find more expensive? Which would you rather pay in the twenty-first century?

Bitcoin might end up consuming half the world's electricity, but if it prevents one war, that would be the best bargain humanity ever got.

Bitcoin might be the most important application of electricity. Can you think of a better use for electricity than neutering mass murderers?

Cryptonetwork Governance as Capital

By [Joel Monegro](#)

Posted February 19, 2019

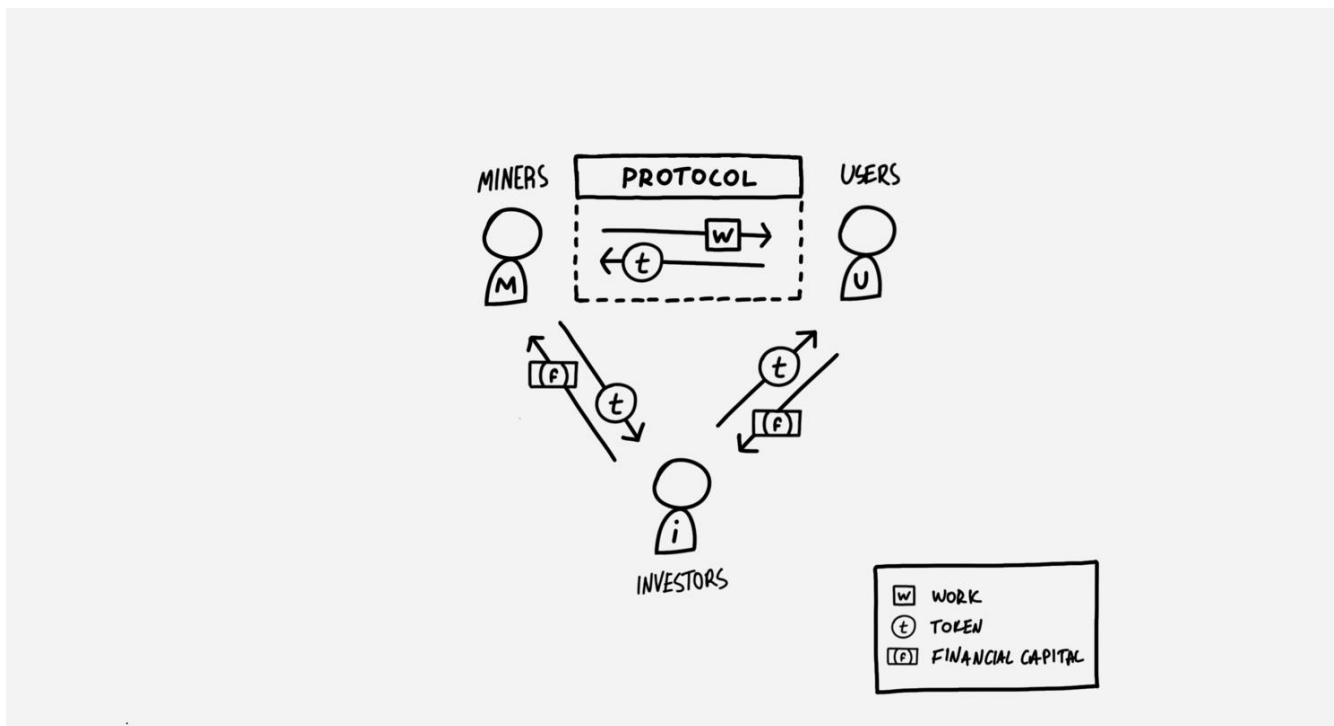
Capital is, in essence, *the power to organize the economic resources of a social system*, and its worth a function of how much of those resources can be directed to the holder's benefit. This understanding reveals the inherent value of *cryptonetwork governance as capital*, and helps us understand tokens with governance rights as new kinds of capital assets.

All forms of capital offer some kind of control over the distribution of economic resources across a group of people – in effect, *governance* over that pool of resources. Productive and human capital, for example, influence which goods and services are offered in the economy (and thus how income is ultimately distributed), financial capital determines the distribution of purchasing power, and equity capital presides over how a company's resources are used. Intangible forms of capital also exhibit this quality: political capital, for example, governs the rules of markets, and social capital drives human attention (and thus behavior).

This insight, that capital is governance (and vice versa) leads to the source of its intrinsic value: whoever has control over a pool of important resources also has the potential to direct some of those resources to their own benefit, so the value of a system's capital can be considered proportional to the value of the resources it governs.

This relationship is very clear in the case of corporate equity, where the value of a share of stock (which is essentially a voting instrument) is rooted in its right to a piece of the company's book and profits – its 'assets under power', so to speak. The relationship is less clear in the intangible realm, where capital does not take the form of tradable assets that can be priced by the market, but remains present nonetheless. For example, we might look at [the global cost of corruption](#) (about \$3.6 trillion/year, or 5% of the economy) to assess part the value of political capital, even though "political capital" is not constructed to produce direct economic gains for its holders. Similarly, we might observe the ability of social media influencers to profit from their fame, even though having lots of followers does not by itself guarantee a right to financial benefit.

This relates to cryptonetworks insofar as they are a new form of social organization. It is useful to think about these ideas through [the cryptoeconomic circle](#), pictured below:



The Cryptoeconomic Circle

The two pillars of trust of a cryptonetwork are its cryptoeconomic and governance models. The cryptoeconomic model defines 'the rules' of the system (what is the unit of work, how do users pay, how miners are compensated, the token supply model, etc.), while the governance model defines who has the *power* to change those rules, and under which conditions.

If capital is the power to organize economic resources, then the power to change the rules of a cryptonetwork forms its capital. And when that power takes the form of a token, it can be traded, priced and modeled by market. In this context, a network's 'assets under power' include (1) the token itself, which is controlled by the cryptoeconomic policy, (2) productive resources, as controlled by the definition of 'work' (e.g. the consensus protocol), and (3) flows of value, as controlled by regulating payment mechanics and other incentives for miners, users and investors. And as the value of these resources grows, so does the value of the capital which governs them.

Certain proof-of-stake systems are good examples of this idea. Here, miners are required to lock a certain amount of tokens in order to be allowed the right to work for the network. The value which flows from users to the supply side is then distributed to miners proportionally to their stake. This way, tokens that can be staked are a form of capital in that they represent the power to organize some of the economic resources of the network, such as production capacity and distribution of

income. And ultimately this is a form of governance, in the sense that staking is a mechanism for deciding how income should be allocated across miners. And so, as the value of that income grows with user demand, so does the value of stakeable tokens.

For example, in [Decred](#), 30% of the block reward is reserved for users who participate in its proof-of-stake consensus layer, and that reward pool is divvied up in proportion to how much \$DCR each participant has staked. Here, \$DCR is a form of capital as it has power over how some of the block reward is distributed. But because Decred also allows the PoS layer to vote on the use of its community pool (which is funded with 10% of each block), as well as on protocol upgrades, the value of \$DCR as a capital asset extends beyond what is connected to block-reward revenues. Such power is harder to quantify, and therefore difficult to price, but remains an important value driver that we might consider a kind of “governance premium”.

I first presented the thesis that governance is capital (and thus the driver of long-term token value) at the [Token Engineering meetup in New York](#) in early 2018, where I showed the following slide which describes the features of what I now call **power tokens**:

INSIGHT

Tokens with governance serve as both *currency* and *capital*.

Currency Function

Power to consume

Short-term focus

High frequency and velocity

Means of exchange, unit of account

Capital Function

Power to govern

Long-term focus

Low frequency and velocity

Store of long-term value

[p]

Slide from [TokenEngineering](#) talk *On The Price and Value of Governance*

The basic principle behind power tokens is that they fuse the features of “utility tokens” and “governance tokens”, which really means the combination of currency and capital – with the capital function being the driver of long-term value. We’ll dive deeper into power tokens, the nuances, and why this combination is important in the next post in the cryptocapitalism series. But for now, the key insight is that what we’re dealing with in the creation of these new assets is the creation of new forms of capital, *network capital*, that is natively digital, and cheap to distribute – and that’s important.

Links

- <https://www.un.org/press/en/2018/sc13493.doc.htm>
- <https://www.placeholder.vc/blog/2019/1/5/the-cryptoeconomic-circle>
- <https://decred.org/>
- <https://www.youtube.com/watch?v=Mwv4nnvTI5E>
- <https://youtu.be/Mwv4nnvTI5E?t=250>

There is no such thing as decentralised governance

Working toward the crypto trias politica

By [Lawrence Lundy-Bryan](#)

Posted on February 20, 2019

TL:DR

- The terms off-chain governance and decentralised governance are used with abandon in the 'crypto' space and without a full grounding in political philosophy.
- Decentralisation, or preventing the concentration of power and increasing individual liberty isn't a binary choice between centralisation and decentralisation, it's a spectrum.
- Different decisions and classes of decisions will need different levels of decentralisation and appropriate mechanisms for conflict resolution to balance efficiency versus diversity.
- Today, most crypto projects are governed by the open-source development tradition based predominantly on Linux and the foundation model instigated by Ethereum. These structures are not robust enough if we are to build inclusive equitable global public utilities.
- On-chain governance solutions are a step in the right direction but are liable to concentration of power in a technocratic elite with the time, knowledge and reputation to vote and decide on policy changes.
- The separation of powers (trias politica) model which forms the basis of almost all liberal democracies provides a more appropriate framework than traditional corporate governance or full on-chain governance. Crypto networks need an executive (implement law), a legislative (create law) and a judiciary (interpret law).
- Three network branches would formalise powers and act as necessary checks and balances on power consolidation. Regular voting and term limits would prevent power grabs by stakeholders, and formalised laws would build trust in the system by users that don't want to participate in governance directly. A separation of powers will form the foundation of a social contract between the network and users.
- We aren't just building businesses, so corporate governance won't work. We aren't just building economies, so economics alone won't work. We are building global communities, so I'm afraid we are going to need politics.

I. Political philosophy for the win

I love decentralised governance and on-chain governance as much as the next person but as with the word 'blockchain', we are suffering from a lack of clarity. What actually is 'on-chain governance'? And why are we doing it? Aragon are building amazing tools and impressive projects like Cardano, Dash, Tezos, Decred, Dfinity, and Polkadot are live or going live with implementations. It all feels a bit 'blockchain 2017' and 'ICO 2018'. (And 'STOs' 2019 by the looks of things). There are some transformational ideas floating around, but it is all thrown together as 'governance'. Ideas of futarchy, quadratic voting, and liquid democracy are unmoored from the anchor of political philosophy. The question being asked isn't a new one: how can we best organise the society/community? We have reached the answer of 'full decentralisation' because that was the answer for a peer-to-peer electronic cash system. It seems like we have decided the answer before we understand the problem.

In thinking through the question of how best to organise, the tension is between self-interest and group interest. How do we create rules to ensure individuals can trust that acting in the group interest also serves their self-interest? In small scales like families, clans and tribes, trust is formed through reputational pressure. But at larger scales like companies and states, trust needs to be codified as less formal pressures are less effective between strangers. Trust is enshrined by institutions into rules, laws and regulations: essentially so that it can scale.

And then Bitcoin came along. A ledger that could be securely amended by all participants anonymously. So for the first time scaling trust without the need for an institution to enforce the rules. Rules would be enforced by cryptography, economic and game theory dynamics. This idea of the 'trust machine' and 'scaling trust' became a common narrative, but it is now clear that decision-making is more complex. The bitcoin network and other public networks using proof-of-work can successfully enforce rules in a collective way, but for rule creation, amendment, and conflict we lack equally effective mechanisms.

II. The crypto trias politica

One of the best ways to contextualise the challenges of decision-making is one that is pretty familiar. Inspiring the Constitution of the United States, the French philosopher Charles-Louis Montesquieu published *The Spirit of the Laws* in 1748 and coined the term the 'separation of powers'. The concept was to divide government responsibilities into three to reduce the potential for the concentration of power and provide for checks and balances. The executive branch would be responsible for implementing and administering the public policy, the legislative branch for enacting the laws, and the judicial branch for interpreting the laws and conflict-

resolution. Certainly, the objectives of nation builders and crypto-network builders are similar: reduce the potential for concentration of power.

“A dependence on the people is, no doubt, the primary control on the government; but experience has taught mankind the necessity of auxiliary precautions.” James Madison

The Executive (Development Team)

The framing is not perfect, but crypto-networks today are like the executive branch lacking a functioning legislative or judicial branch. The executive branch can be seen as the core developers that invented and are tasked with developing the network. They are guiding the technical roadmap and pushing updates. In some cases the executive is formalised as a commercial entity, but in most cases, the executive is an ad hoc collective of individuals without any formal structure. Improvement proposals are an open process but in most cases, the accepted proposals are those from the core developers/executive branch. In the U.K. parliament for example, any member of parliament can propose a bill, but generally only high profile bills supported by well known members of parliament get support. Often proposals are accepted or rejected based on the different visions stakeholders have for the network. E.g. digital cash or digital gold with the Bitcoin network. In a national system of governance you could describe these differing visions for society or the network as political parties. However, unlike national systems with elections, crypto networks do not yet have a mechanism for changing the executive within the system, instead forking is the dominant expression of unhappiness. If crypto-networks are to be the digital communities of the future, it is imperative that a mechanism less destructive than forking is used to express the differing values of the community. Equally, it is unclear if eliminating the executive completely by dissolving the foundation and delegating all decision-making to the network users is an effective way to achieve network robustness and sustainability. A more pragmatic approach might be executive elections every four years acting as a limit to the concentration of power. The creation of a crypto legislative and judiciary would do the same.

Maybe the contours of an elected executive looks a little like the [Collection Code Construction Contract \(C4\)](#). But many projects are fearful of being seen as ‘centralised’ or wielding too much power over the network. Indeed, as networks are still small consisting predominantly of pioneers and early adopters for which any form of centralisation is seen as anathema, this is a reasonable fear. But as networks grow and onboard the early majority, users will have different requirements. They will care about performance, ease-of-use, and innovative new features. An elected executive with a four-year mandate with budget to deliver could outcompete a network that has fully on-chain governance in which proposals are debated but consensus is hard to achieve.

The Legislative (The Foundation)

Very few projects have separated powers between an executive branch and a legislative branch. The legislative is tasked with the creation of laws and in most cases has the ability to allocate budget. The legislative is called a parliament, congress, and assembly depending on country. After the Ethereum Foundation set up in Switzerland, most crypto projects use a foundation structure primarily as a vehicle to raise capital rather than as a check on power. Tezos is an example of the difficulties in delegating budgetary responsibilities to a foundation. One popular approach is for money to be released by a foundation to the development team based on milestones. Blockstack and Aragon are compelling examples of this approach. This grant sign-off function of the foundation to the development team is similar to the process of budget sign-off by the legislative to the executive. However, there are few examples today of foundations acting more like a legislative and taking responsibility for lawmaking or network policy. (Edit: Sovrin's Trust Framework is an example). Network policy is in theory delegated to the users of the network, but in reality, very few users are involved in network policy because of the time commitment and technical understanding required to contribute. On-chain governance approaches such as Dfinity, Tezos and Decred are experimenting with formally delegating some network policy responsibilities to the users of the network, which looks much more like direct democracy a la Switzerland than representative democracy.

The challenge will be in how to encourage participation in the creation and voting on network rules. Voter turnout in real-world elections can be close to 90% in Belgium or just 40% in Chile. And that is just for a single vote for a president or political party. How will on-chain governance projects limit voter fatigue? Or explain complex technical details that need to be voted on? Delegates or representatives are a good way to reflect the aggregate desires of a larger community. Innovation and experimentation should be around the size and structure of the legislative, rather than complete abolition. Vote for different representatives to take decisions on your behalf in areas for which they are experts. A cryptographer on security policy, an economist on budgetary policy, and a constitutional lawyer on constitution changes. With the appropriate rewards for representatives, a system can be designed that has powerful feedback loops between the actions of representative and the represented. It would be interesting to experiment with term limits to try and find an optimal term length to incentivise long-term thinking and high levels of performance. Every decision cannot be fully 'decentralised', in fact, a more robust system would be one in which a legislative body of elected domain-experts makes decisions on behalf of the electorate. You could even add a transaction fee to pay for such a body. Sounds a little bit like a taxation system....

The Judiciary (Miners?)

The third branch and the least developed in the crypto community is the judiciary. It has been argued, most prominently by [Fred Ersham](#), that miners can be considered the judiciary in the sense that they 'enforce' rules. That isn't quite right because in a state the judiciary interprets the rules to resolve disputes. Miners don't really have any power to interpret. The community did also for a period suggest that "code is law" which did away with the need for a court system. With this line of logic, the judiciary is just an interpretive branch and therefore if new law was machine readable you could avoid disputes by well-designed laws. That is indeed a dream scenario, but the fact is, crypto projects will plug into real-world legal infrastructure for the foreseeable future. The SEC will see to that. Therefore dispute resolution will have to refer to existing legal structures as [Mattereum](#), [Kleros](#), and [Aragon](#) take a different path trying to resolve as much as possible with a digital judiciary of jurors and game theory. Interestingly, Aragon throw a prediction market into the mix as a second appeal court. It's possible that with portable reputation and self-sovereign identity, reputation becomes so vital to an individual's ability to participate in the community that it acts as a sufficient deterrent to anti-social behaviours. Who needs prisons if the police could prevent Fortnite for a year? The Chinese social credit system spotted an opportunity early. For the foreseeable future though as real-world assets are on-boarded onto decentralised networks there will need to be an arbiter of conflicts. If we are to build trust in the system, there will need to be an independent branch of the network that does not develop policy. The DAO bug and rolling back of the Ethereum network by the executive branch showed that the network lacked a robust conflict-resolution mechanism resulting in a loss of trust and a fork.

What an independent judiciary will look like in crypto networks is an interesting question. Crypto-economics can only take you so far. As long as bugs exist in software and individuals interpret information differently there will be conflicts to be resolved. All conflicts cannot be automated away by perfectly written contracts. For the foreseeable future there will be a need to have humans in the loop. The exact structure of a digital court could be experimented on for lower-level conflicts. What is the optimal number of jurors to strike a balance between understanding a case and finding consensus? How are jurors selected in order to prevent bias? Are domain-experts chosen to rule on particular cases? Is there room for voting experimentation? For example, how would quadratic voting work for conflict resolution? More questions than answers at this point, but the key is to start asking questions. The more people on-boarded to crypto and the more activity that takes place on networks, high-quality conflict resolution could be key to building sustainable trusted networks.

III. End of corporate governance and toward network constitutions

Surely we just want to build technology and get users to use it? Lean startup style? Right? Wrong. As software has scaled to billions of users, many of the problems Facebook and Google face are those of nation states not corporations. Balancing free

speech and censorship; individual privacy versus collective benefits of data aggregation; state-sponsored disinformation campaigns. You can make the case that Facebook in particular has managed these crises poorly, but I would argue that it is structurally not designed to manage these political problems. Corporate structures are designed to balance the needs of investors, management and to a limited extent employers. Users are not stakeholders in this structure.

Crypto projects are embarking on a vast experiment in inclusive governance. Users are a core stakeholder in decision-making and investors are not prioritised. There is an almighty tug-of-war between all stakeholders as you would expect, but it's clear that if the ambition is to build global digital infrastructure, a traditional corporate structure isn't going to cut it. So the race is on to understand and experiment with governance models which take the best from national governance in terms of limiting the concentration of power and mix it with the efficiency of corporate governance structures. The debate has been fixated on increasing the number of nodes that can validate transactions when referencing how 'decentralised' a network is. From a security perspective, I can understand why. But equally important is the concentration of network policy power and the concentration of conflict-resolution power. DAOs are part of the answer to automate budgetary responsibilities and projects like [Moloch](#) are pushing the envelope. But DAOs should be part of a broader constitutional framework.

I would advocate for the creation of a network constitution that outlines the values of the community. These are basic values for which users would opt into. These values will help guide decision makers in the early days without precedents and when network preferences are hard to gauge. Decisions would be made in line with the values of the community not arbitrarily depending on the needs of the network or the development team at the time. E.g. data will always be owned by the user; all steps will be taken to protect user privacy; state level censorship-resistance will be prioritized; or 10% of all assets held in wallets will be redistributed to invest in charitable efforts. When all code and data is open-source, values are the only sustainable competitive advantage.

Once values have been articulated, the next steps are to formalize the structures for a network executive, network legislative and network judiciary. Checks and balances should be mapped out. And relationships between each body should be defined such as voting mechanisms. This work should be done in the open with the consultation of the network. The timing of this is a challenging question. The risk is slowing down decision-making to a crawl with multiple power-bases preventing decisions from being made e.g. the on and off again U.S. Government shutdown or Brexit deadlock. But equally, there is a risk that without the build-up of the different branches, the executive branch will consolidate power and lose the trust of the network stakeholders. Committing to abolishing the foundation as some crypto projects are planning is one strategy to prevent consolidation. The risk is that the

network does not have the rules and processes in place to effectively make decisions. If this were easy, political science wouldn't exist.

The crypto trias politica

We aren't just building businesses, so corporate governance won't work. We aren't just building economies, so economics alone won't work. We are building global communities, so I'm afraid we are going to need politics. We can't just say 'decentralised governance' or 'on-chain governance' and get the network to vote on all decisions. We all want to meet the goals of inclusive, broad-based, diverse decision-making to limit the concentration of power. But we need to learn from the hundreds of real-world main-nets/nations operating today. These nations all have decision-making processes seeded from a single idea from 1748: the separation of powers. We now have the tools to improve governance and fix some of the misaligned incentives in national governance systems. But let's not throw the baby out with the bathwater. We need a crypto trias politica.

Links

- <https://rfc.zeromq.org/spec:22/C4/>
- <https://medium.com/@FEhrsam/blockchain-governance-programming-our-future-c3bfe30f2d74>
- <https://mattereum.com/>
- <https://kleros.io/>
- <https://blog.aragon.org/aragon-network-jurisdiction-part-1-decentralized-court-c8ab2a675e82/>
- <https://github.com/MolochVentures/moloch>

A Primer on Bitcoin Investor Sentiment and Changes in Saving Behavior

By [Tuur Demeester](#), [Tamás Blummer](#), and [Michiel Lescrauwaet](#)

Posted on February 20, 2019

In our conversations with institutional investors, we often get asked the question “What is your model to value Bitcoin?”. Investors want to know what the fundamental drivers are behind BTC price gyrations, and whether at a given time Bitcoin is overvalued, undervalued, or at fair value. The new measures we suggest here are tools to help with that judgement. We build on work that goes back to 2011, and use the Bitcoin blockchain to extract market information not generally available for traditional commodities.

We suggest two new ways to measure changes in Bitcoin saving behavior:

- **Relative Unrealized Profit/Loss Ratio** ($\approx$ investor sentiment)
- **HODLer Position Change** ($\approx$ insider buying/selling)

Also introduced is the **Liveliness** measure, which reflects the extent to which a cryptocurrency is meaningfully used by savers.

A History of Bitcoin Valuation Research

Here’s an overview of the quantitative approaches we’ve seen Bitcoin investors take to help them decide what its fair value is at any given time.

- In 2010, Bitcoin users tried [calculating](#) the “value” of one Bitcoin by estimating the electricity cost of mining it. However, the usefulness of this was quickly [dismissed](#), as the cost of mining goes up when investors bid up the price of Bitcoin.
- In 2011, early investors [came up](#) with the idea of calculating Bitcoin’s market cap as a valuation tool, and with the concept of ‘[Bitcoin Days Destroyed](#)’. The latter was dubbed an “indicator of market health and participation” and it was the first valuation metric that considered the age of addresses. There was also discussion about a “[Price over Difficulty](#)” ratio, to [determine](#) whether it was better to mine than to buy BTC, and forum threads emerged about how many [lost coins](#) there might be.
- In 2012, Trace Mayer [suggested](#) the 200 Daily Moving Average of Bitcoin’s market capitalization as a value indicator, because it filters out the long-term secular uptrend.

- In 2013, [various authors explored](#) the idea that Bitcoin's price is in a long-term [parabolic uptrend](#), and that deviation from that trend line is [indicative](#) of over- and under valuation.
- On January 1st, 2014, user gbianchi proposed "[Network Value](#)" as the ratio of Bitcoin's address growth and its market capitalization—[similar analyses followed](#) later that year.
- In November 2014, developer Jon Ratcliff [published](#) his analysis of the blockchain, showing the distribution of bitcoins based on age of last use, and commented "This graph shows ... how many bitcoins are actively moving at any one time over time."
- In September 2017, [Willy Woo](#) and [Chris Burniske](#) published research around the [NVT ratio](#), which was called a "PE Ratio for Bitcoin" as it focused on comparing Bitcoin's on-chain volume with its market cap.
- In March 2018, Dmitry Kalichkin suggested a variation on NVT which he dubbed the [90-day NVT ratio](#). Two months later introduced the [Network Value to Metcalfe ratio](#) (NVM) which was based on Daily Active Addresses.
- In April 2018, Dhruv Bansal [updated](#) Ratcliff's work on [UTXO](#) age distribution, and suggested the concept of HODL waves. He commented: "It is not possible to make charts such as the one above for traditional asset classes. It's only Bitcoin and other public blockchains that meticulously track these data throughout their whole histories. This enables post-hoc analyses of large-scale market behavior."
- In October 2018, inspired by Pierre Rochard, Nic Carter and Antoine Le Calvez created the Bitcoin "[realized cap](#)" which is the aggregate value of the UTXOs priced by their value when they last moved. Soon after, Bitcoin "thermocap" or "[accumulated security spend](#)" was suggested, which is the aggregated miner revenues over the entire history of Bitcoin.
- That same month, Murad Mahmudov and David Puell published work on the Bitcoin [Market-Value-to-Realized-Value](#) (MVRV).
- In December 2018, Tamás Blummer introduced the concept of [Liveliness](#), which reflects how much a given blockchain is used for meaningful transaction settlement.

Goal: Measure Changes in Saving Behavior

Given that we view Bitcoin's [primary use case](#) as censorship resistant store of value (digital gold), and its utility as a payment mechanism as only secondary, our main goal in identifying the components of our valuation toolbox is to find data that specifically reflects changes in *saving* behavior.

Limitations and challenges of existing valuation methodologies

The Bitcoin blockchain records a lot of data, but not all data. It is blind to how many bitcoins are [lost](#). It doesn't know whether a transaction represents a transition from

one owner to another (sale), or whether it's simply the same owner moving coins to another address in his control. It also doesn't reflect off-chain transactions—for example it won't show balance transfers from one Bitfinex user to another, or Liquid Sidechain transactions, or Lightning Network transactions.

The limitations of blockchain-recorded information, as well as the commodity nature of cryptocurrencies themselves, have consequences for valuation methodologies:

- With cryptocurrencies, information about real circulating supply is opaque, exchange listing requirements are often extremely loose, and dilution schemes can be stretched to extremes. Assigning a “[market cap](#)” to a cryptocurrency (mined coins × token price) doesn't at all create an objective comparison tool—a coin's “market cap” doesn't teach us anything about the commitment of coin holders. To illustrate: a centralized coin with a premined supply of 1 billion tokens and a single recorded sale of one token for \$10 would yield a \$10 billion market cap, identical to a decentralized coin with a large community of long-term savers. This “market cap” measure is also blind to lost coins, which stretches the comparison with the securities world where the assets are held by transfer agents, making loss a very rare phenomenon.
- The challenge with using the number of active addresses or transaction volumes (e.g. **NVT**, **NVM**) is that these data sources don't allow us to separate behavior that is long-term oriented from behavior that is short term oriented. These measures don't directly differentiate speculators from value investors, and can conceivably be gamed or inflated by moving a large amount of coins back and forth, or by creating a flurry of small on-chain transactions.

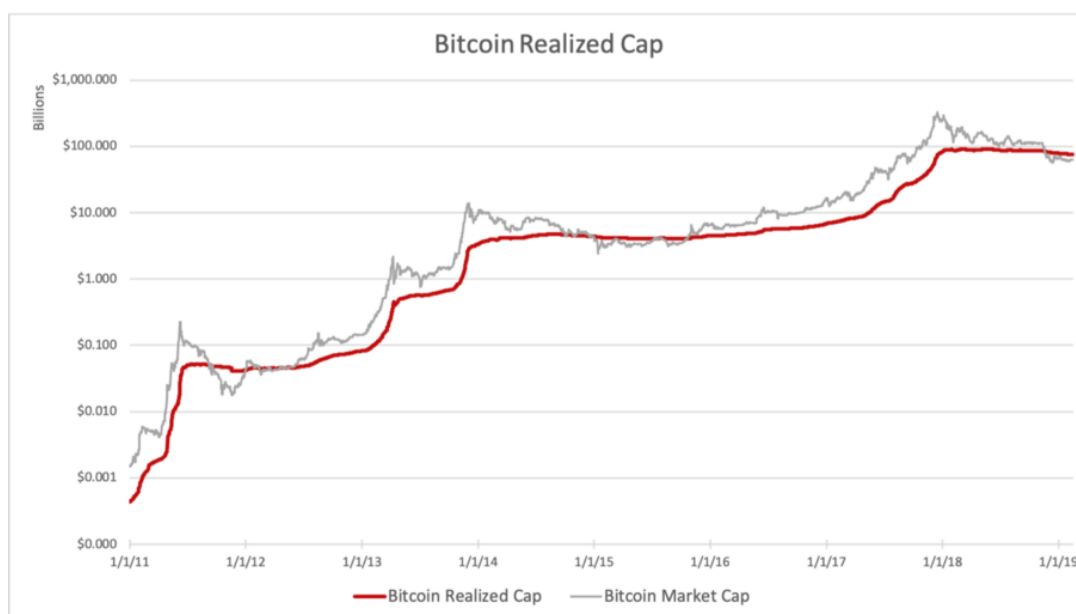
Solution

Our solution is to collect data that places each circulating quantity of Bitcoin *in its historical context*, in the tradition of previous work such as HODL Waves, Realized Cap, and MVRV. We focus on the data provided by *the Bitcoin blockchain*, as this is the ultimate (most secure and final) settlement layer for all its important transactions. By taking the [Output Quantities](#) of a block, and combining it with the [Recorded Time](#) of that block, we learn more about the behavior of Bitcoin savers.

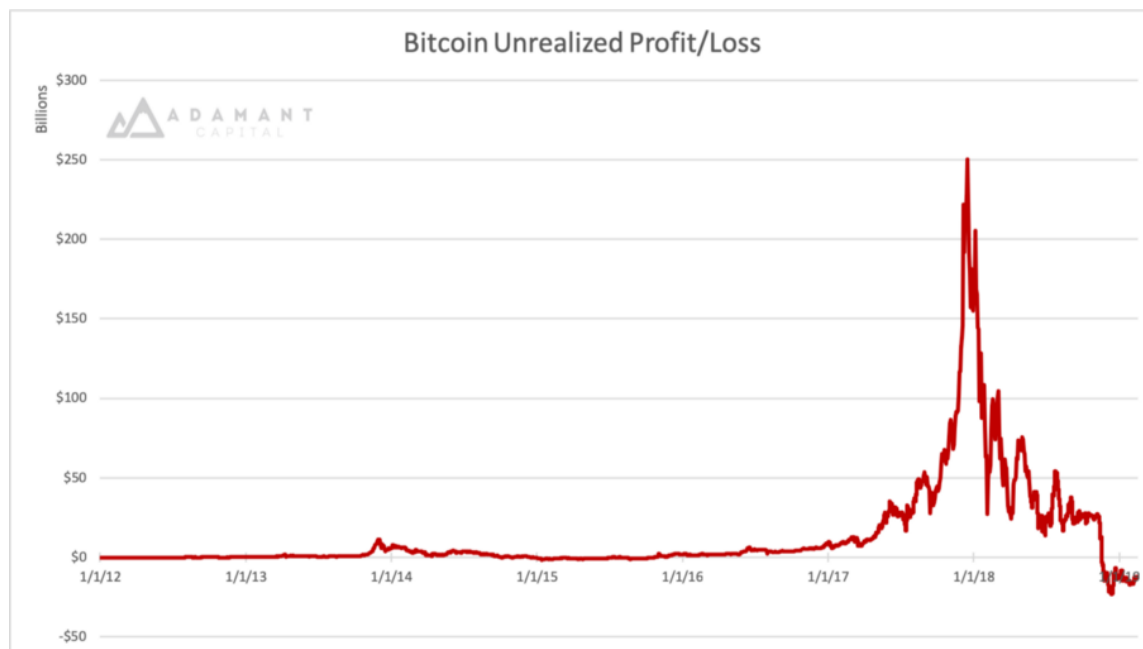
Relative Unrealized P&L (≈investor sentiment)

Every time a bitcoin moves on the blockchain, its market value is realized. The owner was aware of its value and affirmed his control over it at the point of the move. It doesn't matter if the transaction represents the owner sending the coins to somebody else (a sale or gift), or if it is an act of self-dealing.

If we value every coin at the time it last moved and aggregate these values, we arrive at the “[Realized Capitalization](#).”



By subtracting the Realized Cap from the Market Cap, we calculate **Unrealized Profit/Loss (P&L)**:



We see that Bitcoin investors in aggregate currently face a significant unrealized loss, which is quite a change if compared with the 2017 huge unrealized profits.

The measure of Unrealized Profit also contains the unrealizable profit of **Lost Coins**. Some coins are certainly lost as they were associated with a provably un-spendable output script, but the majority of lost coins can only be guessed by setting a threshold of inactivity after we consider them Lost.

The measure of Unrealized P&L estimates the total dollar amount of paper profits/losses in Bitcoin, but it does not clearly filter out the relative change that accompanies it. By dividing Unrealized P&L by the Market Cap, we arrive at the **Relative Unrealized P&L**, which can be interpreted as an indicator of investor sentiment:



When a high percentage of Bitcoin's market cap consists of unrealized profits, it can be interpreted that investors are greedy. The ratio drops as prices decline and investors likely become more fearful. When the unrealized gains turn into unrealized losses, we enter the phase of capitulation and apathy. Here's a suggested illustration:



So why does the percentage of Relative Unrealized P&L go up in a bull market? What this indicates is that on average, investors are realizing profits at a slower rate than the growth in the market cap. For the time being, 20% of the market cap consists of 'underwater' holdings—coins that would generate losses if they were sold today.

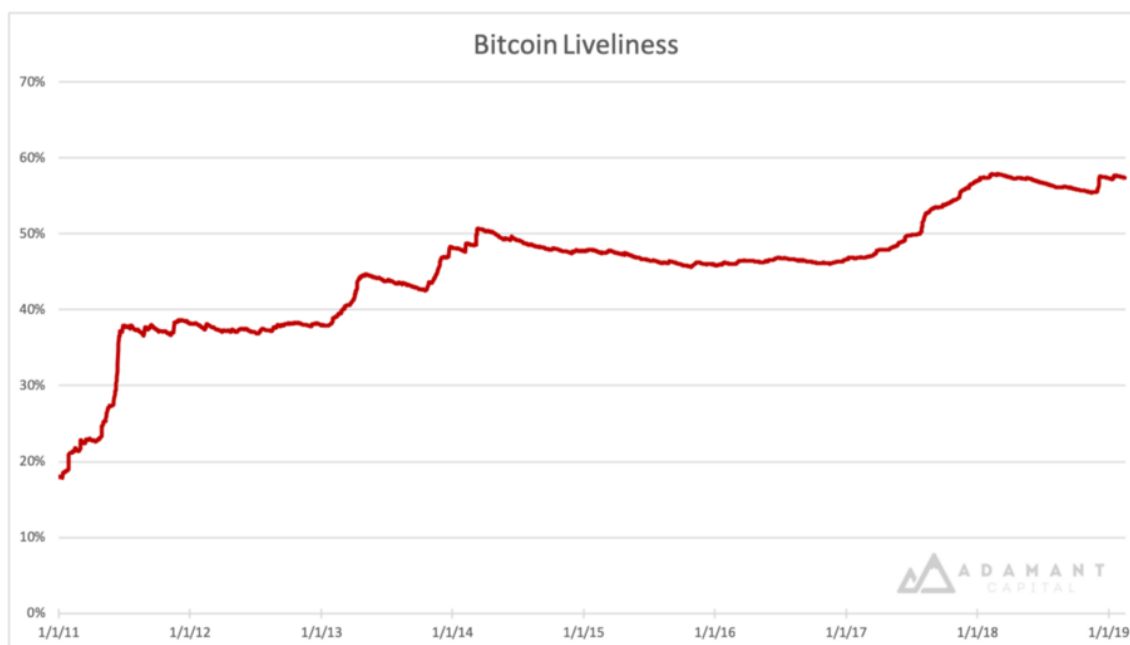
Before we move on to a new suggested valuation tool, **HODLer Net Position Change**, we first need to explain the measure of Bitcoin **Liveliness**.

Liveliness

The idea of old coins moving on the blockchain has always spoken to the imagination of Bitcoin enthusiasts and investors: “What are the ‘Bitcoin whales’ doing?”, “What might Satoshi be up to?”, etc. The analytical work mentioned in our historic overview provides investors with information on how Bitcoin savers move coins at any given time. However, the challenge with measures such as [HODL waves](#) is that they don’t provide us with a clear signal or unambiguous utility. We instead propose *a single measure* that focuses on the coins that move relative to how long they were previously dormant.

What is Liveliness?

Liveliness is a new quantitative measure that gives insights to shifts in saving behavior. The higher the amount of meaningful transaction settlement a blockchain accommodates, the higher its Liveliness.



Liveliness can be defined as the ratio of the sum of Bitcoin Days Destroyed and the sum of all Bitcoin Days Ever Created. (See [here](#) for a more detailed breakdown.)

Let’s illustrate with a few examples:

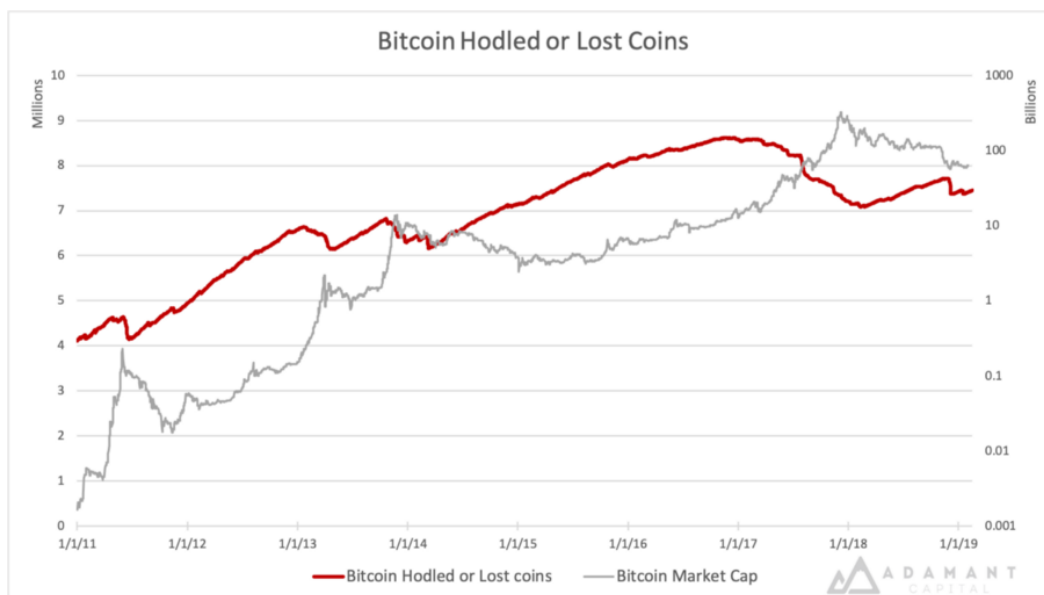
- A blockchain that during its lifetime has not yet seen a transaction other than issuance, has a Liveliness of 0%. Likewise, a blockchain where only one recent

balance is systematically moved back and forth would produce a very low Liveliness—in other words, this measure is unforgiving for lack of meaningful transactions. Bitcoin has high Liveliness if it facilitates the transfer of large amounts of old coins on a regular basis.

- A blockchain where all the coins move within a single block has at that moment a Liveliness of 100%. A blockchain of two years old with no new block rewards, and where exactly one year ago all coins moved within a single block and no transactions moved since, would have a liveliness of 50%. In other words, the measure fluctuates relative to the total lifespan of the blockchain.
- The total circulating supply also impacts Liveliness: if in the previous example 20% more new coins were created in the year since all the coins were moved, then the Liveliness today would not be 50% but only 40%. So this measure also warns us about blockchains with high inflation/dilution.

Liveliness **can be used to weight market cap if comparing cryptocurrencies**, as it will be close to zero for currencies that have inflated market cap through pre-mined coins or wash trading of the same few units.

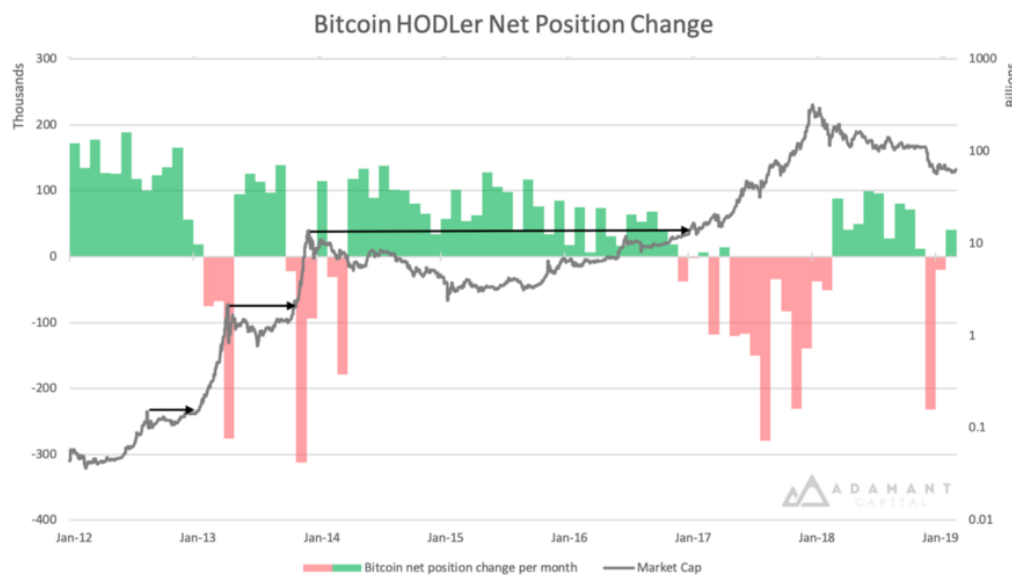
Besides this, Liveliness can also be used as a **foundational tool** from which to derive other insightful time series. One of these metrics is the aggregation of **Lost or HODLed Bitcoins** and alerts us to moves of large and old stashes. For this purpose, subtract Liveliness from 1 and multiply with the circulating supply at the time.



HODLer Position Change (≈insider buying/selling)

Now that we know the approximate number of coins that are held as a long term investment or are lost, we can approximate the monthly position change among

Bitcoin savers. We call this measure **HODLer Net Position Change**. Because it only measures actual moves of coins, our graph naturally excludes lost coins.



We see that significant quantities were cashed out during bull markets of Bitcoin, and net new positions were accumulated by HODLers in bear phases. Net buying seems to switch into net selling once the previous top is reached (cf. arrows on the graph above).

It's important to note that a significant amount of coins are held on Bitcoin exchanges and that mere administrative decisions on their behalf can have a significant impact on measures like HODLer Net Position Change. However, serious effort has been made to de-anonymize exchange addresses, so future analysis should be able to mitigate for "exchange bias."

For example, one anomaly in the graph is the **recent negative position change of meaningful Bitcoin savings** (Dec 2018). While at first sight this is worrisome, [we found evidence](#) suggesting that a significant part of the move stems from Coinbase reshuffling around 5% of all BTC in circulation.

Another notable negative position change is the **278,000 BTC net move in August 2017**. This is likely attributable to the [Bitcoin Cash hard fork](#) (BCH) of that same month. Every Bitcoin private key gave access to an equivalent amount of BCH as the BTC in that wallet. And so with BCH rallying strongly—at some point reaching over 20% of a BTC—Bitcoin HODLers were incentivized to split the two via on-chain transactions and either buy more BCH and sell their BTC, or vice versa. Given how strong the (flawed) narrative was at the time of BCH being "the real Bitcoin," it's conceivable that many old bitcoins were actually sold. More analysis is needed in this area.

Conclusion

By creating tools that measure changes in saving behavior on the Bitcoin settlement layer, we believe to have meaningfully contributed to the valuation debate. **Relative Unrealized Profit/Loss** in Bitcoin tells us about Mr. Market's emotional state, **HODLer Net Position Change** gives us information about how Bitcoin whales are moving their pieces on the chessboard, and **Liveliness** gives us a powerful tool to meaningfully compare long-term investor activity, as well as a platform for building new valuation measures in this space.

In a follow-up article we will share our take on what these and other measures tell us about Bitcoin's valuation today. Feel free to [contact us](#) with questions, or [sign up here](#) for future research updates.

Links

- <https://bitcointalk.org/index.php?topic=98.20>
- <https://bitcointalk.org/index.php?topic=98.msg3568#msg3568>
- <https://bitcoin.stackexchange.com/questions/2047/market-capitalization-over-time>
- <https://bitcointalk.org/index.php?topic=6172.msg90789#msg90789>
- <https://bitcointalk.org/index.php?topic=7427.0>
- <https://bitcoin.stackexchange.com/questions/419/is-there-empirical-data-about-a-relationship-between-bitcoin-price-and-difficult>
- <https://bitcointalk.org/index.php?topic=7253.0;all>
- <https://web.archive.org/web/20130328180243/http://www.runtogold.com/2012/12/during-2012-fiat-currencies-and-gold-collapse-against-bitcoin/>
- <https://altoidnerd.wordpress.com/2013/11/07/the-bitcoin-price-model-large-time-scale-calculations-of-the-bitcoin-price/>
- https://www.reddit.com/r/Bitcoin/comments/2lse5e/predictions_of_470_in_march_were_correct_now_btc/
- <https://www.tradingview.com/chart/BTCUSD/oc3YX0JB-Bitcoin-Daily-Andrews-Pitchfork-Long-term-view/>
- <https://youtu.be/K7LQu-eIOO0?t=377>
- <https://bitcointalk.org/index.php?topic=831547.msg9293359#msg9293359>
- <https://bitcointalk.org/index.php?topic=394221.0;all>
- <https://bitcointalk.org/index.php?topic=655792.0>
- https://www.reddit.com/r/Bitcoin/comments/2lpujs/bitcoin_compared_with_metcalfes_and_zipfs_law/
- <https://bitcointalk.org/index.php?topic=68655.msg9059346#msg9059346>
- https://www.reddit.com/r/Bitcoin/comments/2n205b/an_area_chart_showing_the_distribution_of/

- <https://www.forbes.com/sites/wwoo/2017/09/29/is-bitcoin-in-a-bubble-check-the-nvt-ratio/#40ef77fd6a23>
- <https://medium.com/@cburniske/cryptoasset-valuations-ac83479ffca7>
- <http://charts.woobull.com/bitcoin-nvt-ratio/>
- <https://medium.com/cryptolab/https-medium-com-kalichkin-rethinking-nvt-ratio-2cf810df0ab0>
- <https://medium.com/cryptolab/network-value-to-metcalf-nvm-ratio-fd59ca3add76>
- <https://blog.unchained-capital.com/bitcoin-data-science-pt-1-hodl-waves-7f3501d53f63>
- <https://bitcoin.org/en/glossary/unspent-transaction-output>
- <https://coinmetrics.io/realized-capitalization/>
- <https://medium.com/@RainDogDance/bitcoin-as-a-novel-market-institution-nic-carter-talk-at-baltic-honeybadger-2018-e085f163b213>
- <https://blog.goodaudience.com/bitcoin-market-value-to-realized-value-mvrv-ratio-3ebc914dbaee>
- <https://medium.com/@tamas.blummer/liveliness-of-bitcoin-174001d016da>
- <https://medium.com/@vijayboyapati/the-bullish-case-for-bitcoin-6ecc8bdecc1>
- <https://blog.unchained-capital.com/bitcoin-data-science-pt-2-the-geology-of-lost-coins-79e5a0dc6d1>
- <https://coinmarketcap.com/>
- <https://bitcoin.stackexchange.com/questions/4301/what-is-an-unspent-output>
- <https://bitcoin.stackexchange.com/questions/7788/what-format-is-the-time-of-a-bitcoin-transaction-stored-in>
- <https://en.wikipedia.org/wiki/Hodl>
- <https://medium.com/@tamas.blummer/coinbase-cold-wallet-moves-possible-market-effect-68a09902feab>
- <https://bitcoinmagazine.com/articles/when-fork-forks-what-you-need-know-bitcoin-cash-goes-war/>

Bitcoin's Incentive System or When The Stars Align

By [Misir Mahmudov](#)

Posted February 20, 2019

Time and time again, we realize that forcing people to do good or to change their behavior does not lead to meaningful results. Human beings are stubborn and don't want to change for various reasons. Most importantly, humans can be selfish and are not willing to alter themselves in any way unless there is a personal gain to be earned. On the other hand, incentivizing people to behave in a particular way by rewarding them with something they value consistently produces the intended result.

Alignment of incentives is one of the most important phenomena that make up Bitcoin.

Incentives as a force behind Bitcoin's success

Apart from being a technological breakthrough, Bitcoin is a psychological and social phenomenon. Bitcoin takes human greed and turns it on its head. Bitcoin is fueled by human greed. Bitcoin uses human greed and the natural desire to better one's financial standing to ensure the integrity of the system.

Bitcoin is designed in a way that miners and holders are incentivized to behave in a way that is beneficial to Bitcoin. Any deviation from the optimal behavior on the part of the participants results in a reduction of possible profits. Bitcoin mining and the Proof of Work mechanism is perhaps the best representation of this. Bitcoin miners are incentivized to devote electricity to verify transactions and thus make the network secure and reliable. Their ability to perform this task is rewarded with miner reward (new bitcoins) and transaction fees. If, for example, a miner tried producing invalid blocks (blocks that break the consensus rules), full nodes would reject them and the miners would not be rewarded as a result. The full nodes are run by individuals as well as large processors (e.g. exchanges). These entities are incentivized to act optimally as their objective is a higher price per bitcoin (holders) and a functioning network to earn the fees (exchanges, custodians etc.) Many Bitcoin developers are employed by companies whose business models depend on Bitcoin continuing to grow. It is important to note that many of Bitcoin developers are, to a large extent, ideologically incentivized to contribute to Bitcoin. In his [Bitcoin's Incentive Scheme and the Rational Individual](#), Hugo Nguyen explores the relevance of philosophical alignment with regards to the cypherpunk ethos as an incentive for developers.

Incentives that propel Bitcoin also exist outside of the Bitcoin community itself. Given the fact that Bitcoin is neutral money (not affiliated to any particular country), it can be argued that countries, institutions and various authorities worldwide are in the long run disincentivized from banning and restricting Bitcoin's use and development. Given that Bitcoin is designed to exist and thrive in an adversarial environment, a particular country, say the United States, stands to lose by banning Bitcoin as developers, users and companies working and using Bitcoin (an industry at the forefront of technological and economic innovation) would relocate to a more accommodating jurisdiction. Given the tense relations and the international rivalry among the world's superpowers (US, China etc.) it is practically impossible to imagine all such countries cooperating together to dismantle Bitcoin (e.g. a multi-nation coordinated attack against Bitcoin mining). The fact that the US dollar has been the world's reserve currency for the last fifty years gives the United States an unfair advantage over other countries that depend on the US monetary policy. Many countries stand to gain from Bitcoin's adoption as it would remove their dependence on the US dollar and provide them with a feasible alternative. It is likely that as some nations start to adopt Bitcoin as their reserve currency, the aforementioned value proposition will become increasingly clear.

Importance of Financial Incentives

As already discussed, making people do good (or anything for that matter) by force does not work. Making people do something by incentivizing them, on the other hand, does usually work.

Thus, alignment of incentives is an integral part of what makes Bitcoin work. Bitcoin is an incentive system that rewards individuals for benefiting the world as a whole. Anyone who spends enough time studying Bitcoin will realize that it will have a considerable net positive effect on our society. Its numerous positive externalities markedly outweigh any associated costs. In fact, it is becoming increasingly evident that most of the criticisms towards Bitcoin ("wasteful" mining, "unfair" distribution etc.) are a result of ignorance rather than any substantive data-backed research.

Although the number of bitcoins is strictly limited, the global prosperity that Bitcoin brings about is the opposite of zero-sum. The average human is going to benefit from the adoption of Bitcoin even if they don't necessarily own any bitcoins throughout the process of monetization and don't directly profit from the increase in bitcoin's price. It is likely that these people will live in a world where they will be paid in bitcoin. This means that their wealth will be unseizable, sound and able to move anywhere in the world in a trustless manner.

Bitcoin as a mechanism for enabling positive change

All of us wish that the world was a better place and that people acted more compassionately. In theory, everyone usually wishes only the very best for the rest of the world, however, in practice, it doesn't always play out this way. Human greed stands in the way of any decision, desired change or impact. We need to understand that, oftentimes, people forgo or give up on their moral beliefs and social responsibility in the face of personal financial difficulties. Most people are simply trying to get by and provide for their families. In the light of understanding this, it becomes more clear that expecting people to go out of their way to do something good is often counterintuitive and thus doesn't create sustainable results. Humanitarian and philanthropic efforts don't scale. They are often one time acts whose impact does not last. Similarly, redistribution schemes are too vulnerable. There are too many single points of failure which enable human greed to show itself and eventually cause the system to fail.

The biggest impact comes from aligned incentives that reward individuals for creating positive change in the world. Such systems are scalable. They work because they don't depend on finite sources of human compassion in the face of personal and financial difficulties. In fact, such systems work best because they are conducive to self-preservation. Nobody is good or bad, we are all human. We simply prioritize self-preservation over other things.

It is thus not logical to blame someone for having an X amount of bitcoin, or having bought bitcoin at a cheaper price and now becoming wealthy. Anyone who bought bitcoin at a cheaper price was rewarded for the higher relative risk that they took on when Bitcoin was a lot less robust. The economic incentives in Bitcoin were and are necessary to bootstrap a system that can level the financial playing field for the entirety of the world. To enable this, individuals needed to be incentivized.

You cannot expect people to change just by demanding them to be more compassionate. No matter how much you scream at someone telling them to donate their wealth or to give up their power, it won't happen, definitely not on a large scale. The only way to enable change is to create incentives for people. Unfortunately, when people demand corporations to be more humane, pay higher wages, institutions to be more accommodating, you see little change. The PR team launches a campaign and minimum effort is done only to maintain the brand image. Such methods don't create meaningful results as the incentives on an individual level are not aligned. They are one-sided. The individuals on one side stand to benefit while individuals on the other have to give up much of what they are already so used to.

Bitcoin is fundamentally different. Bitcoin has created a unique incentive system which caters to and encourages parties on both sides. Adoption of Bitcoin has the

ability to benefit all the people on the individual level, no matter where they are in the socio-economic hierarchy. The very corporations and institutions that stand to lose from the adoption of Bitcoin are made up of individuals who stand to benefit massively from the adoption of Bitcoin.

Understanding that every entity, group or collective is made up of self-motivated individuals is key to understanding why Bitcoin will succeed.

Don't expect people to be good. Expect people to act in their own self-interest. If everybody acts in their self-interest in a system of rules that rewards good behavior, then good behavior emerges naturally.

Links

<https://medium.com/@hugonguyen/bitcoins-incentive-scheme-and-the-rational-individual-dc20effa4715>

Crypto Governance: The Startup vs. Nation-State Approach

By [Jack Purdy](#)

Posted February 25, 2019

Intro

Humans like to argue. It's in our nature.

Take any facet of human experience and you can find two people who disagree on it. Nowhere is this more prevalent than in the realm of governance, where we argue who should have power, who gets to make changes to the system, and how decisions are ultimately made. Given the magnitude of the impact governance has, it is easy to see how this became a highly controversial topic.

Now imagine a nascent industry full of highly intelligent people with strong opinions (and egos), where most of the debate occurs on globally accessible platforms. As you can imagine, there is no shortage of debates especially as it pertains to governing this industry. Welcome to crypto.

Crypto governance encapsulates the debates around how we coordinate to make decisions on changing the rules of a protocol. This could include anything from simple upgrades to changing the consensus mechanism to allocating block rewards. It involves many stakeholder groups such as node operators, network providers (miners), core developers, users, speculators, exchanges, and block explorers to name a few. These are diverse groups with varying incentives that frequently conflict with each other. For example, node operators want to keep block size low to reduce the costs of running a full node, while miners have incentives to increase the block size so each block includes more transactions and thus more transaction fees.

It is the interactions between these stakeholder groups that define what a blockchain is, its values and principles and how it evolves over time. This governance process shapes the imagined reality we create surrounding a network, and the value of a cryptoasset lies at this [social layer](#).

Unsurprisingly, there has been a substantial amount of debate on the right way to govern cryptonetworks, which has created various thought-provoking theories. I believe much of the debate is misguided since 'crypto' is too general of a term to apply overarching ideas to. [Jill Carlson explains it](#) well:

Often investors attempt to apply the same priors and heuristics whether they are talking about bitcoin, petrocoin, or filecoin because they are all "crypto". This would be akin to applying the same

fundamental analysis to gold markets, sanctioned Venezuelan debt markets, and the pre-IPO valuation of Dropbox circa 2008.

In the same way we shouldn't apply the same fundamental analysis for these assets, we shouldn't analyze the governance of all cryptoassets in the same manner. We need to more accurately describe what is being governed in order to think about how it should be governed. In this analysis I'm going to delineate between base layer protocols from those further up the [tech stack](#). The former should be governed like an established nation, while the latter an early stage startup.

The Startup Approach

"Moving fast enables us to build more things and learn faster. However, as most companies grow, they slow down too much because they're more afraid of making mistakes than they are of losing opportunities by moving too slowly. We have a saying: 'Move fast and break things.' The idea is that if you never break anything, you're probably not moving fast enough" — Mark Zuckerberg, [IPO Prospectus 2012](#)

Zuck encapsulates this governance theory in the now famous mantra of "move fast and break things". When you are looking at early-stage, user facing applications, you need to be responsive to customer needs. This requires the ability to rapidly iterate in order to meet these changing needs. If you move too fast and there is a bug, it is not the end of the world since there is not a tremendous amount of value in the network. You fix it and move on. **The key is that the stakes are low so there aren't grave consequences if something goes wrong. Failure will not result in large personal losses or a complete loss in faith in the idea ever working again.**

Now what will this governance look like in crypto? It will likely operate like a well-oiled autonomous organization. A good example of a cryptonetwork that caters to this style of governance is Decred. (Note: Given Decred is aiming to be used as money, I am somewhat skeptical if this model makes sense for them, but regardless it is a general model I believe can be effective for more rapid improvements). Decred utilizes on-chain voting to allow DCR holders to participate in the governance process by staking tokens in order to obtain tickets. This lets stakeholders vote on matters such as how the treasury funds are spent to support development or whether consensus changes should be implemented via a hard fork. [Placeholder summarized it best](#)—"Decred's killer feature is good governance, and with good governance you can have any feature you want." **This thinking enables the necessary innovation needed to keep up with consumer needs and avoid a slow descent into irrelevance.**

“Move fast and break things” succeeded in turning Facebook from a scrappy startup to a unicorn, but once they reached scale and had data on 2 billion people, that mantra was no longer appropriate. With that many people at risk, breaking things is no longer the goal or even acceptable for that matter. Rather the goal should be keeping the system secure, and unfortunately Facebook failed at this [exposing the data of millions](#).

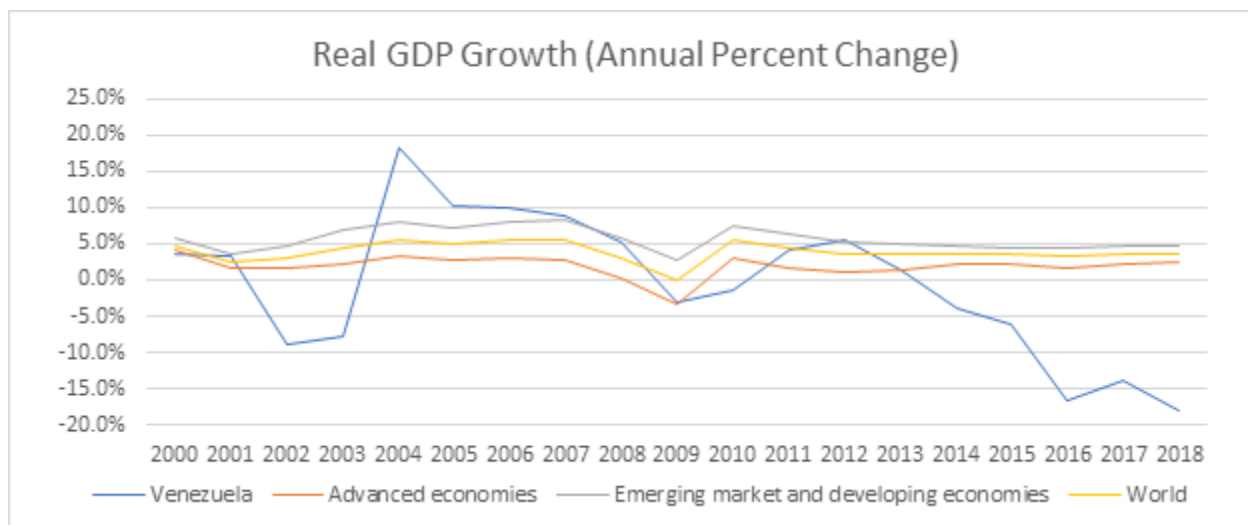
This brings us to our next approach that starkly contrasts with that of the early startup.

The Nation-State Approach

“We have to reinvent socialism. It can't be the kind of socialism that we saw in the Soviet Union, but it will emerge as we develop new systems that are built on cooperation, not competition.” — Hugo Chavez to World Social Forum 2005

In January 2005, Hugo Chavez was embarking on a mission to re-shape Venezuela. That month he [passed land reform](#) allowing the government to seize over 6 million acres of private property. Two years later the government took over the last [privately run oil field](#), with the [banks following shortly after](#). The drastic measures taken by no means stop there, and they continue to this day.

This example is not meant to make a political statement, but simply to demonstrate what can happen when a government attempts to make rapid changes that are unproven and largely experimental. This is a highly simplified illustration and there are a multitude of factors at play but that shouldn't distract from showing the risks of this type of governance. The results of these actions are widely known and evidenced by the graph below.



13 Source: IMF

When there are high stakes on the line to the underlying people, corporation, protocol etc. being governed, then the manner in which decisions and changes are made needs to optimize for the safety and security of those governed. No longer is the motive to innovate in order to outpace competitors because survival is the only way to win out.

Applying this to crypto, base layer protocols such as Bitcoin cannot afford to move fast at the detriment to security. When I refer to security here, I am talking about maintaining the well-being of bitcoin holders. This means not only ensuring the protocol doesn't break, but upholding the censorship resistance, trust-minimized features that keep these holders secure. **A 10x improvement in transaction speed or fees is not worth a 1% decline in security. If a critical bug is exploited or a users funds confiscated, it will be incredibly difficult to regain people's trust in not just Bitcoin but the entire story they tell themselves surrounding a decentralized money.** This is because technology such as Bitcoin is prone to the [Lindy Effect](#), where the future life expectancy is proportional to its current age. Therefore, the longer it survives, the longer it is predicted to survive. If it fails, it not only starts from where it began but behind since its competitors (namely fiat) are now even more Lindy.

While it can be easy to get frustrated with the slow process to upgrade Bitcoin, it should be noted that extreme caution needs to be taken in changing base layer protocols where significant value rests on top. **Valuable networks like Bitcoin need to be governed like national governments, where it is more important to reject unjust laws than to pass just laws.** The more active governance is in a cryptonetwork, the more one requires trust to interact with it and the whole [raison d'être](#) of a decentralized currency is to minimize trust in others. Bitcoin developer [Matt Corallo](#) states:

Of Bitcoin's many properties, trustlessness, or the ability to use Bitcoin without trusting anything but the open-source software you run, is, by far, king. More specifically, interest in Bitcoin appears to almost exclusively derive from a desire to avoid needing to trust some third party or combination of third parties.

This applies to other base layer protocols where there are expected to be valuable dapps built on top of it. In the same way one would be hesitant to incorporate in a country where the laws governing its business are prone to change at anytime, one should be wary to build dapps on top of a protocol that requires trust that the rules won't change in a detrimental fashion. **While this is not an apples to apples comparison, I believe it is useful in highlighting the fact that high stakes situations where there is considerable value on the line necessitate a more ossified governance structure to mitigate risk for the governed.**

Conclusion

Often times in crypto, we like to believe we're reinventing the wheel. Accordingly we come up with unique heuristics and terminology to describe things. While in some cases this is true, often times we're simply repurposing age old ideas to fit this new paradigm. I believe governance is one of these areas where we can learn from a lot from the past. For thousands of years humans have been organizing themselves in different groups to coordinate around shared goals in the form of nation-states, corporations and others social groups. Over time we have improved our standard of living as a result of organizing ourselves into these groups and evolving new ways to govern them. However, innovation in this front has been slow due to the difficulty in testing out alternate approaches (rightfully so) because of the high stakes on the line.

This is a big part of why I am so fascinated with cryptonetworks. They provide us a sandbox to try inventive new ways to organize human behavior by shifting how we incentivize participants. By carefully studying the failures and successes of different crypto projects I believe we can learn more about governance and at a faster pace than has ever been possible. A great analogy is comparing them to [petri dishes](#), where we can test out different ideas on smaller chains and based on the results begin to implement bits and pieces into more established chains.

This shouldn't be a black and white approach, but more of a spectrum based on the amount of value in the network and trust minimization required. **On one end you have Bitcoin that needs to iterate slowly, preserving security at all costs and at the other you have experimental petri dishes that can test the efficacy of new models and look to incorporate them gradually down the tech stack as they grow stronger via the Lindy Effect.**

To conclude, I believe instead of making overarching “laws” about crypto governance like [Szabo’s Law](#), we need to take a more nuanced approach. My hope here was to start separating the governance of mission critical base layer from protocols from more application specific crypto projects. I look forward to expanding my thoughts on the subject in order to further delineate the ways in which cryptonetworks should be governed.

Much of my thinking was influenced by prior work that includes:

- [Bitcoin Governance](#)
- [The Crypto Governance Manifesto](#)
- [Blockchain Governance 101](#)
- [Blockchain Communities and their Emergent Governance](#)
- [Blockchain Governance: Programming Our Future](#)
- [On Governance: Coordination, Layers, and Structural Integrity](#)
- [Cryptonetworks and Cities: Analogies](#)

Links

- <https://medium.com/s/story/bitcoins-social-contract-1f8b05ee24a9>
- <https://medium.com/@jillcarlson>
- <https://medium.com/@jillcarlson/crypto-is-not-an-asset-class-dd28597951b3?ref=tokendaily>
- <https://multicoin.capital/2018/07/10/the-web3-stack/>
- <https://www.sec.gov/Archives/edgar/data/1326801/000119312512034517/d287954dsl.htm>
- <https://medium.com/@placeholdervc>
- <https://www.placeholder.vc/blog/2018/5/12/decred-investment-thesis>
- <https://www.bloomberg.com/news/articles/2018-04-04/facebook-says-data-on-87-million-people-may-have-been-shared>
- <https://www.nytimes.com/2005/01/30/world/americas/venezuela-land-reform-looks-to-seize-idle-farmland.html>
- <https://www.seattletimes.com/nation-world/chvez-finishes-nationalizing-venezuela-oil/>
- <https://worldview.stratfor.com/article/venezuela-bank-nationalizations>
- https://www.imf.org/external/datamapper/NGDP_RPCH@WEO/OEMDC/ADVEC/WEOWORLD/VEN
- <https://medium.com/incerto/an-expert-called-lindy-fdb30f146eaf>
- https://en.wikipedia.org/wiki/Raison_d%27%C3%AAtre
- <https://medium.com/@TheBlueMatt>
- <https://medium.com/alpineintel/on-governance-futarchy-6a6fa2c012b>

- <https://medium.com/cryptolawreview/against-szabos-law-for-a-new-crypto-legal-system-d00d0f3d3827>

Markets Are Eating The World

By [Taylor Pearson](#)

Posted February 28, 2019

For the last hundred years, individuals have worked for firms, and, by historical standards, large ones.

That many of us live in suburbs and drive our cars into the city to go to work at a large office building is so normal that it seems like it has always been this way. Of course, it hasn't. In 1870, almost 50 percent of the U.S. population was employed in agriculture.[1] As of 2008, less than 2 percent of the population is directly employed in agriculture, but many people worked for these relatively new things called "corporations." [2]

Many internet pioneers in the 90's believed that the internet would start to break up corporations by letting people communicate and organize over a vast, open network. This reality has sort-of played out: the "gig economy" and rise in freelancing are persistent, if not explosive, trends. With the re-emergence of blockchain technology, talk of "the death of the firm" has returned. Is there reason to think this time will be different?

To understand why this time might (or might not) be different, let us first take a brief look back into Coasean economics and mechanical clocks.

In his 1937 paper, "The Nature of the Firm," economist R.H. Coase asked "if markets were as efficient as economists believed at the time, why do firms exist at all? Why don't entrepreneurs just go out and hire contractors for every task they need to get done?" [3]

If an entrepreneur hires employees, she has to pay them whether they are working or not. Contractors only get paid for the work they actually do. While the firm itself interacts with the market, buying supplies from suppliers and selling products or services to customers, the employees inside of it are insulated. Each employee does not renegotiate their compensation every time they are asked to do something new. But, why not?

Coase's answer was transaction costs. Contracting out individual tasks can be more expensive than just keeping someone on the payroll because each task involves transaction costs.

Imagine if instead of answering every email yourself, you hired a contractor that was better than you at dealing with the particular issue in that email. However, it costs you something to find them. Once you found them you would have to bargain and

agree on a price for their services then get them to sign a contract and potentially take them to court if they didn't answer the email as stipulated in the contract.

Duke economist Mike Munger calls these three types of transaction costs *triangulation*, how hard it is to find and measure the quality of a service; *transfer*, how hard it is to bargain and agree on a contract for the good or service; and *trust*, whether the counterparty is trustworthy or you have recourse if they aren't.

You might as well just answer the email yourself or, as some executives do, hire a full-time executive assistant. Even if the executive assistant isn't busy all the time, it's still better than hiring someone one off for every email or even every day.

Coase's thesis was that in the presence of these transaction costs, firms will grow larger as long as they can benefit from doing tasks in-house rather than incurring the transaction costs of having to go out and search, bargain and enforce a contract in the market. They will expand or shrink until the cost of making it in the firm equals the cost of buying it on the market.

The lower the transaction costs are, the more efficient markets will be, and the smaller firms will be.

In a world where markets were extremely efficient, it would be very easy to find and measure things (low triangulation costs), it would be very easy to bargain and pay (low transfer costs), and it would be easy to trust the counterparty to fulfill the contract (low trust costs).

In that world, the optimal size of the firm is one person (or a very few people). There's no reason to have a firm because business owners can just buy anything they need on a one-off basis from the market.[4] Most people wouldn't have full-time jobs; they would do contract work.

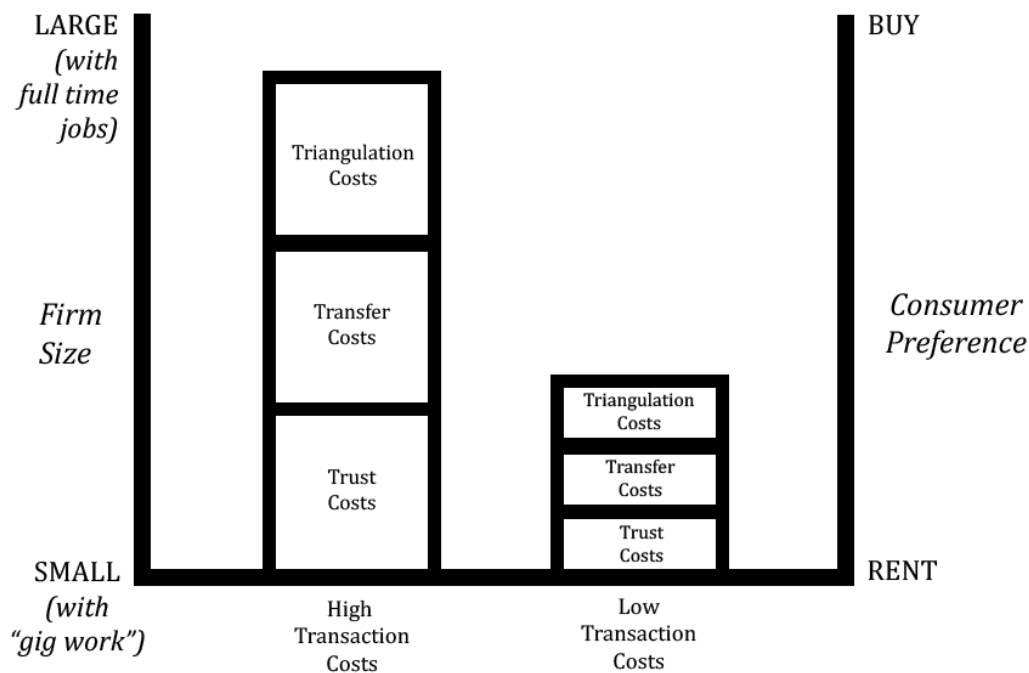
Consumers would need to own very few things. If you needed a fruit dehydrator to prepare for a camping trip twice a year, you could rent one quickly and cheaply. If you wanted to take your family to the beach twice a year, you could easily rent a place just for the days you were there.

On the other hand, in a world that was extremely inefficient, it would be hard to find and measure things (high triangulation costs), it would be difficult to bargain and pay (high transfer costs) and it would be difficult to trust the counterparty to fulfill the contract (high trust costs).

In that world, firms would tend to be large. It would be inefficient to buy things from the market and so entrepreneurs would tend to accumulate large payrolls. Most people would work full-time jobs for large firms. If you wanted to take your family to

the beach twice a year, you would need to own the beach house because it would be too inefficient to rent, the reality before online marketplaces like AirBnB showed up.

Consumers would need to own nearly everything they might conceivably need. Even if they only used their fruit dehydrator twice a year, they'd need to own it because the transaction costs involved in renting it would be too high.



If the structure of the economy is based on transaction costs, then what determines them?

Technological Eras and Transaction Costs

The primary determinant of transaction costs is technology.

The development of the wheel and domestication of horses and oxes decreased transfer costs by making it possible to move more goods further. Farmers who could bring their crops to market using an ox cart rather than carrying it by hand could charge less and still make the same profit.

The development of the modern legal system reduced the transaction cost of trust. It was possible to trust that your counterparty would fulfill their contract because they knew you had recourse if they didn't.

The list goes on: standardized weights and measures, the sail, the compass, the printing press, the limited liability corporation, canals, phones, warranties, [container ships](#) and, more recently, smartphones and the internet.

It's hard to appreciate how impactful many of these technologies has been, because most of them had become so common by the time most of us were born that we take them for granted.

As the author Douglas Adams said, "Anything that is in the world when you're born is normal and ordinary and is just a natural part of the way the world works. Anything that's invented between when you're fifteen and thirty-five is new and exciting and revolutionary and you can probably get a career in it. Anything invented after you're thirty-five is against the natural order of things."

To see how technology affects transaction costs, and how that affects the way our society is organized, let's consider something which we all think of as "normal and ordinary," but which has had a huge impact on our lives: the mechanical clock.

The Unreasonable Effectiveness of the Mechanical Clock

In 1314, The city of Caen installed a mechanical clock with the following inscription: "I give the hours voice to make the common folk rejoice." "Rejoice" is a pretty strong reaction to a clock, but it wasn't overstated, everyone in Caen was pretty jazzed about the mechanical clock. Why?

A key element of why we have jobs today as opposed to working as slaves or serfs bonded to the land as was common in the Feudal system is a direct result of the clock.

Time was important before the invention of the clock but was very hard to measure. Rome was full of sundials, and medieval Europe's bell towers where, time was tolled, were the tallest structures in town.[5]

This was not cheap. In the larger and more important belfries, two bell-ringers lived full time, each serving as a check on the other. The bells themselves were usually financed by local guilds that relied on the time kept to tell their workers when they had to start working and when they could go home.

This system was problematic for a few reasons.

For one, it was expensive. Imagine if you had to pool funds together with your neighbors to hire two guys to sit in the tower down the street full time and ring the bell to wake you up in the morning.

For another, the bell could only signal a few events per day. If you wanted to organize a lunch meeting with a friend, you couldn't ask the belltower to toll just for you. Medieval bell towers had not yet developed snooze functionality.

Finally, sundials suffered from accuracy problems. Something as common as clouds could make it difficult to tell precisely when dawn, dusk, and midday occurred.

In the 14th and 15th centuries, the expensive bell towers of Europe's main cities got a snazzy upgrade that dramatically reduced transaction costs: the mechanical clock.

The key technological breakthrough that allowed the development was the escapement.

The escapement transfers energy to the clock's pendulum to replace the energy lost to friction and keep it on time. Each swing of the pendulum releases a tooth of the escapement's wheel gear, allowing the clock's gear train to advance or "escape" by a set amount. This moves the clock's hands forward at a steady rate.[6]

The accuracy of early mechanical clocks, plus or minus 10-15 minutes per day, was not notably better than late water clocks and less accurate than the sandglass, yet mechanical clocks became widespread. Why?

1. Its automatic striking feature meant the clock could be struck every hour at lower cost, making it easier to schedule events than only striking at dawn, dusk and noon.
2. It was more provably fair than the alternatives, which gave all parties greater confidence that the time being struck was accurate. (Workers were often suspicious that employers could bribe or coerce the bell-ringers to extend the workday, which was harder to do with a mechanical clock.)

Mechanical clocks broadcast by bell towers provided a *fair* (lower trust costs) and *fungible* [7] (lower transfer costs) measure of time. Each hour rung on the bell tower could be trusted to be the same length as another hour.

Most workers in the modern economy earn money based on a time-rate, whether the time period is an hour, a day, a week or a month. This is possible only because we have a measure of time which both employer and employee agree upon. If you hire someone to pressure-wash your garage for an hour, you may argue with them over the quality of the work, but you can both easily agree whether they spent an hour in the garage.

Prior to the advent of the mechanical clock, slavery and serfdom were the primary economic relationships, in part because the transaction cost of measuring time beyond just sunup and sundown was so high, workers were chained to their masters or lords.[8]

The employer is then able to use promotions, raises, and firing to incentivize employees to produce quality services during the time they are being paid for.[9]

In a system based on time-rate wages rather than slavery or serfdom, workers have a choice. If the talented blacksmith can get a higher time-rate wage from a competitor, she's able to go work for them because there is an objective, fungible measure of time she's able to trade.

As history has shown, this was a major productivity and quality-of-life improvement for both parties.[10]

It gradually became clear that mechanical time opened up entirely new categories of economic organization and productivity that had hitherto been not just impossible, but unimaginable.

We could look at almost any technology listed above—standardized weights and measures, the sail, the compass, the printing press, etc.—and do a similar analysis of how it affected transaction costs and eventually how it affected society as a result.

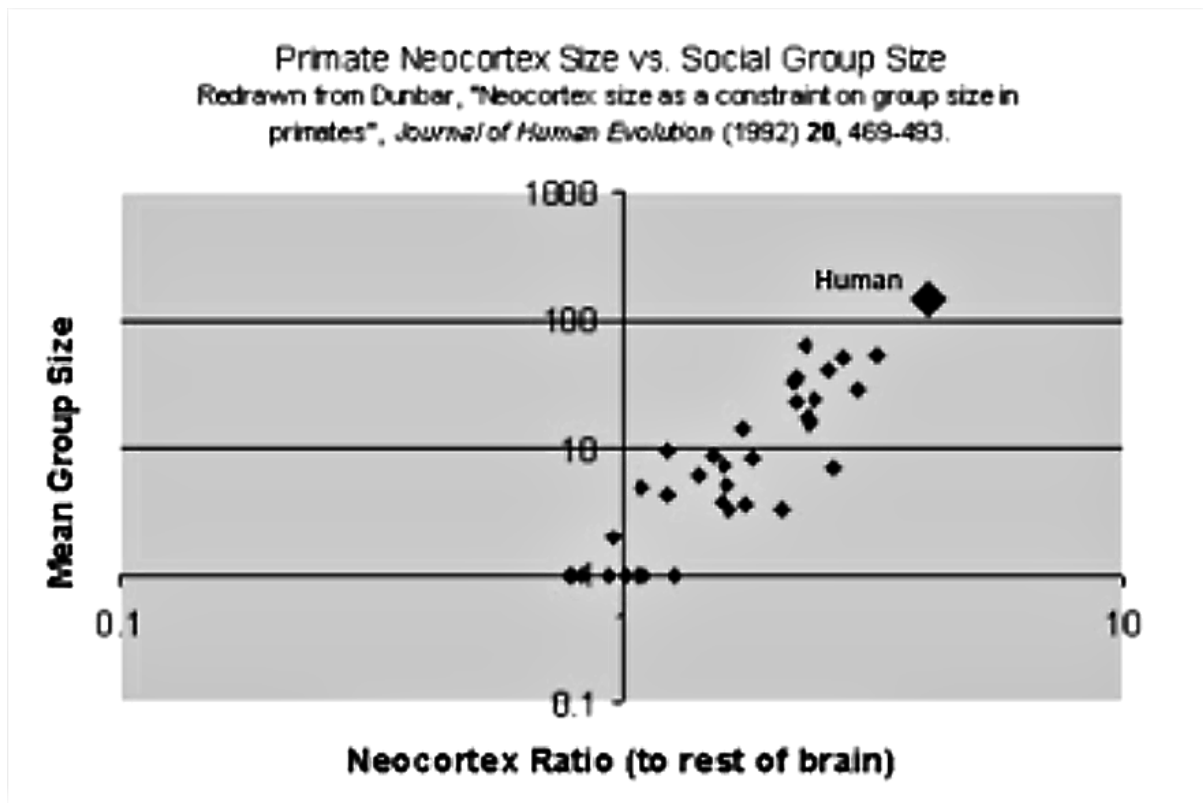
The primary effect is an increase in what we will call *coordination scalability*.

Coordination Scalability

"It is a profoundly erroneous truism, repeated by all copy-books and by eminent people when they are making speeches, that we should cultivate the habit of thinking what we are doing. The precise opposite is the case. Civilization advances by extending the number of important operations which we can perform without thinking about them." — Alfred North Whitehead

About 70,000 years ago, there were between six and ten species of the genus *homo*. Now, of course, there is just one: *Homo sapiens*. Why did *Homo sapiens* prevail over the other species, like *Homo neanderthalensis*?

Homo sapiens prevailed because of their ability to coordinate. Coordination was made possible by increased neocortical size, which led to an ability to work together in large groups, not just as single individuals. Instead of single individuals hunting, groups could hunt and bring down larger prey more safely and efficiently.[11]



The brain of *Homo sapiens* has proven able to invent other, external structures which further increased coordination scalability by expanding the network of other people we could rely on.

Maybe the most important of these was language, but we have evolved many others since, including the mechanical clock.

The increased brain size has driven our species through four coordination revolutions: Neolithic, Industrial, Computing, Blockchain.

Neolithic Era: The Emergence of Division of Labor

The first economic revolution was a shift from humans as hunter-gatherers to homo sapiens as farmers.

Coordination scalability among hunter-gatherers was limited to the size of the band, which tended to range from 15 to 150 individuals.[12] The abandonment of a nomadic way of life and move to agriculture changed this by allowing specialization and the formation of cities.

Agriculture meant that people could, for the first time, *accumulate* wealth. Farmers could save excess crops to eat later or trade them for farming equipment, baskets or

decorations. The problem was that this wealth was suddenly worth stealing and so farmers needed to defend their wealth.

Neolithic societies typically consisted of groups of farmers protected by what Mancur Olson called “stationary bandits,” basically warlords.[13] This allowed the emergence of much greater specialization. Farmers accumulated wealth and paid some to the warlords for protection, but even then there was still some left over, making it possible for individuals to specialize.

A city of 10,000 people requires, but also makes possible, specialists.

The limits of coordination scalability increased from 150 to thousands or, in some cases, tens of thousands. This was not necessarily a boon to human happiness. Anthropologist Jared Diamond called the move to agriculture “the worst mistake in the history of the human race.”[14] The quality of life for individuals declined: lifespans shortened, nutrition was worse leading to smaller stature, and disease was more prevalent.

But this shift was irresistible because specialization created so much more wealth and power that groups which adopted this shift came to dominate those that didn’t. The economies of scale in military specialization, in particular, were overwhelming. Hunt-gatherers couldn’t compete.

In the Neolithic era, the State was the limit of coordination scalability.

Industrial Era: Division of Labor Is Eating the World

Alongside the city-state, a new technology started to emerge that would further increase the limits of coordination scalability: money. To illustrate, let us take the European case, from ancient Greece to modernity, though the path in other parts of the world was broadly similar. Around 630 B.C., the Lydian kings recognized the need for small, easily transported coins worth no more than a few days’ labor. They made these ingots in a standard size—about the size of a thumbnail—and weight, and stamped an emblem of a lion’s head on them.

This eliminated one of the most time-consuming (and highest transaction cost) steps in commerce: weighing gold and silver ingots each time a transaction was made. Merchants could easily count the number of coins without worrying about cheating.

Prior to the invention of coins, trade had been limited to big commercial transactions, like buying a herd of cattle. With the reduced transfer cost facilitated by coins, Lydians began trading in the daily necessities of life—grain, olive oil, beer, wine, and wood.[15]

The variety and abundance of goods which could suddenly be traded led to another innovation: the retail market.

Previously, buyers had to go to the home of sellers of whatever they needed. If you needed olive oil, you had to walk over to the olive oil lady's house to get it. With the amount of trade that began happening after coinage, a central market emerged. Small stalls lined the market where each merchant specialized in (and so could produce more efficiently) a particular good—meat, grain, jewelry, bread, cloth, etc. Instead of having to go the olive oil lady's house, you could go to her stall and pick up bread from the baker while you were there.

From this retail market in Lydia sprang the Greek agora, Medieval market squares in Europe and, the suburban shopping mall and, eventually, the “online shopping malls” Amazon and Google. Though markets were around as early as 7th century BCE Lydia, they really hit their stride in The Industrial Revolution in the 18th century.[16]

Adam Smith was the first to describe in detail the effect of this marketization of the world. Markets made it possible to promote the division of labor *across political units*, not just within them. Instead of each city or country manufacturing all the goods they needed, different political entities could further divide labor. Coordination scalability started to stretch across political borders.

Coming back to Coase, firms will expand or shrink until “making” equals the cost of “buying.” Under this Industrial era, transaction costs made administrative and managerial coordination (making) more efficient than market coordination (buying) for most industries, which led to the rise of large firms.

The major efficiency gain of Industrial companies over their more “artisanal” forebearers was that using the techniques of mass production, they could produce products of a higher quality at a lower price. This was possible only if they were able to enforce standards throughout the supply chain. The triangulation transaction cost can be broken down into search and measurement: a company needed to find the vendor and to be able to measure the quality of the good or service.

In the early Industrial era, the supply chain was extremely fragmented. By bringing all the pieces into the firm, a large vertically integrated company could be more efficient.[17]

As an example, In the 1860s and 1870s, the Carnegie Corporation purchased mines to ensure it had reliable access to the iron ore and coke it needed to make steel. The upstream suppliers were unreliable and non-standardized and Carnegie Corporation could lower the cost of production by simply owning the whole supply chain.

This was the case in nearly every industry. By bringing many discrete entities under one roof and one system of coordination, greater economic efficiencies were gained

and the multi-unit business corporation replaced the small, single-unit enterprise because administrative coordination enabled greater productivity through lower transaction costs per task than was possible before. Economies of scale flourished.

This system of large firms connected by markets greatly increased coordination scalability. Large multinational firms could stretch across political boundaries and provide goods and services more efficiently.

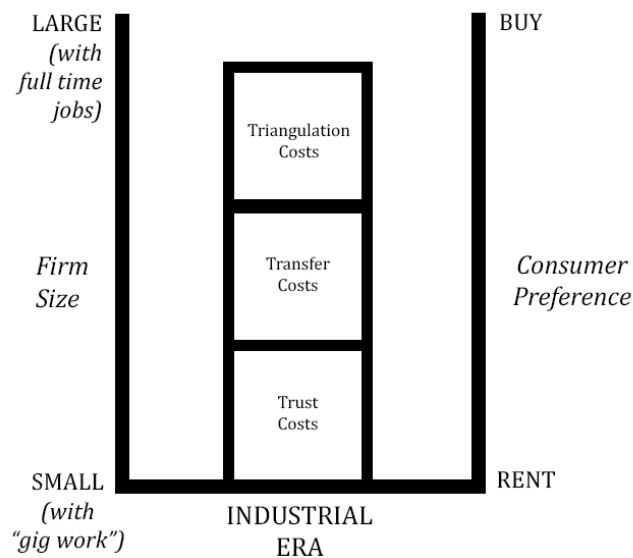
In Henry Ford's world, the point where making equaled the cost of buying was pretty big. Ford built a giant plant at River Rouge just outside Detroit between 1917 and 1928 that took in iron ore and rubber at one end and sent cars out the other. At the factory's peak, 100,000 people worked there. These economies of scale allowed Ford to dramatically drive down the cost of an automobile, making it possible for the middle class to own a car.[18]

As with Carnegie, Ford learned that supplier networks take a while to emerge and grow into something reliable. In 1917, doing everything himself was the only way to get the scale he needed to be able to make an affordable car.

One of the implications of this model was that industrial businesses required huge startup costs.

The only chance any entrepreneur had to compete required starting out with similarly massive amounts of capital required to build a factory large and efficient enough to compete with Ford.

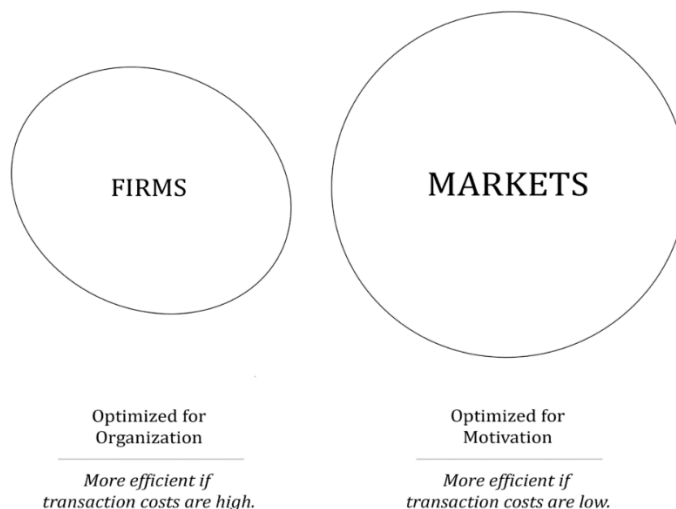
For workers, this meant that someone in a specialized role, like an electric engineer or an underwriter, did not freelance or work for small businesses. Because the most efficient way to produce products was in large organizations, specialized workers could earn the most by working inside large organizations, be they Ford, AT&T or Chase Bank.



At the peak of the Industrial era, there were two dominant institutions: firms and markets.

Work inside the firm allowed for greater organization and specialization which, in the presence of high transaction costs was more economically efficient.

Markets were more chaotic and less organized, but also more motivating. Henry Ford engaged with the market and made out just a touch better than any of his workers; there just wasn't room for many Henry Fords.



This started to dissolve in the second half of the 20th century. Ford no longer takes iron ore and rubber as the inputs to their factories, but has a vast network of upstream suppliers.[19] The design and manufacturing of car parts now happens over a long supply chain, which the car companies ultimately assemble and sell.

One reason is that supplier networks became more standardized and reliable. Ford can now buy ball bearings and brake pads more efficiently than he can make them, so he does. Each company in the supply chain focuses on what they know best and competition forces them to constantly improve.

By the 1880s, it cost Carnegie more to operate the coke ovens in-house than to buy it from an independent source, so he sold off the coke ovens and bought it from the open market. Reduced transaction costs in the form of more standardized and reliable production technology caused both Ford and Carnegie corporation to shrink as Coase's theory would suggest.

The second reason is that if you want to make a car using a network of cooperating companies, you have to be able to coordinate their efforts, and you can do that much better with telecommunication technology broadly and computers specifically. Computers reduce the transaction costs that Coase argued are the *raison d'être* of corporations. That is a fundamental change.[20]

The Computing Era: Software Is Eating the World

Computers, and the software and networks built on top of them, had a new economic logic driven by lower transaction costs.

Internet aggregators such as Amazon, Facebook, Google, Uber and Airbnb reduced the transaction costs for participants on their platforms. For the industries that these platforms affected, the line between "making" and "buying" shifted toward buying. The line between owning and renting shifted toward renting.

Primarily, this was done through a reduction in triangulation costs (how hard it is to find and measure the quality of a service), and transfer costs (how hard it is to bargain and agree on a contract for the good or service).

Triangulation costs came down for two reasons. One was the proliferation of smartphones, which made it possible for services like Uber and Airbnb to exist. The other was the increasing digitization of the economy. Digital goods are both easier to find (think Googling versus going to the library or opening the Yellow Pages) and easier to measure the quality of (I know exactly how many people read my website each day and how many seconds they are there, the local newspaper does not).

The big improvement in transfer costs was the result of matchmaking: bringing together and facilitating the negotiation of mutually beneficial commercial or retail deals.

Take Yelp, the popular restaurant review app. Yelp allows small businesses like restaurants, coffee shops, and bars to advertise to an extremely targeted group: individuals close enough to come to the restaurant and that searched for some relevant term. A barbecue restaurant in Nashville can show ads only to people searching their zip code for terms like “bbq” and “barbecue.” This enables small businesses that couldn’t afford to do radio or television advertising to attract customers.

The existence of online customer reviews gives consumers a more trusted way to evaluate the restaurant.

All of the internet aggregators, including Amazon, Facebook, and Google, enabled new service providers by creating a market and standardizing the rules of that market to reduce transaction costs.[21]

The “sharing economy” is more accurately called the “renting economy” from the perspective of consumers, and the “gig economy” from the perspective of producers. Most of the benefits are the result of new markets enabled by lower transaction costs, which allows consumers to rent rather than own, including “renting” some else’s time rather than employing them full time.

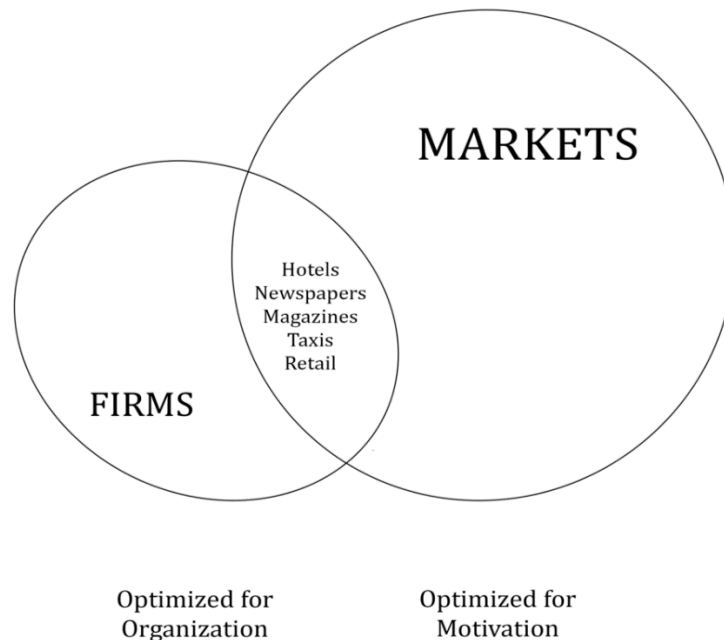
It’s easier to become an Uber driver than a cab driver, and an Airbnb host than a hotel owner. It’s easier to get your product into Amazon than Walmart. It’s easier to advertise your small business on Yelp, Google or Facebook than on a billboard, radio or TV.

Prior to the internet, the product designer was faced with the option of selling locally (which was often too small a market), trying to get into Walmart (which was impossible without significant funding and traction), or simply working for a company that already had distribution in Walmart.

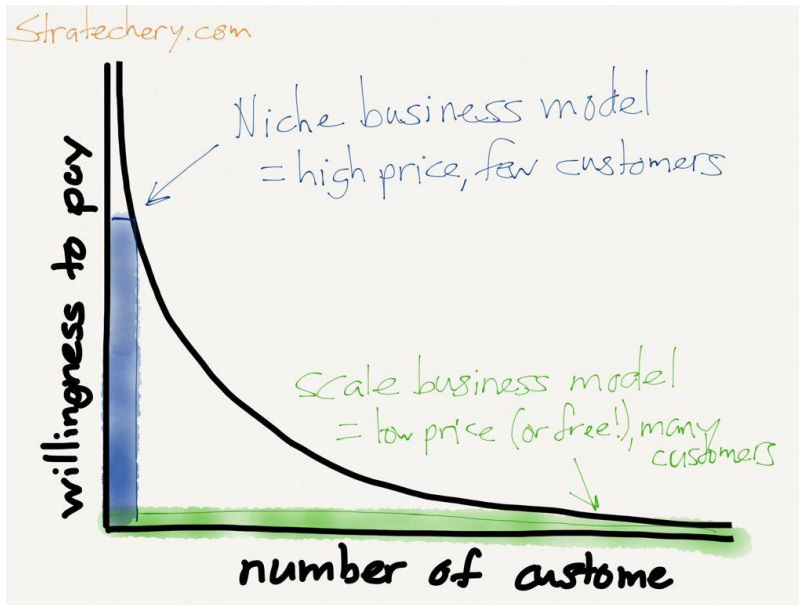
On the internet, they could start distributing nationally or internationally on day one. The “shelf space” of Amazon or Google’s search engine results page was a lot more accessible than the shelf space of Walmart.

As a result, it became possible for people in certain highly specialized roles to work independently of firms entirely. Product designers and marketers could sell products through the internet and the platforms erected on top of it (mostly Amazon and Alibaba in the case of physical products) and have the potential to make as much or more as they could inside a corporation.

This group is highly motivated because their pay is directly based on how many products they sell. The aggregators and the internet were able to reduce the transaction costs that had historically made it economically inefficient or impossible for small businesses and individual entrepreneurs to exist.



The result was that in industries touched by the internet, we saw an industry structure of large aggregators and a long tail [22] of small business which were able to use the aggregators to reach previously unreachable, niche segments of the market. Though there aren't many cities where a high-end cat furniture retail store makes economic sense, on Google or Amazon, it does.



source: stratechery.com

Before

After (Platform-Enabled Markets)

Firms

Platform

Long Tail

Walmart and big box
retailers

Amazon

Niche product designers and
manufacturers

Cab companies

Uber

Drivers with extra seats

Hotel chains

Airbnb

Homeowners with extra rooms

Traditional media outlets

Google and
Facebook

Small offline and niche online
businesses

For these industries, coordination scalability was far greater and could be seen in the emergence of micro-multinational businesses. Businesses as small as a half dozen people could manufacture in China, distribute products in North America, and employ people from Europe and Asia. This sort of outsourcing and the economic efficiencies it created had previously been reserved for large corporations.

As a result, consumers received cheaper, but also more personalized products from the ecosystem of aggregators and small businesses.

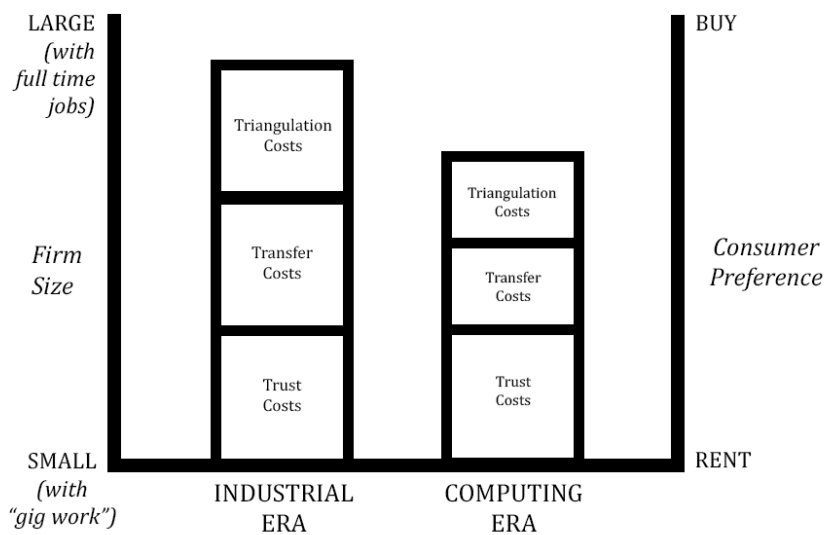
However, the rental economy still represents a tiny fraction of the overall economy. At any given time, only a thin subset of industries are ready to be marketized. What's been done so far is only a small fraction of what will be done in the next few decades.

Yet, we can already start to imagine a world which Munger calls "Tomorrow 3.0." You need a drill to hang some shelves in your new apartment. You open an app on your smartphone and tap "rent drill." An autonomous car picks up a drill and delivers it outside your apartment in a keypad-protected pod and your phone vibrates "drill delivered." Once you're done, you put it back in the pod, which sends a message to another autonomous car nearby to come pick it up. The rental costs \$5, much less than buying a commercial quality power drill. This is, of course, not limited to drills—it could have been a saw, fruit dehydrator, bread machine or deep fryer.

You own almost nothing, but have access to almost everything.

You, nor your neighbors, have a job, at least in the traditional sense. You pick up shifts or client work as needed and maybe manage a few small side businesses. After you finish drilling the shelves in, you might sit down at your computer and see what work requests are open and work for a few hours on designing a new graphic or finishing up the monthly financial statements for a client.

This is a world in which triangulation and transfer costs have come down dramatically, resulting in more renting than buying from consumers and more gig work than full-time jobs for producers.



This is a world we are on our way to already, and there aren't any big, unexpected breakthroughs that need to happen first.

But what about the transaction cost of trust?

In the computer era, the areas that have been affected most are what could be called low-trust industries. If the sleeping mask you order off of Amazon isn't as high-quality as you thought, that's not a life or death problem.

What about areas where trust is essential?

Enter stage right: blockchains.

The Blockchain Era: Blockchain Markets Are Eating the World

One area where trust matters a lot is money. Most of the developed world doesn't think about the possibility of fiat money [23] not being trustworthy because it hasn't happened in our lifetimes. For those that have experienced it, including major currency devaluations, trusting that your money will be worth roughly the same tomorrow as it is today is a big deal.

Citizens of countries like Argentina and particularly Venezuela have been [quicker to adopt bitcoin](#) as a savings vehicle because their economic history made the value of censorship resistance more obvious.

Due to poor governance, the inflation rate in Venezuela averaged [32.42 percent](#) from 1973 until 2017. Argentina was even worse; the inflation rate there averaged [200.80 percent](#) between 1944 and 2017.

The story of North America and Europe is different. In the second half of the 20th century, monetary policy has been stable.

The Bretton Woods Agreement, struck in the aftermath of the Second World War, aggregated control of most of the globe's monetary policy in the hands of the United States. The European powers acceded to this in part because the U.S. dollar was backed by gold, meaning that the U.S. government was subject to the laws of physics and geology of gold mining. They could not expand the money supply any faster than gold could be taken out of the ground.

With the abandonment of the gold standard under Nixon in 1973, control over money and monetary policy has moved into a historically small group of central bankers and powerful political and financial leaders and is no longer restricted by gold.

Fundamentally, the value of the U.S. dollar today is based on trust. There is no gold in a vault that backs the dollars in your pocket. Most fiat currencies today have value because the market trusts that the officials in charge of U.S. monetary policy will manage it responsibly.

It is at this point that the debate around monetary policy devolves into one group that imagines this small group of elitist power brokers sitting in a dark room on large leather couches surrounded by expensive art and mahogany bookshelves filled with copies of *The Fountainhead* smoking cigars and plotting against humanity using obscure financial maneuvering.

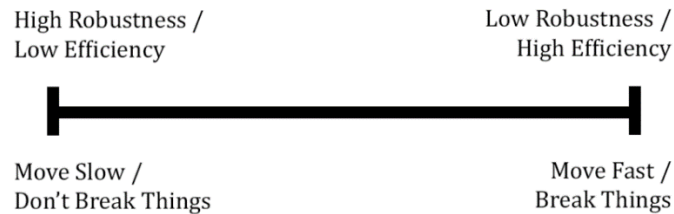
Another group, quite reasonably, points to the economic prosperity of the last half-century under this system and insists on the quackery of the former group.

A better way to understand the tension between a monetary system based on gold versus one based on fiat money this has been offered by political science professor Bruce Bueno de Mesquita: "Democracy is a better form of government than dictatorships, not because presidents are intrinsically better people than dictators, but simply because presidents have less agency and power than dictators."

Bueno de Mesquita calls this [Selectorate Theory](#). The selectorate represents the number of people who have influence in a government, and thus the degree to which power is distributed. The selectorate of a dictatorship will tend to be very small: the dictator and a few cronies. The selectorate in democracy tends to be much larger, typically encompassing the Executive, Legislative, and Judicial branches and the voters which elect them.

Historically, the size of the selectorate involves a tradeoff between the efficiency and the robustness of the governmental system. Let's call this the "Selectorate Spectrum."

The Selectorate Spectrum



Dictatorships can be more efficient than democracies because they don't have to get many people on board to make a decision. Democracies, by contrast, are more robust, but at the cost of efficiency.

Conservatives and progressives alike bemoan how little their elected representatives get done but happily observe how little their opponents accomplish. A single individual with unilateral power can accomplish far more (good or bad) than a government of “checks and balances.” The long-run health of a government means balancing the tradeoff between robustness and efficiency. The number of stakeholders cannot be so large that nothing gets done or the country will never adapt nor too small that one or a small group of individuals can hijack the government for personal gain.

This tension between centralized efficiency and decentralized robustness exists in many other areas. Firms try to balance the size of the selectorate to make it large enough so there is some accountability (e.g. a board and shareholder voting) but not so large as to make it impossible to compete in a market—by centralizing most decisions in the hands of a CEO.

We can view both the current monetary system and the internet aggregators through the lens of the selectorate. In both areas, the trend over the past few decades is that the robustness of a large selectorate has been traded away for the efficiency of a small one.[24]

A few individuals—heads of central banks, leaders of state, corporate CEOs, and leaders of large financial entities like sovereign wealth funds and pensions funds—can move markets and politics globally with even whispers of significant change. This sort of centralizing in the name of efficiency can sometimes lead to long feedback loops with potentially [dramatic consequences](#).

Said another way, much of what appears efficient in the short term may not be efficient but hiding risk somewhere, creating the potential for a blow-up. A large

selectorate tends to appear to be working less efficiently in the short term, but can be more robust in the long term, making it more efficient in the long term as well. It is a story of the Tortoise and the Hare: slow and steady may lose the first leg, but win the race.

In the Beginning, There Was Bitcoin

In October 2008, an anonymous individual or group using the pseudonym Satoshi Nakamoto sent an email to a cypherpunk mailing list, explaining a new system called bitcoin. The opening line of the conclusion summed up the paper:

“We have proposed a system for electronic transactions without relying on trust”

When the network went live a few months later in January 2009, Satoshi embedded the headline of a story running that day in *The London Times*:

“The Times 03/Jan/2009 Chancellor on brink of second bailout for banks”

Though we can't know for sure what was going through Satoshi's mind at the time, the most likely explanation based is that Satoshi was reacting against the decisions being made in response to the 2008 Global Financial Crisis by the small selectorate in charge of monetary policy.

Instead of impactful decisions about the monetary system like a bailout being reliant upon a single individual, the chancellor, Satoshi envisioned bitcoin as a more robust monetary system, with a larger selectorate beyond the control of a single individual.

But why create a new form of money? Throughout history, the most common way for individuals to show their objections to their nation's monetary policy was by trading their currency for some commodity like gold, silver, or livestock that they believed would hold its value better than the government-issued currency.

Gold, in particular, has been used as a form of money for nearly 6,000 years for one primary reason: the stock-to-flow ratio. Because of how gold is deposited in the Earth's crust, it's very difficult to mine. Despite all the technological changes in the last few hundred years, this has meant that the amount of new gold mined in a given year (the flow) has averaged between 1-2 percent of the total gold supply (stock) with very little variation year to year.

As a result, the total gold supply has never increased by more than 1-2 percent per year. In comparison to Venezuela's 32.4 percent inflation and Argentina's 200.80 percent inflation, gold's inflation is far lower and more predictable.

Viewed through the lens of Selectorate Theory, we can say that gold or other commodity forms of money have a larger selectorate and are more robust than government-issued fiat currency. In the same way a larger group of stakeholders in a democracy constrains the actions of any one politician, the geological properties of gold constrained governments and their monetary policy.

Whether or not these constraints were “good” or “bad” is still a matter of debate. The Keynesian school of economics, which has come to be the view of mainstream economics, emerged out of John Maynard Keynes’s reaction to the Great Depression, which he thought was greatly exacerbated by the commitment to the gold standard and that governments should manage monetary policy to soften the cyclical nature of markets.

The Austrian and monetarist schools believe that human behavior is too idiosyncratic to model accurately with mathematics and that minimal government intervention is best. Attempts to intervene can be destabilizing and lead to inflation so a commitment to the gold standard is the lesser evil in the long run.

Taken in good faith, these schools represent different beliefs about the ideal point on the Selectorate Spectrum. Keynesians believe that greater efficiency could be gained by giving government officials greater control over monetary policy without sacrificing much robustness. Austrians and monetarists argue the opposite, that any short-term efficiency gains actually create huge risks to the long-term health of the system.

Viewed as a money, bitcoin has many gold-like properties, embodying something closer to the Austrian and monetarist view of ideal money. For one, we know exactly how many bitcoin will be created—21 million—and the rate at which they will be created. Like gold, the ability to change this is outside of the control of a single or small group of individuals, giving it a predictable stock-to-flow ratio and making it extremely difficult to inflate.

Similar to gold, the core bitcoin protocol also makes great trade-offs in terms of efficiency in the name of robustness.[25]

However, bitcoin has two key properties of fiat money which gold lacks—it is very easy to divide and transport. Someone in Singapore can send 1/100th of a bitcoin to someone in Canada in less than an hour. Sending 1/100th of a gold bar would be a bit trickier.

In his 1998 book, *Cryptonomicon*, science fiction author Neal Stephenson imagined a bitcoin-like money built by the grandchild of Holocaust survivors who wanted to create a way for individuals to escape totalitarian regimes without giving up all their wealth. It was difficult, if not impossible, for Jews to carry gold bars out of Germany,

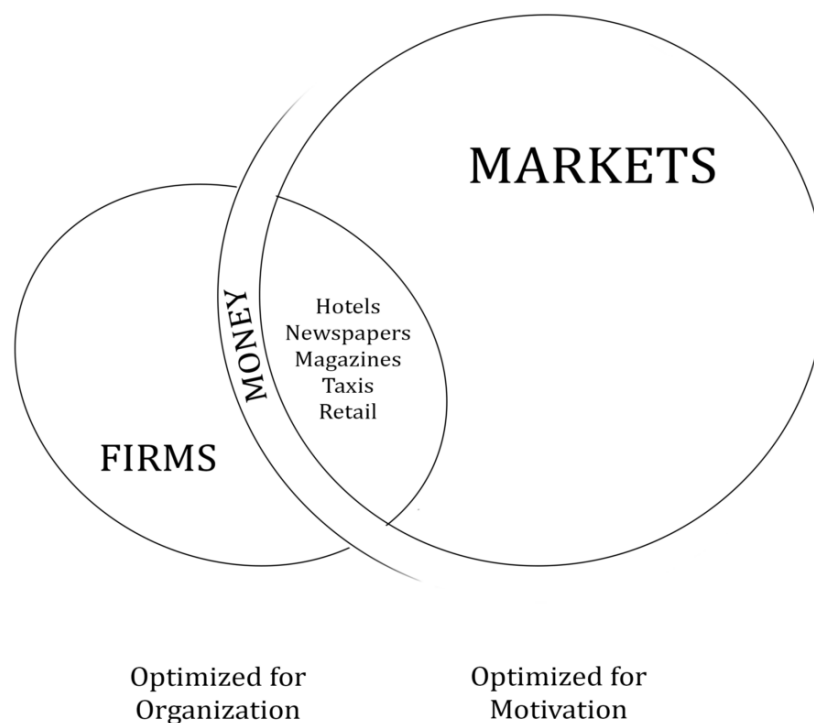
but what if all they had to do was remember a 12-word password phrase? How might history have been different?

Seen in this way, bitcoin offers a potentially better trade-off between robustness and efficiency. Its programmatically defined supply schedule means the inflation rate will be lower than gold (making it more robust) while it's digital nature makes it as divisible and transportable as any fiat currency (making it more efficient).

Using a nifty combination of economic incentives for mining (proof-of-work system) and cryptography (including blockchain), bitcoin allowed individuals to engage in a network that was both open (like a market) and coordinated (like a firm) without needing a single or small group of power brokers to facilitate the coordination.

Said another way, bitcoin was the first example of money going from being controlled from a small group of firm-like entities (central banks) to being market-driven. What cryptocurrency represents is the technology-enabled possibility that anyone can make their own form of money.

Whether or not bitcoin survives, that Pandora's Box is now open. In the same way computing and the internet opened up new areas of the economy to being eaten by markets, blockchain and cryptocurrency technology have opened up a different area to be eaten by markets: money.



The Future of Public Blockchains

Bitcoin is unique among forms of electronic money because it is both trustworthy and maintained by a large selectorate rather than a small one.

There was a group that started to wonder whether the same underlying technology could be used to develop open networks in other areas by reducing the transaction cost of trust.[26]

One group, the monetary maximalists, thinks not. According to them, public blockchains like bitcoin will only ever be useful as money because it is the area where trust is most important and so you can afford to trade everything else away. The refugee fleeing political chaos does not care that a transaction takes an hour to go through and costs \$10 or even \$100. They care about having the most difficult to seize, censorship-resistant form of wealth.

Bitcoin, as it exists today, enhances coordination scalability by allowing any two parties to transact without relying on a centralized intermediary and by allowing individuals in unstable political situations to store their wealth in the most difficult-to-seize form ever created.

The second school of thought is that bitcoin is the first example of a canonical, trustworthy ledger with a large selectorate and that there could be other types of ledgers which are able to emulate it.

At its core, money is just a ledger. The amount of money in your personal bank account is a list of all the transactions coming in (paychecks, deposits, etc.) and all the transactions going out (paying rent, groceries, etc.). When you add all those together, you get a balance for your account.

Historically, this ledger was maintained by a single entity, like your bank. In the case of U.S. dollars, the number in circulation can be figured out by adding up how much money the U.S. government has printed and released into the market and how much it has taken back out of the market.

What else could be seen as a ledger?

The answer is “nearly everything.” Governments and firms can be seen just as groups of ledgers. Governments maintain ledgers of citizenship, passports, tax obligations, social security entitlements and property ownership. Firms maintain ledgers of employment, assets, processes, customers and intellectual property.

Economists sometimes refer to firms as “a nexus of contracts.” The value of the firm comes from those contracts and how they are structured within the “ledger of the firm.” Google has a contract with users to provide search results, with advertisers to display ads to users looking for specific search terms, and with employees to

maintain the quality of their search engine. That particular ledger of contracts is worth quite a lot.

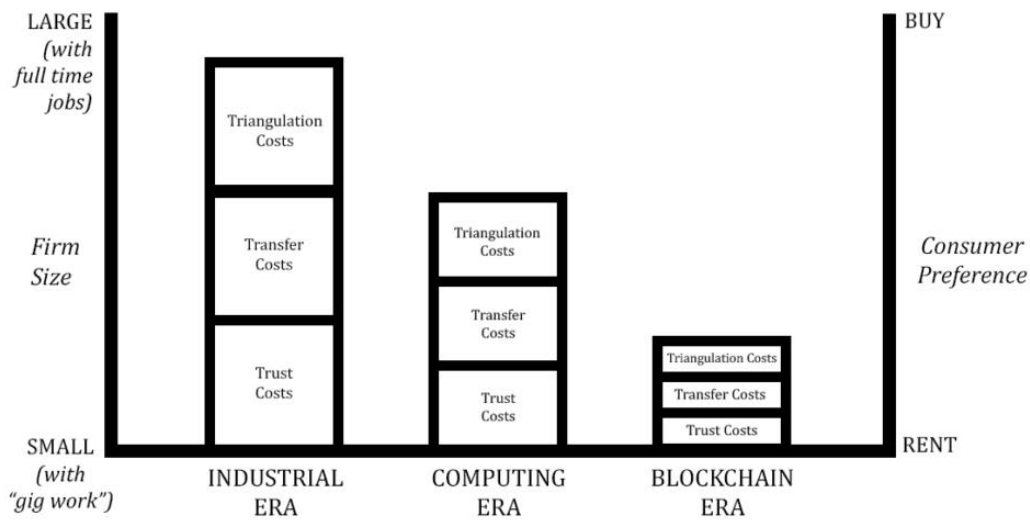
Mechanical time opened up entirely new categories of economic organization. It allowed for trade to be synchronized at great distances—without mechanical time, there would have been no railroads (how would you know when to go?) and no Industrial Revolution. Mechanical time allowed for new modes of employment that lifted people out of serfdom and slavery.[27]

In the same way, it may be that public blockchains make it possible to have ledgers that are trustworthy without requiring a centralized firm to manage them. This would shift the line further in favor of “renting” over “buying” by reducing the transaction cost of trust.

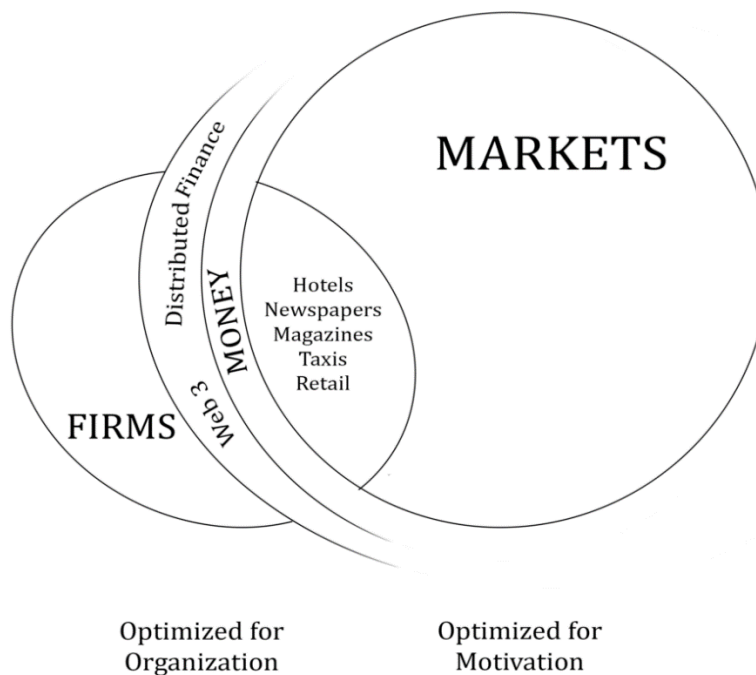
Entrepreneurs may be able to write a valuable app and release for anyone and everyone who needs that functionality. The entrepreneur would collect micro-payments in their wallet. A product designer could release their design into the wild and consumers could download it to be printed on their 3D printer almost immediately.[28]

For the first 10 years of bitcoin’s existence, this hasn’t been possible. Using a blockchain has meant minimizing the transaction cost of trust at all costs, but that may not always be the case. Different proposals are already being built out that allow for more transactions to happen without compromising the trust which bitcoin and other crypto-networks offer.

There are widely differing opinions on what the best way to scale blockchains are. One faction, usually identifying as Web 3/smart contracting platform/Ethereum, believes that scaling quickly at the base layer is essential and can be done with minimal security risk while the other groups believe that scaling should be done slowly and only where it does not sacrifice the censorship-resistant nature of blockchains (bitcoin). Just like the debate between Keynesian and Austrian/monetarist views of monetary policy, these views represent different beliefs about the optimal tradeoff point on the Selectorate Spectrum. But, both groups believe that significant progress can be made on making blockchains more scalable without sacrificing too much trust.



Public blockchains may allow aggregation without the aggregators. For certain use cases, perhaps few, perhaps many, public blockchains like bitcoin will allow the organization and coordination benefits of firms and the motivation of markets while maintaining a large selectorate.



Ultimately, what we call society is a series of overlapping and interacting ledgers.

In order for ledgers to function, they must be organized according to rules.

Historically, rules have required rulers to enforce them. Because of network effects,

these rulers tend to become the most powerful people in society. In medieval Europe, the Pope enforced the rules of Christianity and so he was among the most powerful.

Today, Facebook controls the ledger of our social connections. Different groups of elites control the university ledgers and banking ledgers.

Public blockchains allow people to engage in a coordinated and meritocratic network without requiring a small selectorate.

Blockchains may introduce markets into corners of society that have never before been reached. In doing so, blockchains have the potential to replace ledgers previously run by kings, corporations, and aristocracies. They could extend the logic of the long tail to new industries and lengthen the tail for suppliers and producers by removing rent-seeking behavior and allowing for permissionless innovation.

Public blockchains allow for rules without a ruler. It began with money, but they may move on to corporate ledgers, social ledgers and perhaps eventually, [the nation-state ledger](#).^[29]

Acknowledgments: Credit for the phrase “Markets Are Eating the World” to [Patri Friedman](#).

1. <https://www.bls.gov/opub/mlr/1981/11/art2full.pdf>
2. <https://www.bls.gov/emp/tables/employment-by-major-industry-sector.htm>
3. <http://www3.nccu.edu.tw/~jsfeng/CPEC11.pdf>
4. *There are, of course, other types of transaction costs than the ones listed here. A frequent one brought up in response to Coase is company culture, which nearly all entrepreneurs and investors agree is an important factor in a firm's productivity. This is certainly true, but the broader point about the relationship between firm size and transaction costs hold—culture is just another transaction cost.*
5. <http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/synch.html>
6. <https://en.wikipedia.org/wiki/Escapement>
7. *Fungibility is the property of a good or a commodity whose individual units are interchangeable. For example, one ounce of pure silver is fungible with any other ounce of pure silver. This is not the same for most goods: a dining table chair is not fungible with a fold-out chair.*
8. *Piece rates, paying for some measurement of a finished output like bushels of apples or balls of yarn, seems fairer. But they suffer from two issues: For one, the output of the labor depends partially on the skill and effort of the laborer,*

but also on the vagaries of the work environment. This is particularly true in a society like that of medieval Europe, where nearly everyone worked in agriculture. The best farmer in the world can't make it rain. The employee wants something like insurance that they will still be compensated for the effort in the case of events outside their control, and the employer who has more wealth and knowledge of market conditions takes on these risks in exchange for increased profit potential.

9. For the worker, time doesn't specify costs such as effort, skill or danger. A laborer would want to demand a higher time-rate wage for working in a dangerous mine than in a field. A skilled craftsman might demand a higher time-rate wage than an unskilled craftsman.
10. The advent of the clock was necessary for the shift from farms to cities. Sunup to sundown worked effectively as a schedule for farmers because summer was typically when the most labor on farms was required, so longer days were useful. For craftsman or others working in cities, their work was not as driven by the seasons and so a trusted measure of time that didn't vary with the seasons was necessary. The advent of a trusted measure of time led to an increase in the quantity, quality and variety of goods and services because urban, craftsman type work was now more feasible.
11. <https://unenumerated.blogspot.com/2017/02/money-blockchains-and-social-scalability.html>. I am using the phrase "coordination scalability" synonymously with how Nick uses "social scalability." A few readers suggested that social scalability was a confusing term as it made them think of scaling social networks.
12. 150 is often referred to as Dunbar's number, referring to a number calculated by University of Oxford anthropologist and psychologist Robin Dunbar using a ratio of neocortical volume to total brain volume and mean group size. For more see <https://www.newyorker.com/science/maria-konnikova/social-media-affect-math-dunbar-number-friendships>. The lower band of 15 was cited in Pankaj Ghemawat's [World 3.0](#)
13. <https://www.jstor.org/stable/2938736>
14. <http://discovermagazine.com/1987/may/02-the-worst-mistake-in-the-history-of-the-human-race>
15. Because what else would you want to do besides eat bread dipped in fresh olive oil and drink fresh beer and wine?
16. From [The History of Money by Jack Weatherford](#).
17. It also allowed them to squeeze out competitors at different places in the supply chain and put them out of business which Standard Oil did many times before finally being broken up by anti-trust legislation.
18. <http://www.paulgraham.com/re.html>
19. Tomorrow 3.0 by Michael Munger

20. <http://www.paulgraham.com/re.html>
21. *There were quite a few things, even pre-internet, in the intersection between markets and firms, like approved vendor auction markets for government contracting and bidding, but they were primarily very high ticket items where higher transaction costs could be absorbed. The internet brought down the threshold for these dramatically to something as small as a \$5 cab ride.*
22. *The Long Tail was a concept WIRED editor Chris Anderson used to describe the proliferation of small, niche businesses that were possible after the end of the “tyranny of geography.”* <https://www.wired.com/2004/10/tail/>
23. *From Wikipedia: “Fiat money is a currency without intrinsic value that has been established as money, often by government regulation. Fiat money does not have use value, and has value only because a government maintains its value, or because parties engaging in exchange agree on its value.” By contrast, “Commodity money is created from a good, often a precious metal such as gold or silver.” Almost all of what we call money today, from dollars to euros to yuan, is fiat.*
24. *Small institutions can get both coordination and a larger selectorate by using social norms. This doesn’t enable coordination scalability though as it stops working somewhere around Dunbar’s number of 150.*
25. *Visa processes thousands of transactions per second, while the bitcoin network’s decentralized structure processes a mere seven transactions per second. The key difference being that Visa transactions are easily reversed or censored whereas bitcoin’s are not.*
26. <https://medium.com/@cdixon/crypto-tokens-a-breakthrough-in-open-network-design-e600975be2ef>
27. <https://medium.com/cryptoeconomics-australia/the-blockchain-economy-a-beginners-guide-to-institutional-cryptoeconomics-64bf2f2beec4>
28. <https://medium.com/cryptoeconomics-australia/the-blockchain-economy-a-beginners-guide-to-institutional-cryptoeconomics-64bf2f2beec4>
29. <https://twitter.com/naval/status/877467629308395521>

The Best Time to Buy & Build Tokens

By [Chris Burniske](#)

Posted February 28, 2019

Over the last few quarters, we've watched entrepreneurs shift their fundraising focus from token-based protocols to the relative safety of equity-capitalized, cash-flow extracting businesses. Within crypto, if 2017 deal-flow was 75% token-based, 25% equity-based, then 2019 has been the inverse, and the token-based deals are continuing to slow [1].

Long run, we expect there to be [thousands of equity-capitalized businesses making use of each successful protocol](#), which means there will be more companies than protocols, and the noted inversion of deal-flow is rational. Furthermore, we should expect a reversion to the psychological safety of what's known in a time of heightened risk aversion.

That said, *just as people in 2017 regretted their 2014/2015/2016 decision to abandon bitcoin for blockchain, many people in 2021 will regret their 2018/2019/2020 decision to abandon tokens for equity*. Especially if they had a good idea but faltered due to the bearishness of the climate. This will apply to both entrepreneurs and investors, and the regret will harden conviction behind tokens over the long run.

Regret won't come because launching or investing in a successful token-based protocol is easy [2]. Candidly, launching a protocol has a greater chance of failure than launching a company, because the playbooks of protocols are being written as we speak. But the feeling of lost opportunity will arise when the protocols that become successful dwarf the scale of most companies, and people realize that many successful models were hidden in plain sight in 2018/2019/2020. When this happens, there will be a strong sense of FOMO, which is likely to bring another (better-regulated) token-boom in the middle-stage of the next bull market [3].

Frenzied booms tend to happen in the middle of crypto's bull markets due to the combination of 1) influxes of new people 2) [availability bias](#) 3) hasty expected value (EV) calculations, where $EV = \text{Probability} \times \text{Reward}$.

When new entrepreneurs and investors enter crypto in a bull market, it appears like everyone doing the "new thing" is making tons of money. They overweight the probability of the new thing succeeding (*availability bias*) and combine it with the large rewards they're witnessing. Huge expected value!

But when the bear market comes calling, these new entrants watch in despair as the probability of their “new thing(s)” succeeding plummet (the vast majority of new things will fail), and asset values fall off a cliff. Low expected value.

As the bear market drags on, new entrants’ *availability bias* switches to the much deeper mental-grooves of things they’ve seen work over long periods of time. Given crypto’s only been around for 10 years, these tend to be non-crypto native models. The path to success for proven models appears clearer to them, and while the reward may not be as astronomical, it could still be pretty good, and so the majority of new entrants set down a path that represents a reversion to the mean.

Given bull markets tend to at least double the number of participants in crypto, there are more “new people” involved at the end of a bull market than there were “old people” at the beginning—to put it bluntly, the noobs outnumber the OGs.

If the new people revert to what’s known, it swings the majority of activity in that direction, which is what we saw with “blockchain not bitcoin” in 2015, and what we’re seeing with “equities not tokens” in 2019. Meanwhile, the smaller group of committed OGs that have thought about the “new thing” for a long time will carry on with conviction because they’ve been through these cycles before, which has hardened their availability bias towards crypto-native models and weighted their EV calculations in the direction of the “new thing.”

Coming back to today, people have been shaken from the token-dream because the idea has lost social momentum, is undergoing its first *availability hardening*, and 95% of the tokens in the market don’t work. I’ll come back to the social momentum and availability hardening in a moment, but want to first underscore that many people were pointing out in 2017 that 95% of ICOs launching were opportunistic junk, and so we shouldn’t be surprised in 2019 when it turns out that 95% of the tokens in the market are indeed junk and don’t work.

But don’t let the tokens that aren’t working, and never were going to work, distract you from the tokens that were thought through thoroughly from inception and *are showing signs of working*. Roughly, I’d say there are less than 50 tokens with *real utility* in existence, placing us at < 2.5% of the tokens listed on CoinMarketCap; but 50 still provides plenty of inspiration to study and learn from.

Now to the social momentum and availability hardening of ideas in crypto. As crazy as it was, 2017 represented the mainstream birth of the idea of a token for each network. Yes, seeds of the idea were laid for years prior, but it was in 2017 that the concept blossomed to a scale where it consumed society, albeit briefly.

[As Nouriel put it](#), “It is clear by now that Bitcoin and other cryptocurrencies represent the mother of all bubbles, which explains why literally every human being I met

between Thanksgiving and Christmas of 2017 asked me first if they should buy them.” No, the mainstream didn’t grasp all the nuances and ramifications, and nor did most entrepreneurs or investors (maybe none of us did), but at the very least, many became aware.

Post the 2017 idea-frenzy and brief social momentum, *we now find ourselves in 2019 where the concept of a token for each network is going through its first serious bear market*. Tokens have lost momentum, they’re no longer cool, and if anything, the first reaction is one of skepticism. And so [useful implementations of tokens](#) are being proven right now, but to far less fanfare than 2017. The doubters have stopped paying attention, the haters have mistakenly equated depression with defeat.

But the token models that get through this bear market, and then inflect in the proximate bull market, will thereby be hardened when they reach their 2nd bear market. The process is akin to what bitcoin went through in 2014 and 2015, after its first mainstream bubble of 2013. In 2014 and 2015, bitcoin wasn’t taken for granted as something that was destined to survive in the way I see it characterized now. Instead, it was severely doubted.

But bitcoin is now taken for granted precisely because of the battle-testing it went through in 2014 and 2015 (not to mention the wild times before the mainstream was watching). Regardless of whether people stayed committed to bitcoin in 2014/2015 or jumped to blockchain-land, they all then watched what bitcoin did in 2017. *The availability bias shifted strongly towards probability of bitcoin succeeding, the indelibility of the impression weighted by the money that was made or lost.*

Committed bitcoin entrepreneurs have learned to avoid the mistake of defecting when they should be building; committed investors have learned to not divest when they should invest. While other token-based protocols have ridden a little on bitcoin’s pioneering coattails, they still have a doubt trail to trod before conviction in the underlying ideas becomes hardened (in particular, the non-PoW tokens).

So where does that leave us now? As this bear market persists, we can expect a continued shift in focus towards cash-flow extracting, equity-capitalized businesses, as teams quietly sideline plans for a token (if they ever had one). For many teams, dreams of a token won’t die entirely, they’ll instead be placed on backburners as they watch to see what cryptonetworks are gaining traction [4], and what cryptoeconomic models are being put to use [5].

When the next bull market arrives, the token-models that are providing *real utility* [6] are likely to go through another parabolic frenzy, with the fodder of speculation around radical innovation turbocharged by early-liquidity and a continued [long-bias in the cryptomarkets](#).

There will be another rush of opportunistic and poorly-thought-through launches as people scramble to make up for lost time. While capital will be plentiful again, it will be a bad time to be an entrepreneur or investor trying to do thoughtful work in the space. Quality entrepreneurs will get lost in the noise or raise too much money, which will haunt them later. Quality investors will get drunk on their own kool-aid or become jaded with the behavior they're witnessing.

But in the following bear market, builders and investors won't forget the lesson. *Availability biases* will have been hardened in favor of tokens, and there will be more competition around building and funding protocols, which is good for crypto. But in my opinion, if you have the conviction, 2019 will have been the best time to be a token builder or buyer.

Footnotes:

[1] Token-based deals can start out as an equity investment, aligning early-investors and developers for a period in what we call a *placeholder development company* (Joel will write about this more soon). But if the intent is ultimately to give investors a claim on tokens (as opposed to cash-flows), I still consider such an equity-structuring to be a token-based deal, placing it in the 25% minority of 2019.

[2] In fact, many teams and investors currently regret their 2017-token-decisions if they were made rashly and for opportunistic reasons.

[3] I disagree with many of my beloved crypto friends that say, "alts are never coming back." To the contrary, I think 2017 was likely the warm-up.

[4] Those that have already launched a cryptoasset will continue to iterate on their models. Most will fail, some will work, and those that work everyone will learn from. Relatively few, on a comparable basis, will attempt to launch tokens in this bear market, but by-and-large the attempts will be more thoughtful. One variable contributing to fewer, but more thoughtful token-launches, is that capital's harder to come by for a token team right now. Investors are asking tougher questions given the heightened perceived risk of funding protocols, leading to a more robust selection process.

[5] In the future we will see more cryptonetworks that closely follow the cryptoeconomic-playbook of other already-successful networks that are provisioning similar, but still different, services. To some extent, this pattern of behavior has happened already, first with proof-of-work, more recently with (delegated)-proof-of-stake. But thus far the strokes of imitation have been much rougher than the granularity that I think we can expect in the future.

For example, I expect the provisioning of most “compute commodities” to end up with very similar cryptoeconomic models, where there will be a *capital asset* model to coordinate supply-siders to bond their assets to provision the service (and ensure castigation should they misbehave), with rewards doled out according to some function from there. Sure, the functions will vary, as will the supply-inflation and deflation rates, but the basic principles will be *taken for granted* in a way that we almost can’t fathom now. There will be *best practices*, as opposed to *best guesses*.

[6] What will *real utility* look like? It will be cryptonetworks that take in capital and labor as inputs and spit out a novel-yet-useful service, or a service on par with that which a company already provides, but at a fraction of the cost. If the service is novel—such as the censorship-resistant digital gold that bitcoin has become—then it will get a pass on the cost-efficiency front (for now). If the service is undifferentiated from what an equity-capitalized business already produces, then the cryptonetwork will have to offer it an order-of-magnitude cheaper to get people to definitively make the switch (note that undifferentiated means the service is just as reliable, easy-to-use, interoperable, etc).

This is not to say every service will thrive when provisioned by a cryptonetwork. Only the services that thrive off decentralization, be it for cost, trust, or performance reasons, will survive over the long run. Many other services will continue to be better provisioned under an equity-model, not to mention the many companies that will build viable businesses by [amalgamating and candy-coating the underlying services](#) provided by cryptonetworks.

Links

- <https://www.placeholder.vc/blog/2018/11/30/cryptonetworks-are-not-companies>
- https://en.wikipedia.org/wiki/Availability_heuristic
- <https://www.banking.senate.gov/imo/media/doc/Roubini%20Testimony%2010-11-18.pdf>
<https://www.banking.senate.gov/imo/media/doc/Roubini%20Testimony%2010-11-18.pdf>
- <https://www.placeholder.vc/about>
- <https://twitter.com/cburniske/status/1087011245612503041>
- <https://twitter.com/cburniske/status/1055476651914600449>

Opinion: Some of the Top Cryptocurrencies Aren't Really Cryptocurrencies

By [Kyle Torpey](#)

Posted March 1, 2019

Cryptocurrency comparison websites like [CoinMarketCap](#) and [Messari's OnChainFX](#) allow visitors to look through the details of thousands of different crypto assets. From coins that run on their own blockchains to ERC-20 tokens, there is a wide variety of assets listed on these sites.

But what defines a cryptocurrency? Why isn't a virtual currency like World of Warcraft gold listed on these sites? Obviously, it would be difficult to calculate the value of all World of Warcraft gold in existence due to a lack of data around supply numbers, but another key reason this sort of virtual currency is not included on cryptocurrency comparison websites is that in-game currencies tend to be too centralized to be worth comparing to actual cryptocurrencies.

But how decentralized must a digital currency be to be considered a cryptocurrency? Bitcoin's seemingly sufficient level of decentralization and censorship resistance is what allowed it to succeed where countless other digital cash schemes failed, so this should be viewed as the interesting aspect of the technology that must be preserved. In other words, this is why we're here.

Having said that, it's unclear if a number of other top "cryptocurrencies" are more similar to Bitcoin or World of Warcraft gold.

Why Bitcoin is interesting

In Bitcoin, [Proof-of-work](#) is used to figure out who gets to add the next block of transactions to the ledger. This system is referred to as dynamic-membership multi-party signature (DMMS) in the [sidechains white paper](#). To quote the paper:

"A DMMS is a digital signature formed by a set of signers which has no fixed size. Bitcoin's blockheaders are DMMSes because their proof-of-work has the property that anyone can contribute with no enrolment process. Further, contribution is weighted by computational power rather than one threshold signature contribution per party, which allows anonymous membership without risk of a Sybil attack (when one party joins many times and has disproportionate input into the signature). For this reason, the DMMS has also been described as a solution to the Byzantine Generals Problem."

This excerpt from the sidechains white paper describes Bitcoin's key innovation: the ability to order the history of transactions without the use of known, trusted entities.

After all, [Liberty Reserve](#) and [E-gold](#) were both shut down because it was rather easy to simply target the known entities who were processing pseudonymous transactions on the internet. Bitcoin is much more resistant to regulatory attacks, which is why it is often compared to the file-sharing protocol BitTorrent.

Due to use of DMMS, Bitcoin is not issued and controlled by a specific entity. This is part of what underpins Bitcoin's "digital gold" comparison.

This is not to say there isn't plenty of room for improvement in the realm of DMMS. For example, the level of centralization found in Bitcoin mining today is [often viewed as a deterrent to the existence of secure SPV sidechains](#). Due to the current lack of privacy in Bitcoin, mining centralization also opens up the possibility of transaction censorship.

Defining a cryptocurrency

If the key breakthrough with Bitcoin was the ability for potentially-anonymous actors to order transactions and prevent double spending, then shouldn't this be the threshold by which cryptocurrencies are defined? One would think so, but some of the top cryptocurrencies today (as measured by market cap) do not meet this basic requirement.

Ripple and Stellar are the two most obvious examples of items listed on cryptocurrency comparison websites that aren't really cryptocurrencies. Both of these projects run on systems that require users to choose which entity or group of entities they wish to trust with solving the double-spending problem. As hinted at in the aforementioned sidechains white paper, these trusted entities cannot be anonymous because that opens the system up to [Sybil attacks](#).

Indeed, lists of both [Ripple](#) and [Stellar](#) validators are publicly available.

Yes, it's true that the validators in these systems are potentially dynamic, but that isn't as important as anonymity because it is the potential anonymity that allows the system to persist in the face of a worldwide government crackdown.

The level of censorship resistance available in Ripple and Stellar is an open question at this time, as these systems are likely somewhere in between Liberty Reserve and Bitcoin in this regard. The question must be asked: What would happen if criminal activity became rampant on these systems? Who would decide to publicly advertise themselves as one of the operators of the system? And if they did, how difficult would it be for various governments around the world to outlaw the system? It's not like governments don't already work together on issues like money laundering and tax evasion.

Imagine if Bitcoin was originally structured like Ripple or Stellar. What would have happened when [US Senators Chuck Schumer and Joe Manchin demanded a crackdown on Silk Road and Bitcoin back in 2011](#)? Would the peer-to-peer digital cash system still exist?

It may be true that systems like Ripple and Stellar can only provide censorship resistance for as long as the technology remains overly complex to regulators. For now, “blockchain” may be a technology that provides [regulatory arbitrage](#) through its name more than its real-world functionality.

Even some proof-of-stake systems are potentially too centralized to be considered true cryptocurrencies. EOS, which is currently the number four “crypto asset” [ranked by market cap](#) uses a system where EOS token holders effectively vote on who will be processing transactions. Much like Ripple and Stellar, EOS faces an issue where these entities cannot be anonymous. After all, [users need to know 15 of the 21 block producers aren't the same person](#).

These networks also tend to have higher costs associated with node operation (as compared to Bitcoin) due to their allowance of more on-chain activity and a general acceptance of increased resource requirements for operating a node. This has the side effect of further limiting who has the ability to order transactions on the network. [Drivechains creator Paul Sztorc has written about the cost of operating a full node as a measure of decentralization for Bitcoin](#).

A related issue previously occurred with Steem, which is another system that runs on a consensus algorithm similar to what is used by EOS. [Steemit CEO Ned Scott listed the growing cost of operating full nodes](#) as a reason the company was forced to downsize its work force last year.

A proof of stake-based system (especially one using the delegated-proof-of-stake model) that doesn't have many users, is relatively centralized in terms of coin distribution, and has a high cost of operating a full node will not be substantially different than what's offered by Ripple and Stellar.

Various stablecoins, such as Tether, [also face issues similar to what is seen in Ripple, Stellar, and EOS](#) because there needs to be some trusted entity to hold the real-world asset, such as US dollars or gold, that backs the stablecoin. Additionally, more decentralized stablecoins based on collateralized crypto assets need to have some trusted [oracle](#) or group of oracles to function properly, although projects like [Augur](#) and [Bitcoin Hivemind](#) intend to find a decentralized solution to the oracle problem.

With all of this in mind, perhaps it would be prudent for crypto asset comparison websites to create more stringent standards for inclusion, or at least make it clear that all “cryptocurrencies” are not created equal.

Update: This article has been updated on 3/4/2019 to remove a specific claim regarding the total size of the EOS blockchain from [another source that has since been further clarified](#). Additionally, the article has been updated to note that a malicious party or parties need control over 15 out of the 21 EOS block producers (rather than a simple majority) to attack the network.

Heterodox Economics and the Rise of Blockchain

By [Allen Farrington](#)

Posted Mar 2, 2019

The fastest and most decentralized build-out of infrastructure in the history of economic development is not being covered by the mainstream financial media in the slightest. Even this is a charitable summary that allows for the interpretation that they deem other news to be more important. They don't; they have no idea what is going on here or why it matters.

To whom then do we turn? I have in the past referenced Chris Dixon, Fred Ehrsam, Ben Thomson, and Marc Andreessen, and they certainly do know a thing or two. But I have a more fun idea. Satoshi Nakamoto invented blockchain based in part on wanting to disprove widespread economic delusions, by example rather than argument, and embedded in the bitcoin genesis block [a reference](#) to mainstream economists having no idea how anything really works. To stay true to this strain of autodidact arrogance I do not intend to summarise contemporary commentary on blockchain. I intend instead to dig up the work of equally arrogant autodidacts from well before blockchain existed and see what they might have to say about it.

My plan is as follows: I will review three brilliant books from decidedly heterodox economists: [Technological Revolutions and Financial Capital](#), by Carlota Perez; [Cities and the Wealth of Nations](#), by Jane Jacobs; and, [The Mystery of Capital](#), by Hernando de Soto. I will then briefly draw ties between the three, and finally I will attempt to extrapolate the thinking of all three authors to what I can only imagine will be some of the consequences of the rise of blockchain.

To the best of my knowledge, none of the three reference each other. But to my mind, they are kindred spirits, and their works complement one another wonderfully, not just in what they propose, but what they *oppose*. In all three, there is a delicious strain of contempt for the mainstream of economic thought, most of all its adoption of pseudo-mathematical reasoning rooted in physics envy. As a mathematician, I found this part of the reading experience to be particularly delightful. If physics is applied mathematics, then twentieth century economics is misapplied mathematics.

But this attitude is not just an excuse for sarcastic quips, on their part or on mine. It is precisely because these authors' thoughts are so original, so abstract, and so removed from the blind historicism of the dominant paradigms of academia that they can be so naturally extended to the next great revolution in finance, technology,

and economics. Nobel Prize winning economists call Bitcoin evil and needing to be banned, while Perez, Jacobs, and de Soto are intrigued. Stiglitz, Shiller, and Krugman are moved to whine; Perez, Jacobs and de Soto are moved to think.

So think we shall.

Technological Revolutions and Financial Capital, by Carlota Perez

This book could perhaps be thought of as a sociological theory of the interplay of capital markets and technological development. Perez uses extensive historical analysis to back up axiomatic social theorizing as to which people are likely to do what, when, and why. There are no equations, no models, and no absurd idealizations of economic phenomena that leave twenty assumptions at the door; markets are not efficient and capital is not a homogenous lump of potential utility whose price reflects its risk. Capital is wielded by different people with different bases of knowledge, objectives, opportunities and access to it in the first place. It is therefore not surprising that certain patterns tend to repeat in the financing of foundational technologies; not because the solution to the differential equation of the economy is sinusoidal, but because large enough groups of people in similar enough circumstances are relatively predictable.

Perez begins by making a distinction between financial capital and production capital, which is key in setting the stage for the emergence of a new technology. *“Financial capital represents the criteria and behaviour of those agents who possess wealth in the form of money or other paper assets. In that condition, they will perform those actions that, in their understanding, are most likely to increase net wealth.”* By contrast, *“production capital embodies the motives and behaviors of those agents who generate new wealth by producing goods or performing services.”*

We might wonder from this definition whether this is not just a verbose articulation of lenders and borrowers. In a sense it is, in accurately describing the transfer of capital, but not at all in describing the roles and behaviours of those involved. It is the role of financial capital not just to save and lend, and of production capital not just to borrow and invest. It is arguably the role of *both* to aim to seek out the best return for the very different sources of capital they control, given the very different circumstances in which they find themselves. Perez teases out how the existence of these differing aims balance and enable mere *finance* to be channeled to *production*. Her argument in essence is that this channeling is neither a smooth nor obviously rational process, but one of experimentation, discovery, and *“irrational exuberance,”* and that the stages of a capital cycle can be largely captured by observing the interaction of the two groups: *“the object here is to clearly distinguish between the actual process of wealth creation and the enabling mechanisms,*

such as finance, which influence its possibility and shape the ultimate distribution of its results.”

Perez identifies four stages interspersed with three key events. The first event is the ‘big bang’, in which the industrial potential of a new technology becomes clear. This leads to the ‘irruption phase’, in which financial capital senses the above-average returns potential of the novel production capital relative to anything else on offer and in turn gives the new technologists the means to attempt to realize the potential of their inventions.

As these above average returns become well known, we enter the ‘frenzy phase’. Nothing necessarily changes with the technological advance of the production capital, at least at first. The phase is defined by a steady decoupling of financial and production capital, that ends with financial capital run amok and a crash that forces the recoupling in the next phase. The frenzy starts from the realization that the new technology, highly returning as it is, forms only a very limited portion of the overall economy and will continue to do so for quite some time. And yet the high yields from its nonetheless rapid growth become addictive. Perez sums up with a touch of gleeful sarcasm, *“in order to achieve the same high yield from all investments as from the successful new sectors, financial capital becomes highly ‘innovative’.”*

This forces a decoupling. *“After the growing confidence in the previous phase, financial capital becomes convinced it can live and thrive on its own. Brilliant successes in a sort of gambling world make it believe itself capable of generating wealth by its own actions, almost like having invented magic rules for a new sort of economy. Production capital, including the revolutionary industries, becomes one more object of manipulation and speculation.”*

And, *“the entrepreneurs of the new firms as much as the management of the old (whether modernizing or not) are forced to do whatever is necessary to attract the players in the casino and then worry as much — or more — about the performance of their stock valuations as about their actual profits. Financial capital reigns arrogant and production capital has no alternative but to adapt to the new rules; some agents with glee, others with horror.”*

This may sound familiar to readers of, among many possibilities, *Capital Account*, by the managers of Marathon Asset Management, describing the ‘frenzy’ of the fifth technological revolution (more on what the different revolutions were shortly). *“Increasingly, companies presented investors with another measure of earnings — EBITDA, or earnings before interest, tax, depreciation and amortisation — so stripped of the ordinary expenses of business that it became known jokingly as ‘earnings before bad stuff’. Chief executives justified the massive corporate takeovers of the era on the grounds that they were earnings enhancing. They also spent hundreds of billions of dollars during this period on buying back their highly*

priced shares. Why? Because share repurchases boosted earnings-per-share (EPS). In Enron's last annual report to shareholders before its bankruptcy, the pioneering energy company claimed to be 'laser-focused on earnings per share'." Financial capital begins to treat its own numbers as a closed game, without any reference to the actual productivity of production capital. Any accounting trick to get the numbers up will do, because the numbers are no longer *representations* of what is important in the real world; only the numbers are important; the numbers *are* the real world.

Over and above simple accounting fraud, however, is the effect on production capital, which has to play to this tune whether it wants to or not. The typical example from the dot com bubble has entered folklore: add 'dot com' to your name and your stock price will quadruple overnight despite scarce other changes.

After some point of mindless asset price inflation and capital gains divorced from productivity gains, the bubble must pop. This is the second key event Perez identifies, 'the crash'. It is simple enough to grasp: financial capital has, for a long time, appreciated solely on the expectation of future capital gains, thoroughly decoupled from the real gains only production capital can bring. This cannot continue forever, and, moreover, once it starts to reverse, it will likely reverse very quickly. When it is clear that there are no capital gains to be made, the gamblers will cash out, accelerating the process of decline.

The time in between the crash and Perez's next event, 'the recomposition', will see a number of changes. The practices of financial capital will likely be reformed to protect investors from the scams that were inevitably willed up in the frenzy to meet its impossible demands. The potential of the technology will nonetheless be appreciated and industry standards and regulations will be drawn up to ensure sense and cooperation in its future deployment. But ultimately what each of these achieves is to embed this technological revolution in the economic, legal, and cultural fabric.

Perez argues that this sets the stage for a 'synergy' phase of recoupled financial and production capital and harmonious growth of both. The key to avoiding the absurdities of the frenzy, as has been established in the gap between the crash and the recomposition, is that financial capital is no longer under delusions of wealth creation. Production capital is now in control, with financial capital merely facilitating its needs. Regulation of the new industries is clear and the relevant infrastructure is understood, meaning that real long-term planning can begin. Free of the burden of ridiculous expectations for short term growth inflicted by financial capital, firms can, ironically, secure real growth in a sustainable manner. Fresh from the memory of the ruinous crash, financial capital is happy with its supporting role since the capital returns it facilitates now reflect real returns, and paper wealth is largely real wealth. Perez makes a crucial point that this phase is likely to be thought of as more harmonious than all others, since there will be a more equitable

distribution of the benefits of the new technology. Its productivity enhancement will seep into more and more industries and deliver a more evenly distributed increase in real wealth, as opposed to the prior enormous fake returns to whoever happened to arrive at the frenzy first and enormous real losses to whoever happened to arrive last.

The final phase, 'maturity', is reached only eventually and is rather slipped into without an event marking its arrival, since the new technology can only open so many investment opportunities and, as they are exhausted, returns will fall. After the prior harmony, financial capital will once again become uneasy. Guardians of pools of capital that do not return what some still remember from earlier in the cycle, or perhaps what is simply insufficient to match real liabilities, become anxious for new opportunities. It is in direct contrast to the stagnation of returns during the maturity phase that the irruption of the next cycle seems so appealing.

Although I mentioned above that economic and legal frameworks formed around the Internet following the dotcom crash, what was arguably more important was not the misery of failed investments but the experiments the failures represented and the work that went into the experimentation. In some sense, the decoupling of financial and production capital and the magnetism of transient capital returns that financial capital represented forced an enormous industrial experiment to take place. We know now that the experiment in aggregate was a fantastic success. Not only have 'Internet' companies (but what isn't these days?) created orders of magnitude more capital value than was capital wasted in irrational exuberance but, as [Marc Andreessen](#), professional baller, is fond of pointing out, [most of the ideas](#) that lost spectacular amounts of money are now the bases of healthy, profitable, growing businesses. Price charts on a shorter than deserved timescale may appear to indicate enormous waste. But the long enough timescale must include the reconciliation, the golden age, and the maturity phase; the times in which the random-seeming results of the totality of experiments drive immense productivity gains across all industries. Perez argues none would happen in the first place without the irrational exuberance of the grand experiment.

"When the economy is shaken again by a powerful set of new opportunities with the emergence of the next technological revolution, society is still strongly wedded to the old paradigm and its institutional framework. The world of computers, flexible production, and the Internet has a different logic and different requirements from those that facilitated the spread of the automobile, synthetic materials, mass production and the highway network. Suddenly, in relation to the new technologies, the old habits and regulations becomes obstacles, the old services and infrastructures are found wanting, the old organizations and institutions are inadequate. A new context must be created; a new 'common sense' must emerge and propagate."

The rewards financial capital offers in the frenzy are required for the propagation. Financial capital needs some arrogance to light the first match, but it is failing to keep this arrogance in check that eventually burns down the house.

Perez also does an excellent job of chronicling the economic history of the technological revolutions about which she simultaneously theorizes. I do not want to repeat any of this here, as any attempted simplification of this part of her work would surely reduce to an uninteresting list of events. Still, I cannot praise her enough for how well she balances the two desires. It would be both dishonest and easy to take an analysis of historical patterns, however excellent in its own right, and simply lift all and only the commonalities to form a theory that, by definition, explains everything. But she does not do this. Rather than misplaced historicism, Perez takes a philosophical approach, working from common sense definitions of financial and production capital to develop a loose theory of how they are likely to interact, within some bounds. The coupling of historical analysis is done to show that this theory seems entirely reasonable. But it is not total. Perez admits when the theory does not match history, when one cycle's historical unfolding looks quite unlike another, and when she frankly does not know the answer to some or other question posed by the approach.

Perez seems very aware that the looseness of the theory is a natural constraint of the theory describing people, at its heart. Not 'economies' or 'technologies' or 'nations', but individuals with knowledge and motivations. The only major debt she perhaps owes is to Schumpeter, whom she acknowledges throughout, explicitly pointing to the 'creative destruction' evident as one technological revolution reshapes the legacy of its predecessors, but also in its implicit methodological individualism. As I said above, it is really a sociological theory from which economic consequences follow.

Jacobs attempts something similar, if not even more dramatic. While Perez is about equally concerned with the connections between *who* drives economic progress, *how* they do it, and *why*, Jacobs is solely concerned with *where*. In this unusual interpretation, she complements Perez well. Jacob's answer is, in cities.

Cities and the Wealth of Nations, by Jane Jacobs

Jacobs' book can arguably be reduced to a single theorem, which is remarkable given the breadth of the implications she teases out. The theorem is that there is no such thing as a national economy. It is a linguistic construct, existing only as a useless and confusing taxonomical tool and not in any way reflecting the functioning of the real world. The proper object of consideration, the "*salient entity of economic life*," as Jacobs repeatedly refers to it, is the city.

Only in cities, Jacobs argues, does any meaningful economic activity take place, in that the economic environment anywhere else will be solely influenced by the

activities of cities, and never the other way around. Cities are important because they alone engage in 'import replacing'. This is the process of gradually developing the means to produce better versions of goods or services that were previously imported. Jacobs comments that, *"any settlement that becomes good at import-replacing becomes a city. And any city that repeatedly experiences, from time to time, explosive episodes of import-replacing keeps its economy up-to-date and helps keep itself capable of casting forth streams of innovative and expert work."*

What is intriguing about Jacobs' theory, and what perhaps provides a cute link to Perez, is that she rationalizes this theory almost entirely in social terms. It could be thought of as a sociological theory of *where* innovation and growth happens and why it happens there. Economic innovation happens where there is a diverse set of industrial operations active in proximity, and which export some portion of their output. Such an economic entity will still import, of course, for at least two reasons: that it is more efficient to buy the raw materials required for the specialized production than to produce them, and that the exports are ultimately exchanged for high quality specialist goods from elsewhere. But the key moments are when these imports are replaced by superior goods from within this economic unit.

It would obviously be unusual if every potential improvement to a production process was only ever discovered by precisely the people already involved in that process, and not anywhere else in the world. What happens only where there is a diversity of industrial processes is that such a discovery can immediately be put into effect; there is a ready base of potential customers given that this good is already being imported, it will be spread very quickly amongst all the different industries who could also benefit from the same innovation in their industrial processes. There are two additional sources of accelerating industrial processes that are only to be found in cities: people with experience managing this kind of enterprise and with expertise potentially relevant to it, and the availability of long-term capital commitments to scale the enterprise. The latter is particularly elusive since the savings on offer will need to come from a pool that is, in aggregate, stable and growing in order to have a suitable risk profile; in other words, they need to be sourced from a diverse and thriving economy, the likes of which are only to be found in a city.

Contrast this opportunity for innovation in a city to what would or could happen in a town with one major industry. There are no potential customers outside the industry, so there is an enormous risk of the unknown in pursuing a market for the good. There are no adjacent industries to which to spread the improvement, nor to have received it from. There are no experts in anything beyond this one industry, highly dependent on exports. And there are no pools of capital capable of long-term commitments, because the risk inherent in this economic unit are huge; if there is a wobble in the grain market, let's say, the entire economy could collapse. Meaningful innovations are

very unlikely to occur here—while they may be conceived, they will not be put to practice.

Having made the innovation, if this enterprise is truly successful it will replace its prior imports, and hence acquire the trading power to import even more specialist products that it cannot (yet) produce itself. Jacobs argues that a city may as well be defined, at least in economic terms, by its ability to replace imports:

“Whenever a city replaces imports with its own production, other settlements, mostly other cities, lose sales accordingly. However, these other settlements — either the same ones which have lost export sales or different ones — gain an equivalent value of new export work. This is because an import-replacing city does not, upon replacing former imports, import less than it otherwise would, but shifts to other purchases in lieu of what it no longer needs from outside. Economic life as a whole has expanded to the extent that the import-replacing city has everything it formerly had, plus its complement of new and different imports. Indeed, as far as I can see, city import-replacing is in this way at the root of all economic expansion.”

After dutifully, but a little drudgingly, taxonomising the variety of regional economies that exist in addition to cities and how they all interact with one another, Jacobs comes upon the concept of feedback mechanisms that mediate these interactions. One extremely important such mechanism is the valuation of the currency used to facilitate imports and exports. The problem, as throughout, is that currencies today tend to cover economic activity throughout a nation, and nations are not salient economic entities. Jacobs impudently announces that, *“today we take it for granted that the elimination of multitudinous currencies in favour of fewer national or imperial currencies represents economic progress and promotes the stability of economic life. But this conventional belief is at least worth questioning. In view of the function that currencies serve as economic feedback controls. I am going to argue that national or imperial currencies give faulty and destructive feedback to city economies and that this in turn leads to profound structural economic flaws, some of which cannot be overcome no matter how hard we try.”*

If a nation runs a deficit in its balance of payments, importing more than it exports, we might think of this as reflecting a larger supply of this currency in the market—it is being offered up for exchange for foreign currencies so import purchases can be made—than there is demand for it—foreigners wanting this currency to purchase the exports. This shift in supply and demand ought to make it cheaper relative to foreign currencies. This is all well understood.

However, Jacobs makes two important points that are less well understood. While the common mainstream response to such movements is to diagnose precisely which interventions are required to counterbalance the changes and achieve ‘stability’. But we know better by now than to countenance the mainstream,

moreover to view 'stability' as at all desirable beyond in an irrelevant aesthetic sense. We want volatility and dynamism! Jacobs argues that this change in price is a valuable feedback mechanism on the state of economic activity; the depreciated currency makes imports dearer, helping local manufacturers compete, and also makes their products cheaper for foreign buyers to export; the change in value acts simultaneously as both a tariff and an export subsidy. Moreover, it will do so for exactly as long as is needed, as is dictated by the response in economic activity to the circumstances—not by a bureaucrat or a committee.

The second problem is that nations are not salient economic entities. Unlike freakish exceptions such as Singapore, which Jacobs gives high praise and seems to have proven right in backing some thirty-five years later, most nations are a mixture of numerous salient economic entities, many or none of which may be dynamic import-replacing cities. The feedback each requires to coordinate economic activity will be dramatically different. Any institutions that obscure or distort the feedback will retard economic development, since they will broadcast incessant noise over the crucial signal, and economic energy will be misused, or not used at all where it should be. Jacobs criticizes national currencies on this account in a wonderfully vivid passage that is worth quoting in full;

"National currencies, then, are potent feedback but impotent at triggering appropriate corrections. To picture how such a thing can be, imagine a group of people who are all properly equipped with diaphragms and lungs but who share only one single brain-stem breathing centre. In this goofy arrangement, the breathing centre would receive consolidated feedback on the carbon dioxide level of the whole group without discriminating among the individuals producing it. Everybody's diaphragm would thus be triggered to contract at the same time. But suppose some of those people were sleeping, while others were playing tennis. Suppose some were reading about feedback controls, while others were chopping wood. Some would have to halt what they were doing and subside into a lower common denominator of activity. Worse yet, suppose some were swimming and diving, and for some reason, such as the breaking of the surf, had not control over the timing of their submersions. Imagine what would happen to them. In such an arrangement, feedback control would be working perfectly on its own terms but the result would be devastating because of a flaw designed right into the system.

I have had to propose a preposterous situation because systems as structurally flawed as this don't exist in nature; they wouldn't last. Nor do they exist in the machines we deliberately design to incorporate mechanical, chemical or electronic feedback controls; machines this badly conceived wouldn't work. Nations, from this point of view, don't work either.

Nations are flawed in this way because they are not discrete economic units, although intellectually we pretend that they are and compile statistics about them

based on that goofy premise. Nations include, among other things in their economic grab bags, differing city economies that need different corrections at given times, and yet all share a currency that gives all of them the same information at a given time. The consolidated information is bad specific information for them even with respect to their foreign trade, and it is no information at all with respect to their trade with one another, as opposed to their international trade. Yet this wretched feedback is powerful stuff.

Because currency feedback, at bottom, all has to do with imports and exports and the balance or lack of balance between them, the appropriate responding mechanisms for such information are cities and their regions. Cities are the specific economic units that can replace imports with their own production, and the specific units that cast up streams of new kinds of exports. It is bootless to suppose that amorphous, undifferentiated statistical collections of a nation's economies perform those functions, because they don't."

Jacobs acknowledges the historical reasons for this economically unfortunate development—little more than the vast expansion of centralised government in the late nineteenth century and the adoption of state monetarism as a tool of social control—but casts her eye wider than the immediate moment. She points firstly to city currencies (currencies of salient economic entities) being the norm in the early economic development of Europe at the end of the middle ages, beginning in Venice. Not only did Venice have a city currency, but it welcomed the simultaneous circulation of Byzantine coinage due to the bedrock of trade with the Eastern Empire, whose imports Venice slowly but surely began to replace. The Hanseatic League, a federation of German and Baltic cities that drove the economic development of northern Europe, following in Venice's wake, had no league currency but allowed cities to mint their own, subject to valuable feedback from volatile intercity trade.

But Jacobs also holds out hope for the future. With incredible prescience—this being 1984—she comments on the possibility of a future multiplication of currencies that,

"the technical difficulties and inconveniences that would entail are surmountable, increasingly so with the aid of computers, instantaneous communications systems and such devices as credit cards which — even in their current rudimentary and limited uses — are already convenient for simultaneous transactions involving diverse currencies. On my card I can order, say, books from London payable in pounds, shirts from the Boston city region payable in U.S dollars, and garden seeds payable in my own currency, Canadian dollars, all the transactions being equally convenient as far as I am concerned."

It will not surprise the reader that this insight will be returned to below.

Since Jacobs can't resist the occasional dig at mainstream economics, I don't feel so bad about having this same instinct. Lest the reader think I had discarded this guilty pleasure in the introduction, I will conclude the discussion of Jacobs with the final paragraph from the first chapter, itself hardly more than 20 pages of mocking the then-state-of-the-art:

"One thing we do know by now because events have rubbed our faces in it: it would be rash to suppose that macro-economics, as it stands today, has guidance for us. Several centuries of hard, ingenious thought about supply and demand chasing each other around, tails in their mouths, have told us almost nothing about the rise and decline of wealth. We must find more realistic and fruitful lines of observation and thought than we have tried to use so far. Choosing among the existing schools of thought is bootless. We are on our own."

I couldn't agree more, Jane. Whatever might Hernando think?

[The Mystery of Capital](#), by Hernando de Soto

Why capitalism triumphs in the West and fails everywhere else, the subtitle of this book, is an excellent description of its thesis. Capitalism often fails outside the West, proposes de Soto, because the framework of broadly unregulated marketplaces is necessary for economic development, but not sufficient. Also necessary, and in a sense anthropologically prior, is a well-documented and well understood institution of private property. Many countries outside the West that attempted nominally economic capitalistic reforms failed to realize anything like the expected gains in productivity because although their citizens could in theory access free markets, they were strongly incentivized to conduct their economic activity outside the law. This was because, in one form or another, it was needlessly difficult to ascertain legal ownership of assets and easier to abide by extralegal social conventions regarding asset ownership.

The book is impressive not for the complexity of its reasoning but for the lengths gone to in order to demonstrate to a desirable degree that the reasoning is on the right track. De Soto and his team of researchers gathered copious data from Cairo, Lima, Manila, Port-au-Prince, and Mexico City to try to assess both the difficulties of formal asset ownership, and the potential value of the assets pushed outside formal systems by these difficulties.

They found that in Peru, it takes 5 separate procedures to legally acquire a home, and that the first of these procedures involves 207 steps and 21 government agencies. De Soto's team spent six hours a day on this task and completed in 289 days later. In Egypt, somebody wanting to legally register a lot on state-owned desert land would have to go through 77 steps across 31 agencies, in a process that could take between 5 and 14 years. Similar stories abound outside the West, with the obvious result that

virtually none of the poor bother to opt into the legal framework for asset ownership, preferring to abide by local customs instead. De Soto elaborates that,

“... in every country we investigated, we found that it is very nearly as difficult to stay legal as it is to become legal. Inevitably, migrants do not so much break the law as the law breaks them. In 1976, two-thirds of those who worked in Venezuela were employed in legally established enterprises; today the proportion is less than half. Thirty years ago, more than two-thirds of the new housing erected in Brazil was intended for rent. Today, only about 3 percent of new construction is officially listed as rental housing. To where did that market vanish? To the extralegal areas of Brazilian cities called favelas, which operating outside the highly regulated formal economy and function according to supply and demand. There are no rent controls in the favelas; rents are paid in US dollars, and renters who do not pay are rapidly evacuated.”

The stifling conditions in the formal economy push more and more entrepreneurial energy into the extralegal sector. De Soto's team estimated how much value was trapped in these 'shadow economies'. Confining the search solely to real estate, they found that in Manila, for example, the extralegal sector held \$133bn of value, or four times the market value of all publicly listed companies in the Philippines, and fourteen times the foreign direct investment in the preceding 25 years. In Port-au-Prince, the informal sector held 97% of all property, valued at \$5bn, or over 158x all foreign direct investment in Haiti, ever.

While these figures are staggering, we might wonder why these circumstances are even so bad, if there appears, after all, to be a thriving free market outside the meddling reach of the state. To rebut this fallacy, De Soto teases at an important economic principle throughout the book. Contrary to a variety of naïve popular conceptions, the driving force of free markets is not markets, nor money nor even assets, but *capital*. By which we must mean something less material than any of the former; a kind of economic potential energy stored in the transformation of materials into higher and higher forms of complex good, but always ready to be rereleased to work again the same process of transformation. Seen this way, capital is not any particular thing or even behaviour—it can exist only as an emergent property of a social system in which the exchange of shares of ownership of private assets is seamless. Clearly 'private assets' is a complex social construction, and even more complex still is 'shares' of assets, and so we quickly realize that clear representational systems matter as much to productivity under capitalism as does 'freedom', if not more so. Where de Soto studies, the poor lack neither assets nor free markets, but representational systems to realize the capital in these assets in markets. This is why these staggering figures represent such a tragedy: this value cannot be put back to productive work. All this capital is dead.

I will mention two further points before moving on. The first is a call to humility on the part of 'the West' that de Soto takes great care to make and that it would be unfair to leave out here. Though he extols 'the West' frequently, de Soto is careful to emphasize that this is first of all based on the economic state of affairs at the time of writing, which of course has been vastly different in the past and may well be in the future. But more importantly that his own partial theory as to why this is the case isolates the representational tools that gave rise to such circumstances as of the utmost importance and of no essential connection to those who discovered them:

"Throughout history people have confused the efficiency of the representational tools they have inherited to create surplus value with the inherent values of their culture. They forget that often what gives an edge to a particular group of people is the innovative use they make of a representational system developed by another culture. For example, Northerners had to copy the legal institutions of ancient Rome to organise themselves and learn the Greek alphabet and the Arabic number symbols and systems to convey information and calculate. And so, today, few are aware of the tremendous edge that formal property systems have given Western societies. As a result, many Westerners have been led to believe that what underpins their successful capitalism is the work ethic they have inherited or the existential anguish created by their religions — in spite of the fact that people all over the world all work hard when they can ... Therefore, a great part of the research agenda needed to explain why capitalism fails outside the West remained mired in a mass of unexamined and largely untestable assumptions labelled 'culture,' whose main effect is to allow too many of those who live in the privileged enclaves of this world to enjoy feeling superior."

Secondly, lest the reader think I had let up poking fun at mainstream economics, I will conclude this section with the same quote de Soto uses to begin *The Mystery of Capital*, from an address by the great (and heterodox) Ronald Coase:

"Economics, over the years, has become more and more abstract and divorced from events in the real world. Economists, by and large, do not study the workings of the actual economic system. They theorize about it. As Ely Devons, an English economist, once said at a meeting, "If economists wished to study the horse, they wouldn't go and look at horses. They'd sit in their studies and say to themselves, 'What would I do if I were a horse?'" And they would soon discover that they would maximize their utilities."

The Threads of Heterodox Economics

Given three works, all on the same broadly defined topic, and all wonderfully original, it is surely possible to draw many more connections than I intend to here. This will be a short section, and I do not so much intend to draw parallels in economic theory as in methodology and intellectual outlook. The allure of public blockchains is that to a

large extent they demand their own economic theory, which we can only hope to craft from first principles by teasing out the best of these three authors' first principles approaches.

Firstly, none of the three ever discuss static equilibria. They are not interested in describing precisely how things are at a given moment, but rather how things change. They are interested solely in causation. They understand that economic phenomena are causal processes driven by the behavior of individual people. People are not static. They have motivations and goals. They act. They are *alive*. There is no static human who can be mathematically described without reference to time.

Largely for this reason there is not a single equation across the three books. The argumentation is verbal. The reasons given for why things happen are the reasons the people doing those things acted in the way they did. Perez describes the interactions of people at the verge of financial and production capital. Jacobs describes the interactions of people with their physical environment. De Soto describes the interaction of people with agents of the law. People are messy. They *can* be described, but not with equations.

This basis of understanding lends itself naturally to a proper, we might say *Hayekian*, appreciation of what markets really are: engines of coordination of dispersed knowledge and desires. There are no static equilibria because competition is a process, not a state. We can try to grasp how markets work in the abstract, but if we lose our intellectual humility and suppose we can understand a given market *entirely* and *in its particulars*, then we must not understand markets in the first place. That twentieth century economics largely became self-indulgently enamored with the opposite view—that every snapshot of time can be plotted on a graph and all economic data gathered and understood in its totality—explains the disdain across all three for the mainstream. Since the mainstream largely disdains public blockchains (to the extent they understand them at all) we are in a good place to continue.

Blockchain and the Tying of the Threads

There is a straightforward appeal to Perez in the context of blockchain in explaining the bubble of 2017 and the worthwhile done since. I won't rehash it here however as I think it is pretty obvious and have nothing to add. One thought I have had, however, is that it is possible that this technology will provide an exception to Perez's theory in some respects, but not all, insofar as it being baked into the technology itself that anybody can become financially involved without much intermediation—certainly a tiny amount relative to traditional securities. I think this goes a long way to explain the magnitude of 2017, which in some respects truly was a bubble like no other. What I wonder, though, and don't have a good answer to, is whether this breaks the sociological thesis that relies on financial capital being institutionalized to some or

other extent. This space may come to have heavy institutional involvement one day, but only by coincidence, not design, as for all other investable securities. But I really don't know, so I'll leave that one for now.

What I think is actually the most interesting to observe now is the extent to which this potentially problematic area is being addressed. You may or may not believe in the likelihood of eventual institutional involvement. But a necessary precondition, which is as a matter of fact being worked on by many brilliant people who clearly do think it is likely, is both operational infrastructure to enable it within that environment. We also clearly need a regulatory environment that treats it as clearly as it does other asset classes, given that clearly defines the opportunity cost of financial capital that may be allocated here.

What is encouraging, however, is that we have certainly had one frenzy, irruption, and crash in 2017, and it seems to have played out much as Perez would have predicted. Financial capital (with a mildly altered definition) ran amok, production was helpless to prevent it, paper gains enticed dumber and dumber money, so dumb that even outright scams became worthwhile endeavours, etc. etc., and then it all collapsed. We are now in a phase in which financial capital has been chastened and tamed, timeframes have been reset for the long term, and real wealth creation can be driven by people who know what they are doing. I certainly hope we don't have to go through this again, but it strikes me as fantastic evidence in favour of Perez's overall approach. This is the first technological revolution since her work, and her theory works (nearly) perfectly as an explanatory tool.

Jacobs, we recall, is primarily interested in where economic activity takes place, and what regions it is sensible to describe as *salient economic entities*. 'Nations', she argues, are rarely good examples, but cities almost always are. Not to criticize Jacobs at all, as it would be pointlessly anachronistic, but I think that the existence and proliferation of essentially digital goods throw this model into question, and that resolving this novel tension leads naturally to the best way to think about blockchain. For example, does the economic activity that happens through Google all 'happen' in Mountain View, California? In a sense, yes, but in a far more obvious sense, no. Google's services are digital and very barely able to be defined in a traditional physical sense. Unlike even Amazon, which is a marvel of digital engineering but whose end product is clearly Alice in place A selling a widget to Bob in place B, it's not entirely clear how to make such definitions for Google. (which is the legal basis for its tax-scams-in-all-but-actuality)

Blockchains take this to its extreme because there isn't even a corporation involved. In some respects, it makes a lot of sense to think of blockchains as *actually being* corporations; clearly not legally, but in that they are associations of individuals contributing to a common enterprise that itself is clearly acting as a discrete unit and according to a charter. This is an area of thought that is still very much developing

and I don't want to send the reader too far down the rabbit hole against their will, but it seems to make sense to a lot of people to treat blockchains as, additionally, closed economies for a single digital service with digitally native currencies, and with on ramps to other digital assets and, at the edge of the system, to fiat currency. Where further to go with this observation is a matter of intense debate that need not concern us here, but it is however clear that they are in no way physical. It's a bit like asking, *where is BitTorrent?* The only sensible answer is, *on the Internet*, which may or may not register with what was expected by the questioner.

Regardless of any further philosophical interpretations, it is clear that this exclusively online activity constitutes economic productivity that it makes no sense to ascribe to the US or France or Bolivia or wherever. The only sense in which it makes sense to do so for Google is that the operational backend of Google is highly centralized and has a corporation built around it in order to be allowed to be a profitable corporation and be protected by law. It is a little torturous, but it is not completely nonsensical to consider Google's economic activities as having a geographic footprint. But public blockchains ought to have no reverse engineering to tie them to a physical location—whether this is true in fact is a matter of degree and debate. But in their purest form, it arguably *only* makes sense to consider them as Jacobs' *salient economic entities*.

This leads to probably Jacobs' most interesting argument—that of the feedback metaphor. I don't want to speculate on precise technical visions, lest we fall into yet more rabbit holes, but suffice it to say that it is clearly desirable that as many blockchains as possible will be capable of interoperability. We needn't even think too hard about what this might mean beyond an analogue of using Facebook to log into Spotify and using Spotify to post on Facebook. Those two networks are 'interoperable' under a suitably light interpretation. So, hopefully, will be blockchains, under an interpretation that is actually more rigorous. What is potentially fascinating, however, is that this interoperability will not be on the basis of corporate agreements, but rather of automated exchange of their native currencies. Given this will be inherently digital it will ideally be fairly seamless also. Therefore, we might think, we will get exactly the kind of dynamic feedback system for these salient economies that Jacobs craved in real life, and bemoaned the structural imposition of national currencies for non-salient economic entities as preventing. Economists might even be able to observe, for the first time in hundreds of years, a genuinely free market for money spontaneously emerging, unbounded by sovereign constraints.

Finally, to de Soto. The obvious instantiation of his work in this realm is in tokenizing at the very least real estate, but ideally as much 'property' as possible. It doesn't take much to realise how representational systems would be vastly improved under such a system, from which the rest of de Soto's argument follows. This would 'enliven' multitudes of 'dead capital', and bring about enormous trade and wealth on the back of what is really little more than altering incentives. This is well researched and argued elsewhere and I have little to add but approval.

However, I think there is a more interesting line of de Soto's thought to follow in this context. De Soto's core thesis is sociological rather than economic; contrary to popular conception, law is an exercise in engineering, not in morality. If it is engineered poorly—immorally or otherwise—people will simply ignore it. But the law is also potentially enabling, and so effective engineering ought to be the goal, since the opportunity cost is potentially enormous. People can 'ignore' stupid or unjust laws regarding capital accumulation by creating shadow economies, but not by creating real economies. There is an implicit loss even in the use of the word 'shadow'. It is less real.

The same will be true with the economic potential of blockchain. It exists. It works. It isn't going away. And so, lawmakers have a choice. They can engineer legal frameworks that enable productivity, capital accumulation, wealth and wellbeing using this incredible technology. Or they can be stupid and unjust and create shadow economies at enormous opportunity cost.

I have never had the pleasure of any of their company or correspondence, but here is what I imagine each of my heterodox heroes would say:

Jacobs would advise to take these seriously as salient economic entities and allow their development as highly dynamic systems of information feedback. Do not force them into any previous paradigms because it almost certainly won't work. Perez would encourage governmental leadership to facilitate a move past the crash, no less to prevent another. Let financial capital be involved but not in control. Perez, in other words, would make the case for effective integration of the technology into the mainstream. De Soto would warn of what would happen if we fail to: shadow economies will develop at enormous opportunity cost to the wellbeing of all mankind. If they would have said this, then I would agree.

But most importantly, all would be skeptical of mainstream economists. Unfortunate as it is, this is invariably a good idea. After all, so was Satoshi, one of the most heterodox economists of all time.

follow me on Twitter @allenf32

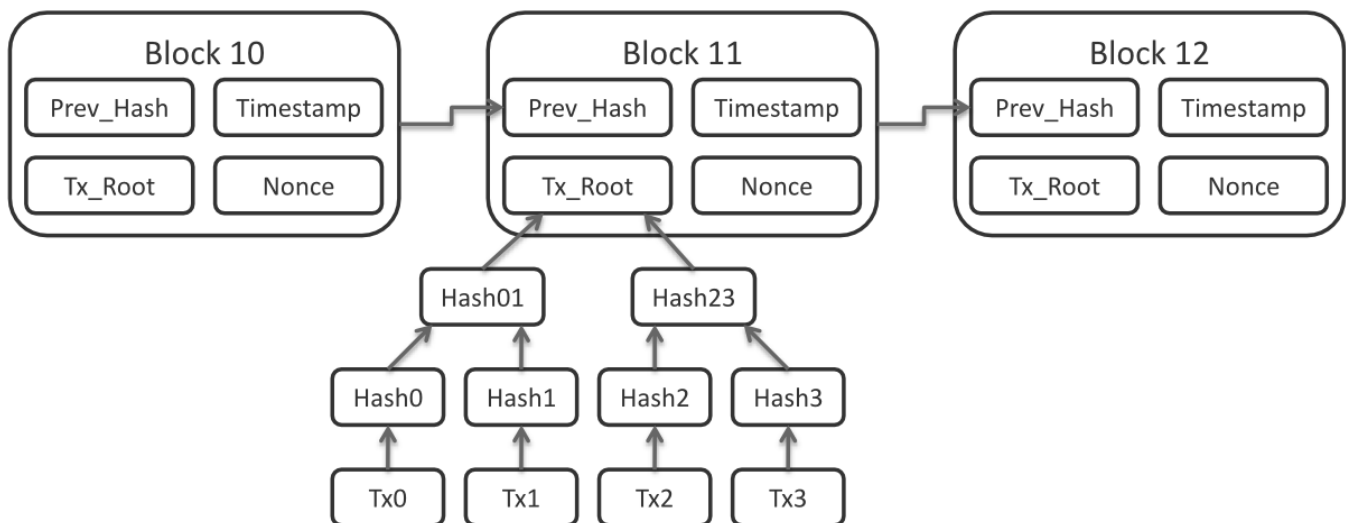
Bitcoin Timestamp Security

By [Jameson Lopp](#)

Posted March 3

Bitcoin is often referred to as a secure timestamping service. We never had a global record of truth with trustworthy timestamps, so how did this come about? It's generally due to Proof of Work being combined to a few simple rules by which miners must abide. The primary functions of miners are to:

- Take unordered unconfirmed transactions and put them in a specific order
- Bundle up the transactions into a valid container (block)
- Timestamp the block within an acceptable range of time



This final attribute is what enables Bitcoin to have a controlled release of the supply of bitcoins. Otherwise Bitcoin would suffer from rapid inflation whenever the hashrate increased. But it turns out that this attribute assigns quite a bit of utility to the Bitcoin protocol and also makes it possible for folks to [use Bitcoin as a data anchor](#) for other services. Because we have reasonably strong assurances that timestamps fall within a given range and we have mathematical assurance of the amount of energy required to rewrite the blockchain history, Bitcoin provides a sound anchor for timestamping of data. But how reliable is it?

Bitcoin's Timestamp Flexibility

In order for the time field of a block header to be considered valid by nodes it must meet two criteria:

1. Be less than [2 hours in the future](#) from your computer's current time

2. Be [greater than the median timestamp](#) of the [past 11 blocks](#)

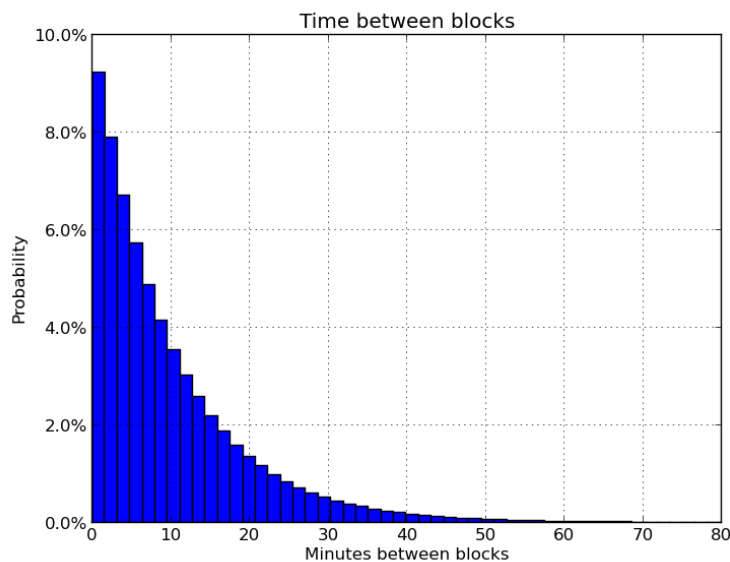
The first rule makes sense—we obviously don’t want anyone claiming to be from the future and it’s very easy for nodes to reject such claims because we’re all in general agreement about what time it currently is. There are a variety of ways that one can check the current time, though a very popular means of computers syncing their clocks is via the [Network Time Protocol](#).

However, ensuring that the time isn’t too far *before* a sensible point is harder. This is because we can’t assume that a node is validating the block anywhere near the time it is initially created. Nodes need to be able to leave and rejoin the network for any reason or no reason. A node that was too far behind the tip of the chain would start rejecting historical blocks if they had to be created within a few hours of the current time.

*“Nodes can leave and rejoin the network at will, accepting the proof-of-work chain as proof of what happened while they were gone.” —
Satoshi Nakamoto, Bitcoin Whitepaper*

Perhaps counterintuitively, there is no rule requiring that a block’s timestamp has to be *after* the timestamp of the previous block. If you think about it, such a rule could cause problems—if a miner created a block with a timestamp nearly 2 hours in the future, the next block would also have to be far in the future—it would be harder for other miners to self-correct the median time of the past 11 blocks.

Also, recall that while blocks are expected to be produced about every 10 minutes, there is no real guarantee. Blocks could range from anywhere from several milliseconds to several hours apart. While the expected median time of the past 11 blocks should be 1 hour ago, it could be far more or far less.



14 Source: <https://en.bitcoin.it/wiki/Confirmation>

Pushing the Window

If you think about how an adversary might try to expand the acceptable timestamp window, it's pretty clear that no adversary will be able to push the timestamps to be more than 2 hours in the future, no matter how much hashpower they have. However, an attacker with sufficient hashpower could put some drag on the progression of "bitcoin time" by only minting blocks with timestamps that are barely valid—that are just one second after the median time of the past 11 blocks.

Are there incentives to do this? In the extreme case a "time warp attack" offers short term financial incentives that we'll discuss later. It's less clear what incentives may exist for only dragging the timestamps by a few hours here and there. Though considering that other protocols can be built on top of Bitcoin (such as Lightning Network) and can involve [time locks](#), there could be other protocols in the future that can be gamed by slowing the progression of timestamps on the blockchain.

Hashpower Time Dragging

Since the earliest valid block time is based upon the median time of the past 11 blocks, an adversarial miner needs to generate a lot of blocks in order to induce any noticeable drag on the MTP.

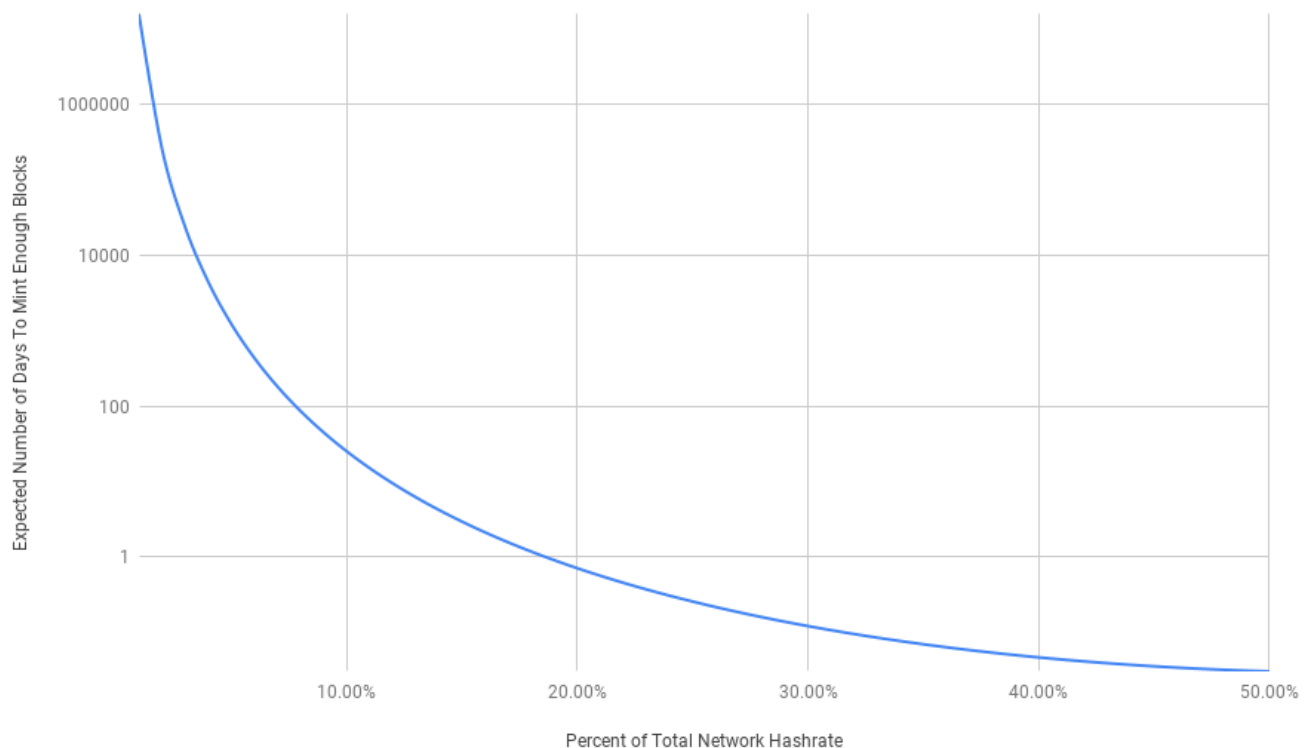
Let's assume a situation where all miners are roughly in sync via NTP but there is one adversarial miner who is trying to drag the median time of the past 11 blocks as much as possible.

One point is quite clear: it was a smart [decision by Satoshi](#) to use the median timestamp of the past 11 blocks rather than the average, as average would be more manipulable. Another way to think of “median time past” is that it basically means the timestamp of the 6th most recent block if all of the timestamps are in order. If they aren’t, the algorithm just re-orders them. As such, *if you want to have a non-negligible effect on this value* you need to have solved 6 of the past 11 blocks. In order to sustain such an attack you’d need 55% hashpower, at which point one of the main assumptions of Bitcoin’s thermodynamic security breaks down. But a miner with less hashpower *could* still achieve this on occasion if they have a streak of luck.

How hard is it to find 6 out of 11 blocks? Well, the chance that a given miner will solve the next block is basically the same as their percentage of the total network hashrate. Thus, if you only have 1% of the hashrate (which is still quite a lot) then your chance of minting 6 out of any 11 contiguous blocks = $(0.01^6 * 0.99^5) * (11! / (5! * 6!))$ = about one in 2 billion. If you maintained 1% of the hashrate then the expected number of blocks that would need to occur before you found 6 out of 11 would be over 43,000 years.

A more generalized formula for the expected wait time to pull off a successful time drag attack would be:

$$(1 / (462 * (\% \text{ hashrate}^6 * (1 - \% \text{ hashrate})^5))) / 144 \text{ blocks/day} = \# \text{ days}$$



As we can see, for attackers to conduct such an attack on any meaningful timescale then they'd need a decent size mining pool with at least 10% of the total network hashrate.

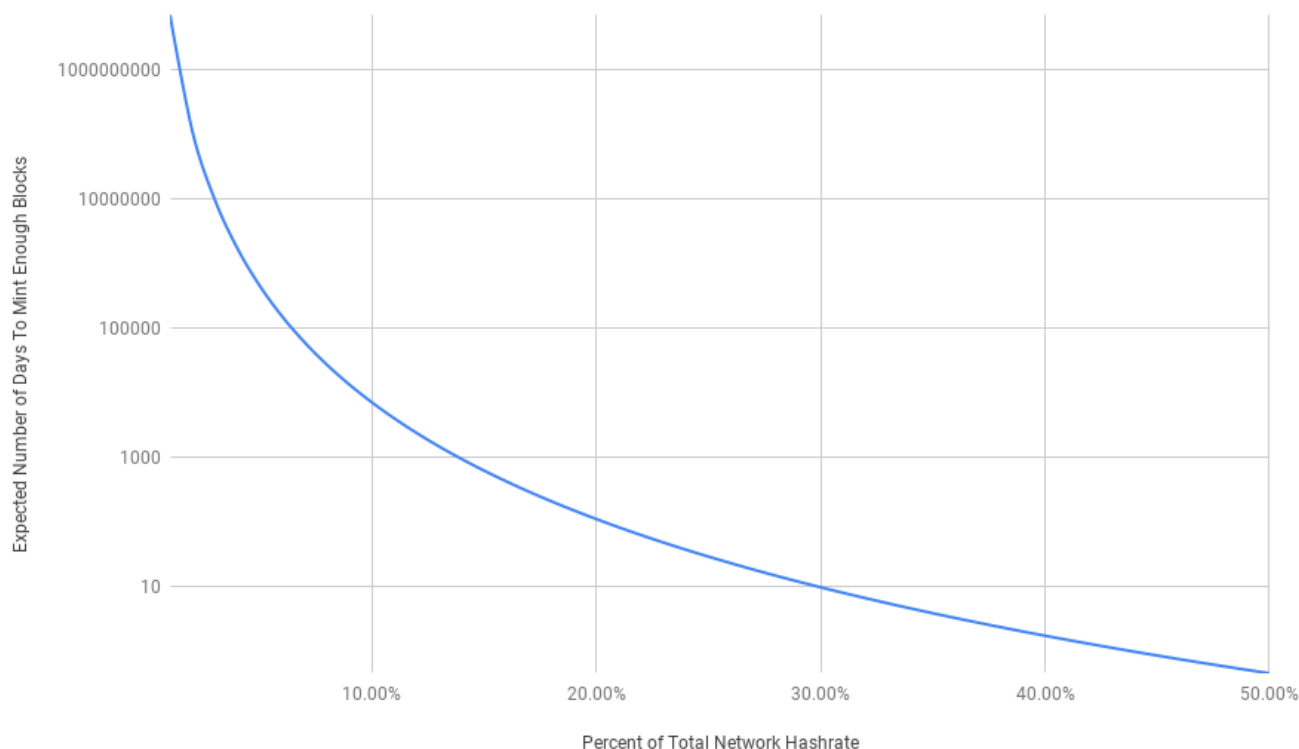
Maximum Drag

However, in order to induce the **maximum** drag on the MTP a miner would want to solve 6 blocks in a row. If their 6 of the past 11 blocks are not all in order, then time gaps created by other miners would force the adversarial miner to set the timestamps of their blocks more than one second after each other because the MTP for each block would jump forward significantly as honest miners place more accurate timestamps on their blocks.

How hard is it to solve 6 blocks in a row? If we once again assume a miner with 1% of the network hashrate then the chance of minting any given streak of 6 blocks in a row is 0.01^6 = roughly one in a trillion. If you maintained 1% of the hashrate then the expected number of blocks that would need to occur before you found 6 in a row would be nearly 2 million years.

A more generalized version of the expected time to successful time drag attack formula would be:

$$(1 / \% \text{ hashrate}^6) / 144 \text{ blocks/day} = \# \text{ days}$$



This attack is even more difficult to pull off, requiring more like 20% or 30% of the network hashrate to occur in a reasonable timeframe. As you may imagine, this happens quite rarely and when it does, people notice. The [last times it happened](#) were [in July 2014 by GHash](#), which had over 40% of the hashpower for a while and even [touched 51% for a short time](#). It also [happened 9 months earlier](#) when BTC Guild had nearly half of the hashpower. If you have 50% of the hashpower then your chance of minting 6 blocks in a row is $0.5^6 = \text{one in } 64$. If you maintained 50% of the hashrate then you could expect to find 6 blocks in a row nearly every 12 hours.

It's clear that it's not possible to sustain a drag on Bitcoin's Median Time Past on a long term time scale without majority hashpower, but you could drag it by as much as several hours for a short period (a block or so) with the right combination of luck and patience. If you assume that other miners are fairly accurate with their timestamps, then the median time past should be approximately 1 hour ago, though it could be several hours more due to the variability in blocks being found. If you manage to mint 6 blocks with timestamps of 1 hour ago plus 1 second, 2 seconds, 3 seconds, etc then at the 6th block the MTP would be approximately 2 hours ago. If we assume an extreme condition of 1 hour gaps between blocks, then the MTP would be 6 hours ago.

By allowing a reasonable amount of flexibility with block timestamps and then taking a median time of recent blocks, we end up with an algorithm that is pretty

hard to game but is not so brittle as to adversely affect miners who are somewhat out of sync with the real time.

Let's Do the Time Warp Again

What if an attacker did have more than 50% of the network hashpower and they wanted to slow the passage of Bitcoin time? They could do some pretty nasty stuff. Such an adversarial miner could prevent the timestamp from advancing by more than 1 second with each new block. If they did this for a long enough period of time and ended up creating blocks on the difficulty retarget intervals with timestamps that made it look like the previous 2016 blocks took far more than 2 weeks to create, they could game [the retargeting logic](#) to decrease the mining difficulty by up to 75% every 2016 blocks. Eventually with the difficulty low enough, they could mint as many blocks as they wanted in a given time period and thus receive more mining reward than expected. An optimized time warp attack [could mine all the remaining bitcoin in 18.7 days](#). We've actually seen similar behavior occur on Bitcoin's testnet3 due to a [quirk in the difficulty retargeting](#) and now testnet3 has minted 1,482,878 blocks in 8 years, about 350% of the expected emission.

Time warp attacks are nothing new. Such an attack was first performed against a coin called "[Geist Geld](#)" in 2011 and it was discussed as being a "[variant of the 51% attack](#)" on BitcoinTalk. Geist Geld was intended to test out the upper limits of block generation rate via very short block times, as well as the behavior of a cryptocurrency with (almost) stable generation rate and no upper limit or alteration to supply.

[Whitecoin appears to have also suffered from a time warp attack](#) that was conducted in 2014.

In 2018 [Verge](#) was hit by such an attack. And then 6 weeks later [it was hit again!](#)

In general, cryptocurrencies that have a minority of hashpower for a given style of hardware (ASICs or GPUs) [are vulnerable to time warp attacks](#) because they are inherently vulnerable to 51% attacks.

Interestingly, while time warping is often referred to as an attack because it results in unintended behavior of the system, some people have shown that it can be exploited for potentially desired uses. In 2015 Vitalik Buterin [described a way to speed up blocks](#) via a soft fork and thus increase on-chain capacity. In 2018 Bitcoin developer Mark Friedenbach made a proposal for leveraging this unintended behavior in order to add new functionality to Bitcoin. In his "[Forward Blocks](#)" proposal, Mark states that his method enables scaling up on-chain transaction volume to 3584X current levels, changing the proof-of-work algorithm in a backwards compatible way, sharding, a rebateable fee market for consensus fee detection, and smoothing out drops in miner subsidy along with prerequisite

protocol pieces for confidential transactions, mimblewimble, unlinkable anonymous spends, and sidechains.

Such proposals are contentious, however, and would likely force anyone building systems reliant upon the timestamps in the Bitcoin block headers to look elsewhere for that data. It would also be fairly easy for such a change to be blocked, as Greg Maxwell [stated on the Bitcoin developer mailing list](#):

It can be fixed with a soft-fork that further constraints block timestamps, and a couple of proposals have been floated along these lines.

In Conclusion

Bitcoin's timestamp security and the simple rules constraining the window of acceptable timestamps have withstood 10 years in an adversarial environment despite their known weaknesses. We know that a 51% cabal of miners could wreak havoc on the network, at least for a short time, but this has never happened—likely because the incentives are not aligned for miners to do so. Rational miners would not choose a short term gain in return for killing the long term golden goose.

Thanks to [Jimmy Song](#) and [David A. Harding](#).

What Do Wyoming's 13 New Blockchain Laws Mean?

By [Caitlin Long](#)

Posted March 4, 2019

Wyoming has now enacted a total of 13 blockchain-enabling laws, making it the only US state to provide a comprehensive, welcoming legal framework that enables blockchain technology to flourish, both for individuals and companies. These laws enable innovation and creativity, and are meant to bring capital, jobs and revenue into Wyoming.

Law and technology are discrete systems. For a new technology to attain wide adoption, the law and technology must be “backwards-compatible,” as early bitcoin investor Trace Mayer puts it. In a nutshell, that’s what Wyoming has now done for blockchain technology.

Here’s an analysis of what I think it all means. NONE of what follows is legal or tax advice—this is for educational purposes only. You may not rely on it and you must seek a qualified adviser to advise you about how you can take advantage of the great opportunities Wyoming offers!

In sum, Wyoming is already the “Delaware of digital asset law,” a reference to Delaware’s lead in corporate law. More than a dozen other US states and Congress are now following Wyoming’s lead by enacting our bills (usually just one or two of Wyoming’s bills). But no other state is likely to catch up to Wyoming—it’s a very tall order for any legislature to enact 13 bills on a single topic in a compressed time frame, especially when another state has already claimed first-mover advantage.

Here are the top highlights regarding Wyoming’s newest blockchain laws:

- [Recognizes](#) direct property rights for individual owners of digital assets of all types (virtual currencies, digital securities and utility tokens) and applies the super-negotiability rules of commercial law to virtual currencies—which foster their liquidity—by applying the very same rules that apply to money. Wyoming’s commercial law reflects the true nature of digital assets (directly owned, peer-to-peer assets), and I strongly encourage other states to adopt Wyoming’s same commercial law protections;
- [Creates](#) a fintech sandbox to provide regulatory relief to financial innovators from existing laws for up to 3 years. It’s broadly reciprocal with fintech sandboxes both in the US and globally;
- [Authorizes](#) a new type of state-chartered depository institution to provide basic banking services to blockchain and other businesses. The bank is required to have 100% reserves, cannot lend, is for business depositors only, and FDIC

insurance is optional. Such banks could be operating as soon as March 31, 2020;

- [Authorizes](#) the first true “qualified custodian” for digital assets which is a bank. Wyoming banks can start such operations as soon as September 1, 2019. Wyoming’s digital asset custodians will stand out above all others because they will respect the DIRECT ownership nature of digital assets! These new custodians won't be like traditional securities custodians, because for a Wyoming-based custodian investors will still DIRECTLY own their digital assets under custody as a BAILMENT, which means they retain direct ownership while merely giving up control (much like valet parking). Today, institutional investors are forced to be *de facto* creditors of their securities custodians, since all publicly-traded securities are owned indirectly. Custody under bailment is possible in securities custody today, but it's neutered by the fact that all securities are owned indirectly—investors can't directly own the real security, and therefore they're really just counterparties to the custodian. So, what Wyoming has done is truly revolutionary—BAILMENT + DIRECT ownership! It doesn't exist in securities custody today! Customers of Wyoming custodians can still choose indirect ownership, but it's on much more investor-friendly terms than exist in securities custody today. In sum, Wyoming will become known as the home of SOLVENT, investor-friendly digital asset custodians to which investment fiduciaries are likely to migrate over time.

Why would a staunch supporter of #NotYourKeysNotYourCoins, as I am, help set up a digital asset custodian—especially when I acknowledge all third parties can be security holes? Answer: the custodian is for large institutional investors, which are required by federal securities law to store the assets they manage at an independent custodian. And, now, these institutional investors will be able to directly own the digital assets they custody at solvent Wyoming custodians.

Capital ultimately flows to where it's treated best. For digital assets within the US, I'm pretty confident that will end up being Wyoming. It's all about its legal regime respecting DIRECT ownership of digital assets, whether by individuals or institutional investors. I was formerly a fiduciary of pension plans and, based on that experience, I think it will become a very big deal that provably SOLVENT custodians exist. As more and more securities are natively-issued on blockchains in the next several years, Wyoming's custodians will likely become the preferred digital-asset custodians of 401(k) plans and mutual funds—and they will help make securities markets fair to regular investors!

Here are some common questions about Wyoming's laws. Again, this is not legal or tax advice!

1. DO YOU NEED TO MOVE TO WYOMING TO BENEFIT FROM ITS BLOCKCHAIN LAWS?

No, not unless you're starting a Wyoming bank or custodian. For everyone else, it's pretty easy to take advantage of Wyoming's blockchain laws. Just ask your attorney!

2. HOW CAN INDIVIDUALS BENEFIT FROM THE WYOMING BLOCKCHAIN LAWS?

Individual owners of digital assets can gain the protections of Wyoming's laws by moving to Wyoming, or you may physically locate your cold storage digital assets somewhere in Wyoming or set up your own Wyoming LLC, corporation, trust, foundation or other business entity (through which to own your digital assets). As I'll discuss below, there's a particular reason why owning digital assets via a Wyoming entity may be beneficial. From a personal wealth planning and protection standpoint, Wyoming's laws really can't be beat. Billions of dollars in trust assets are already managed in our state. Wyoming invented the LLC in 1977 and this year it revamped its trust and statutory foundation laws to be the best in the US. Its LLC laws have very strong privacy protections, and Wyoming is frequently cited as the tax-friendliest state in the United States (more on that below).

3. HOW CAN BUSINESSES BENEFIT FROM WYOMING'S BLOCKCHAIN LAWS?

Businesses have 3 ways to benefit and they're not mutually exclusive. Your business can (1) simply apply Wyoming law to its contracts involving digital assets, (2) legally domicile in Wyoming and/or (3) physically locate in Wyoming. If you own a blockchain business, you should already be asking your attorney why the company is still domiciled anywhere other than Wyoming and examine the costs/benefits of converting to a Wyoming domicile. One objection I've heard from attorneys is that Wyoming doesn't have a special court for resolving complex business disputes like Delaware does. Well, Wyoming just solved that by setting up its own business court ("Chancery Court") this year, details of which are [here](#).

4. HOW ARE THE TAXES IN WYOMING?

Basically, there are none at the state level—in most cases! In the US, federal taxes are distinct from state taxes and federal taxes apply to every American—but Wyoming can (and does) offer what's probably the friendliest *state* tax regime. Wyoming often comes up #1 on surveys of the best states for tax purposes. At the state level, Wyoming has no personal income tax, no corporate income tax, and almost none of the other "gotcha" taxes that frequently hit businesses domiciled in other US states, such as franchise taxes or gross-receipts taxes.

Every Delaware-registered business should be asking your tax adviser how much you pay in Delaware franchise taxes every year and then calculate how much you'd save by redomiciling to Wyoming (hint hint!). And, for digital assets specifically, last year

Wyoming [exempted](#) them from property taxes. Sales taxes apply to tangible personal property, but Wyoming's legislature this year [classified](#) digital assets as *intangible personal property* so...you can fill in the blank.

As for federal tax relief, Wyoming can't fix the IRS's terrible tax treatment of digital assets (yes, spending bitcoin on a cup of coffee triggers federal capital gains tax). But there are [25 opportunity zones](#) located around Wyoming that provide potential capital gains tax deferral—again, talk to your tax adviser. Some of these locations might be great spots for cold-storage vaults, mining operations and/or the new headquarters of your start-up or investment fund.

In short, there are very good tax reasons why, as they say, “the billionaires are pushing out the millionaires” in Jackson Hole, Wyoming, and why so many tax-motivated relocations to Wyoming are happening. Wyoming is America's tax-friendliest state in many ways—and it has the clearest, tax-friendly approach to digital assets.

5. WHAT DOES WYOMING'S NEW COMMERCIAL LAW FOR DIGITAL ASSETS MEAN?

Wyoming is the first state to clarify the treatment of digital assets under existing commercial laws (e.g., the Uniform Commercial Code (UCC)), and [this](#) is probably the most important of Wyoming's new blockchain laws. Laws governing commerce are the foundational laws of business—they're a “protocol layer” of the legal system. These laws are essentially the plumbing that makes every financial transaction possible, and most importantly, they provide rules for what happens when a transaction doesn't go smoothly—ensuring parties have certainty regarding their rights and duties.

States control commercial laws in the US, so the federal government cannot trump what Wyoming has just created. I strongly encourage other states to enact Wyoming's same statutory language, which you can find [here](#).

Wyoming's commercial law for digital assets is WAY too detailed to analyze here, but I'll highlight my favorite four parts of it. First, as described above, it maps virtual currencies to the super-negotiability rules of money under existing law. In plain terms, this means a bitcoin purchaser can buy bitcoin free and clear of any pre-existing liens against it, unless the purchaser was defrauding a lender who had previously made a loan against that bitcoin. Second, it defines “control” in a manner that's consistent with how blockchain assets are actually controlled. It also enables a smart contract to take control of a digital asset—very forward-thinking! Third, it makes security interests in digital assets “possessory security interests,” which means Wyoming law applies as long as the assets are, under this law, “located in” Wyoming—and the law makes it very easy to “locate” the digital assets in Wyoming. Possessory security interests have priority over other types of security interests. (For this reason

alone, I suspect most coin lending and prime brokerage businesses will want to domicile in Wyoming.) Fourth, it extinguishes pre-existing liens after two years—to match the statute of limitations for fraudulent conveyance under federal bankruptcy law.

The latter is one reason why it may make sense for individuals to store digital assets in Wyoming or through a Wyoming LLC, trust or other entity. Here's the issue that may solve. It's possible—though admittedly an edge case—that a judge will enforce a prior lien against bitcoin that you, an innocent purchaser, did not know existed. To my knowledge that hasn't actually happened yet, but as bitcoin lending markets grow and as more merchants accept bitcoin (which may be covered by an all-assets lien over the merchant's inventory), the issue will inevitably arise. Some attorneys have called this [bitcoin's Achilles heel](#), and many speculate this “surprise” lien risk is one of the reasons why new bitcoins trade at a premium over older bitcoins in OTC markets. Well, Wyoming law provides a solution—ask your attorney about the myriad ways to get your digital assets subject to Wyoming law for two years!

6. ANYTHING ELSE?

Yes, a lot. Wyoming's money transmitter law [exempts crypto-to-crypto](#) transactions, effective as of last year. Many lawyers worry that Lightning Network transactions may run afoul of money transmitter laws. Well, not in Wyoming (#probably!—check with your lawyer!) At least three other states that I know of have either enacted, or are in process of enacting, Wyoming's same money transmitter exemption for crypto-to-crypto transactions.

If you're working on security tokens, you won't find a friendlier state because Wyoming law legally recognizes both [uncertificated](#) and [certificated](#) blockchain shares of stock. Delaware was first to recognize blockchain shares, but it only recognizes uncertificated versions. Wyoming's new law regarding certificated shares just took effect this week, and WOW, Missouri was lightning fast in already copying it! Imitation is the sincerest form of flattery!

Wyoming was the first state to exempt [utility tokens](#) from its state securities laws, which took effect last year. State law doesn't trump federal laws regarding securities, but I'm pleased that Arizona also enacted a similar law last year and five other states have proposed it this year. Wyoming's law also heavily influenced the proposed federal [Token Taxonomy Act](#) in Congress. It's really true that the impetus to change bad federal law sometimes bubbles up from the states—and 7 states supporting a common cause is actually a lot, just one year into the effort—it's already a “movement” to push back against the SEC's view that most digital assets are securities.

And Wyoming added a couple of sweeteners to attract cryptocurrency miners to Wyoming as well.

One bill enables Wyoming's electric utilities to [negotiate directly](#) with miners, instead of requiring them to go through the ratemaking process. All gains and losses from mining agreements remain with the utility's shareholders, thereby completely insulating retail electric customers from these transactions.

And, with a goal to help Wyoming's struggling coal industry—which is crucial to Wyoming and is trying to recover from low coal prices—Wyoming passed a [bill](#) to provide a process for Wyoming's electric utilities to sell the coal-fired generation plants they would otherwise permanently be shutting down. Potential buyers may include crypto miners, among others, and I'm told power costs available in Wyoming would be highly competitive with the best electricity prices available to miners around the world.

7. WHAT'S IN THIS FOR WYOMING?

CAPITAL, JOBS and REVENUE. It's really that simple.

8. WILL THERE BE PROBLEMS FOR WYOMING?

Sure. But Wyoming is ready, and its laws are pretty punitive on fraudsters. (Remember, rehypothecation is a felony in Wyoming...in New York, it wins bankers big bonuses. In Wyoming, it might land you in jail.)

9. TELL ME MORE ABOUT WYOMING'S QUALIFIED CUSTODIAN LAW

It's an opt-in regime available to any Wyoming bank, including its new special-purpose depository institutions. A bank license is superior to a trust company license for digital asset custody, for many reasons. Some have expressed concerns about triggering the Bank Holding Company Act (BHCA) by obtaining a Wyoming bank license, but a Wyoming special-purpose depository institution does not meet the definition of "bank" under the BHCA because it can't make commercial loans. The US Supreme Court has [rejected](#) previous attempts by the Federal Reserve to expand this definition, so Wyoming's special-purpose depository institution is a pretty neat regulatory option for those wanting to become qualified custodians of digital assets.

Wyoming's new law also ensures that digital asset owners have legal certainty about how their assets will be treated and the nature of the custodial relationship (clear laws that specifically govern digital assets + a Chancery Court exclusively devoted to fast resolution of business disputes). Digital assets held in custody today in any other state lack this certainty!

Wyoming's law contains many investor protections, and SOLVENT custodians will have no problem complying with these provisions. Institutional investors can expect

that Wyoming-based qualified custodians will actually be SOLVENT for three basic reasons:

- The custody relationship is legally a BAILMENT (akin to valet parking for your car, where you give up control but not ownership of your asset). This is far superior to how securities custodians traditionally work, where investors are *de facto* creditors of their custodians, which are leveraged and may or may not actually have on hand the assets they've promised to investors.
- The law's investor protections are a big deal—all value from digital assets (including forks, airdrops and staking) belongs to investors unless otherwise expressly agreed. This model is distinct from both traditional securities custodians and crypto exchanges, where investors are usually *de facto* creditors and where the firms frequently trade with customers' assets behind the scenes.
- Rehypothecation of assets—the practice of pledging the same asset as collateral for different loans, which is rampant in the securities industry and which poses solvency risks to traditional securities custodians—is expressly prohibited by Wyoming's new digital asset law. It was already a felony in Wyoming anyway, per a 1986 Supreme Court case ([Smith v State](#)).

In a nutshell, Wyoming's digital asset custodians will simply be service providers to institutional investors, who will still own their digital assets. They will not be counterparties that are *de facto* hedge funds in a relationship that is too often "heads I win, tails I win." Fiduciaries of institutional investors will, I believe, appreciate this and migrate to Wyoming-based digital asset custodians.

Let me close by thanking the wise Wyoming legislators and Governor Gordon, who stand for strong property rights and are welcoming this industry with meaningful laws. Thank you also to all the small army of industry supporters who showed up to support the Wyoming Blockchain Coalition's events along the way, and to those who provided comments on our draft laws. We're all volunteers who crowdsourced this effort!

Very special thank you to Rep. Tyler Lindholm and Sen. Ogden Driskill, who led the posse so effectively. Special thanks to Steve Lupien of the Digital Asset Trade Association for his strong, intrepid support on the ground. Biggest thanks go to Chris Land, legislative draftsman extraordinaire and unsung hero of this massive undertaking—a true expert in commercial law and digital asset law. Yes, we even talked about the draft UCC bill on Christmas day!

I didn't intend to spend the last 14 months volunteering—but am so glad I did because it benefited two things I dearly love, Wyoming and blockchain. It's probable that my deep attraction to blockchain stems from my Wyoming upbringing.

Wyoming instilled in me deep-seeded philosophies that have a strong cultural overlap with those of blockchain (i.e., what's mine is mine and what's yours is yours, good fences make good neighbors, rugged individualism, clear property rights and low taxes). Owing to this strong cultural overlap, it makes perfect sense that Wyoming will be the home of blockchain in the US!

I'll be hunkering down in the next few months to help advise the Wyoming Banking Division on the rules drafting process for institutional digital asset custody and special-purpose depository institutions. And I finally hope to finish the book I started writing about the intersection of Wall Street and blockchain. If only I weren't such a slow writer! :-)

Links

- <https://www.wyoleg.gov/Legislation/2019/sf0125>
- <https://www.wyoleg.gov/Legislation/2019/hb0057>
- <https://www.wyoleg.gov/Legislation/2019/hb0074>
- <https://wyoleg.gov/Legislation/2019/SF0104>
- <https://www.wyoleg.gov/Legislation/2018/SF0111>
- <https://www.wyoleg.gov/Legislation/2019/SF0125>
- <http://wyomingbusiness.org/news/wyoming-names-25-opportunity-zones-for-10962>
- <https://www.wyoleg.gov/Legislation/2019/sf0125>
- <https://www.usv.com/post/531eec41c4072a1e3a04f7cc/is-the-ucc-the-achilles-heel-of-bitcoin>
- <https://www.wyoleg.gov/Legislation/2018/HB0019>
- <https://www.wyoleg.gov/Legislation/2018/HB0101>
- <https://www.wyoleg.gov/Legislation/2019/hb0185>
- <https://www.wyoleg.gov/Legislation/2018/HB0070>
- <https://www.congress.gov/bill/115th-congress/house-bill/7356>
- <https://www.wyoleg.gov/Legislation/2019/hb0113>
- <https://www.wyoleg.gov/Legislation/2019/sf0159>
- <https://supreme.justia.com/cases/federal/us/474/361/>
- <https://law.justia.com/cases/wyoming/supreme-court/1986/121666.html>

Tweetstorm: Economic History

By [Nick Szabo](#)

Posted March 3, 2019

Economic history has been dominated by basics: growing food & fuel, mating & child rearing, fighting wars, clothing & shelter, worrying about afterlife. Occasionally there have been major agricultural surpluses, which have been spent in a bizarre variety of ways (thread) /1

Agricultural surpluses have been spent on military parades, crown jewels, tall cathedrals, vast priesthoods, gigantic tombs, arrays of monoliths, treasure fleets, moon shots, & a dizzying variety of other things. /2

These seem like irrational bubbles, yet in many cases persisted for or recurred across centuries or millennia. We moderns seem to be trending towards competitions for scholastic credentials & efforts at longer & healthier lives, each of which appeal to insatiable needs. /3

Almost any way developed countries spend our titanic industrial surpluses will be epic frivolity by historical standards, whether it be sprawling regulatory & scholastic priesthoods or a “service economy” where mobile servants wait on the tables of secular priests & investors. /4

There are no solid standards of historical precedent or economic rationality that can help us much in predicting which forms of frivolity will dominate, rather they point to the optionality & unpredictability among a vast universe of choices. /5

Why digital tokens need better tax treatment

By [Blockchain Association](#)

Posted March 4, 2019

As we've [written before](#), blockchain technology allows for a new wave of business model innovation that we think will make the internet work better for all of us. Unfortunately, there are some public policy issues that need to be addressed before these networks can reach their full potential, including tax law.

The tax code has a reasonable *de minimis* exemption for personal foreign currency transactions

To understand the burdens imposed by the US tax code on the emerging decentralized blockchain economy, think back to the last time you traveled internationally. When you got off the plane, you probably visited an exchange kiosk to acquire a few hundred dollars worth of local currency. Perhaps you used that cash to pay for a taxi to your hotel, or to purchase breakfast at a café up the street. Depending on your destination, you may have needed to rely more extensively on cash for things like lodging and local tours. When you returned home, did you painstakingly review each of these transactions to calculate any foreign exchange gains for tax purposes? Of course you didn't. That would be a logistical nightmare.

The US tax code recognizes the prohibitive complexity of keeping track of personal transactions in foreign currency. To address this complexity, [section 988\(e\)](#) of the code provides a very reasonable exception for exactly the situation described above. The exception works by excluding any gain that an individual realizes as the result of a personal transaction in foreign currency from the individual's taxable income so long as the gain is less than \$200.

Virtual currencies should also have a *de minimis* exemption

Currently cryptocurrencies and blockchain tokens do not qualify for this exception. Based on [guidance issued in 2014](#), the IRS treats virtual currencies as property under US tax law. This means that the sale or exchange of blockchain tokens for fiat currency or other goods and services is a taxable event. Consequently, if a user [spends \\$0.09 worth of Bitcoin to buy candy from a vending machine](#), she is required to calculate (and pay) the tax liability associated with that transaction.

While this may seem like an inconvenience derailing the plans of a small number of ideologues that want to use bitcoin to buy coffee, it is actually a much bigger problem. Many of the imaginative business models that innovators are developing in the blockchain industry become untenable under the weight of this type of tax treatment. Open blockchain networks promise to enable these new business models

by providing efficient payment rails that don't currently exist for traditional fiat currencies. Requiring users to track gains and losses on each micro-transaction they engage in across dozens of different digital currencies significantly erodes these efficiency gains.

The ecosystem needs the Cryptocurrency Tax Fairness Act

As our friends at Coin Center have pointed out, [cryptocurrency taxation is broken](#) and needs to be improved in order for the full potential of blockchain technology to be realized in the US. Luckily, the solution is relatively simple. We believe that the smoothest approach is for lawmakers to extend the *de minimis* exemption for personal transactions in foreign currency to cover transactions in blockchain tokens as well. The legislative language required to extend the exemption is minimal and, in the last congressional session, Representatives Polis and Schweikart [introduced a bill](#) that would have made the required changes. We are working with lawmakers and other allies to get this bill reintroduced and moved in this new legislative session.

We believe that the provisions of this bill are crucial for ensuring that the US remains competitive in the quickly evolving and highly promising blockchain industry. As the tax code currently stands, US citizens and entrepreneurs are at a significant disadvantage to citizens of countries like [Germany](#) and [Italy](#), which both already exempt personal cryptocurrency transactions from the burdensome requirements that our tax code currently imposes. While it may seem like a relatively minor policy wrinkle given the nascent state of the open blockchain economy today, addressing this issue sooner rather than later will more fully allow all Americans to benefit from the advantages offered by the emerging new internet.

Links

- <https://medium.com/@BlockchainAssoc/why-digital-tokens-are-the-foundation-for-a-new-internet-7a2dbbceb4f5>
- <https://www.wired.com/story/how-blockchain-can-wrest-the-internet-from-corporations/>
- <https://www.law.cornell.edu/uscode/text/26/988>
- <https://www.irs.gov/pub/irs-drop/n-14-21.pdf>
- <https://coincenter.org/link/we-demonstrated-the-bitcoin-lightning-network-in-congress>
- <https://coincenter.org/entry/bitcoin-taxation-is-broken-here-s-how-to-fix-it>
- <https://coincenter.org/entry/rep-polis-schweikert-introduce-cryptocurrency-tax-fairness-act-in-congress>
- <http://www.nomoretax.eu/bitcoin-tax-haven-germany/>
- <https://www.loc.gov/law/help/cryptocurrency/world-survey.php>

Bitcoin Has a Branding Problem—It's Evolution, Not Revolution

For technologists and historians, it may well be a revolution; but for everyone else—it's an evolution in personal finance.

By [Ryan Radloff](#)

Posted March 6, 2019

Before we get started I've broken this post out into two parts to address the point, so please bear with me regarding format.

Part 1—I take a look at how our financial lives trend towards convenience (and as a result, dependence on intermediaries); and whether we should expect that to change anytime soon.

Part 2—I look at the larger evolution of assets from physical to 'digital' over the last 35+ years; and where bitcoin fits in that trend.

Both parts are important to illustrate a critical point—for the end user, bitcoin doesn't exist in a vacuum. It exists on a spectrum of evolution for consumers and the best thing we can do to drive adoption is acknowledge this nuance.

Part 1: Trending Towards Convenience (Dependence)

As an American residing in London, it takes me around two weeks from the moment I walk into a local bank branch to complete the arduous and highly manual process of verification (a.k.a. **K**now **Y**our **C**ustomer) in order to become an account holder.

This system is so inefficient that it has birthed a new array of challenger banks (e.g. Revolut, Monzo and Starling Bank). These banks focus on eliminating the inefficiencies and friction of traditional banking, and claim to put us more in control of our finances than ever before.

This model and mission has driven rapid growth for the aforementioned companies, and altered our notion of what a bank looks and feels like.

Yet at the same time, it's a model and mission which, to borrow from *The Wizard of Oz*, asks us to "*Pay no attention to that man behind the curtain...*"

...and perhaps more than ever before, that is the paradox at play here.

Pay No Attention to That Man Behind the Curtain

While new Fintech banks/platforms provide the illusion of closer proximity to our finances, in many cases these platforms are nothing more than a re-engineered interface for the traditional financial system, with new branding.

For example, Yolt is really just a slick front-end for Dutch multinational bank ING; Wealthify, a brilliant UI owned by Aviva; Zelle—founded by Bank of America, Wells Fargo and JPMorgan Chase—backed by even more banks; and Nutmeg, the mobile choice for investment management, is substantially owned by Goldman Sachs.

Sure, with a few taps I can send £4 I owe you for that latte faster than ever before. But the net result (trade-off) of the rapid digitalisation of the financial system is a requisite increase in specialised financial intermediaries layered on top of each other, built to eliminate the ‘friction’ points of the legacy world.

And here lies the paradox:

While we’ve been hit with slogans like ‘New Money’ as we venture deeper down the path of convenience banking, we’re really just interacting with a new facade of the legacy financial system.

With that context, it’s easy to understand why people are confused when a truly digital, fully bearer asset enters the picture—‘New Money’ incarnate.

We don’t initially understand 1) how it’s different than what we already have and 2) why we should ever be concerned about what is going on behind the curtain of our new digital banks.

After all... we’re in control of our finances, not them — so who cares?!

To the second point, what most people don’t realise is the unfortunate reality that the existing system has ‘evolved’ into an incredibly complex web of financial intermediaries built on top of and around each other. All meant to distribute risk more evenly (yet rarely do), the actual result is an opaque fiefdom for risky (and unscrupulous) behaviour.

Look no further than some of these headlines from the last few years...

- [HSBC to pay \\$1.9 billion U.S. fine in money-laundering case](#)
- [Watchdogs impose \\$3.4B fines in bank forex probe](#)
- [Deutsche Bank settles silver, gold price manipulation suits](#)
- [Banks face \\$1bn bill over fees-for-no-service scandal](#)

- [JPMorgan to pay more than \\$135 million for improper handling of American Depositary Receipts \(ADRS\)](#)
- [Wells Fargo is paying \\$575 million to states to settle fake account claims](#)

This isn't even to mention banks' central role in the 2008 financial crisis, the lasting effects of which have been well documented and which no doubt impacted countless families in immense ways—my own included.

As [Elaine Ou opined for Bloomberg](#):

“Financial institutions make people feel safe by hiding risk behind layers of complexity. Crypto brings risk front and centre and brags about it on the internet.”

And to the first point regarding how digital assets are different than what we already have... those outside of crypto-land have their PayPal app, their Venmo accounts and can easily send \$4 internationally to a friend without using Bank of America or Barclays. **Why do they need anything new, much less a revolution?**

Revolution is a rallying cry for early adopters, and a historians' view on what is actually evolution, in real-time.

Revolutions are inconvenient, messy and disruptive to the status quo, a default which we are unfortunately biased towards.

Revolutions often only happen as an absolute necessity, when 'society' has exhausted all other options and tensions have evolved to a breaking point.

So when outsiders (read: people we would like to eventually opt-in to this new system) hear the “revolution” declaration from bitcoiners, it simply doesn't resonate. Humans are wired to seek confirmation of our own biases and be sceptical of new ideas that challenge or threaten our worldview.

The Evolution Amidst the Revolution

Challenger Fintech banks are winning hearts and minds by capitalising on the weaknesses of bigger, bulkier competitors. Legacy banks are now 'evolving' with their own facades meant to capture those same hearts and minds.

Consumers are loving the evolution toward convenience and 'control.'

I would argue that Bitcoin is simply part of this larger migration away from our parents “brick and mortar” banks toward more nimble, digital financial services.

While Bitcoin is a revolution with respect to approach, infrastructure and (dis)intermediation; to the consumer, it will (and should) feel like it is part of the same evolution that they have been part of all along.

Although Bitcoin does indeed seek to revolutionise the financial industry by separating money and state, “revolution” doesn’t need to be the lede.

From most people’s perspective, we’ve gotten along just fine paying no attention to that ‘man behind the curtain.’ Why should we expect to change that behaviour en masse all of a sudden?

Part 2: Reframing Bitcoin in the Progression to Digital Finance

In an effort to track the larger progression towards digital finance (an evolution over 35+ years in the making), our research team at CoinShares developed a qualitative approach that plots the dependency of an asset on financial intermediaries against how digital an asset is (as defined below).

As I touched on in the previous section, we witnessed an explosion in the number of financial intermediaries as we’ve moved towards ‘convenience banking’. The truth, however, is that the number of intermediaries has been mushrooming for much longer, coinciding with a shift in preference towards digital proxies for financial assets.

For the purposes of this exercise, we defined “dependency” as an asset’s dependence on—or independence from—third-party intermediaries in order to buy, sell, and custody said asset. We’ve plotted this on the y-axis in the charts below.

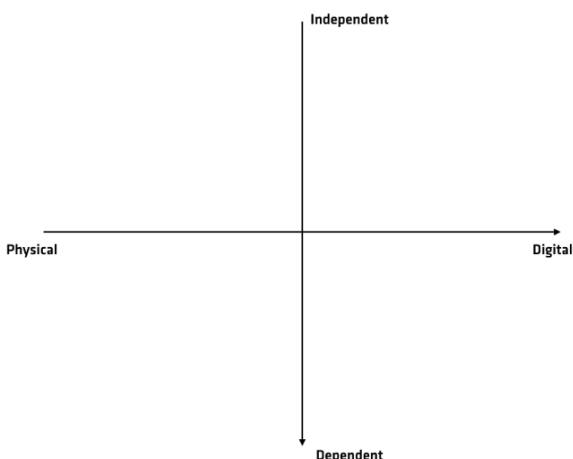
On the X-axis, we plotted how “digital” an asset has become. This was measured by tracking the preference to interact with that asset in a non-physical, ‘proxied’ format (i.e. digital)—whether it be an ETF, option, future, etc.—rather than the underlying asset itself.

For both of these measures, we used quantitative data whenever available, and supplemented with qualitative observations when it was not. In these instances, we identified specific inflection points to warrant movement on the ‘dependency’ y-axis.

For example, fine wine is generally considered an illiquid asset. In 1982, it was tradable in rare circumstances when a buyer and seller were paired. Yet in 2000, [Liv-ex launched](#) to bring transparency and efficiency to fine wine trading via an electronic exchange. A few years later, they launched the [Liv-ex 100 Fine Wine Index](#). Today, there are a number of structured investment vehicles (e.g. the [Vinculum Wine](#)

[Fund](#)) that offer exposure to this asset class—beyond purchasing the wines themselves; but this also introduced new intermediaries to the process.

CoinShares Independence Analysis



Methodology

x-axis = digital

Ratio derived between physical traded and futures (as a proxy for digital volume)

y-axis = dependency

Scoring derived from dependency on financial intermediaries, custodians, and average correlation of assets

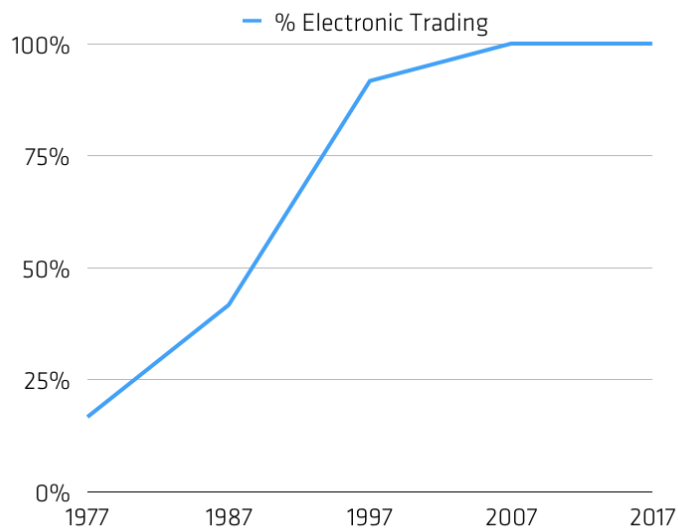
Indices used:

Equity = MSCI World Index
Debt = FTSE G7 Index
Oil = European Brent Spot/Futures
Base Metals = Bloomberg Base Metals Spot
Gold = Gold Spot/Futures
Real Estate = FTSE EPRA Nareit Developed Index
Wine = Liv-ex 100 Benchmark Fine Wine Index
BTC = Bitcoin spot

CoinShares Research

Across nearly all asset classes, as transactions shifted to the digital sphere, they required more intermediaries; and as a result, rendered assets 'more dependent.' The exceptions were equities and real estate, which involved a number of intermediaries even before this shift to digital.

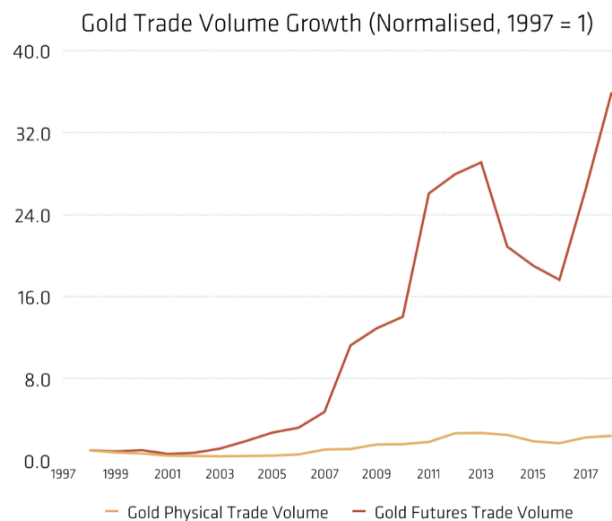
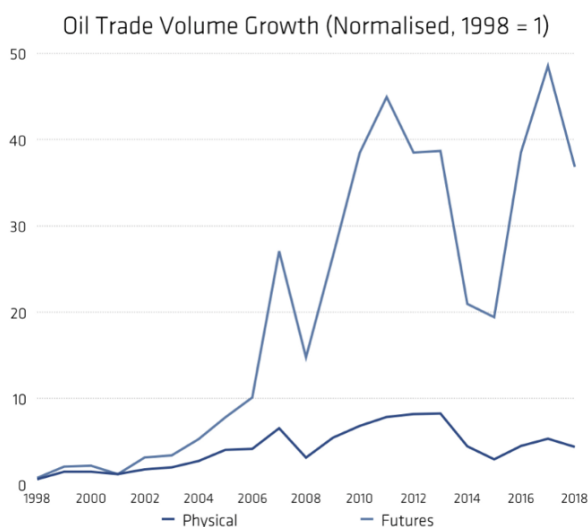
As a part of this mini-survey, we also looked at the shift in transaction volumes from physical trades to electronic ones. This became one of our proxies for the digitalisation of assets—the transition of exchange volumes from [open outcry](#) to electronic trades.



Open Outcry trading versus electronic — CoinShares Research

In a short amount of time, digitised, electronic trading accounted for more than 50% of all bids placed. By the early 2000s, open-outcry trading was effectively extinct.

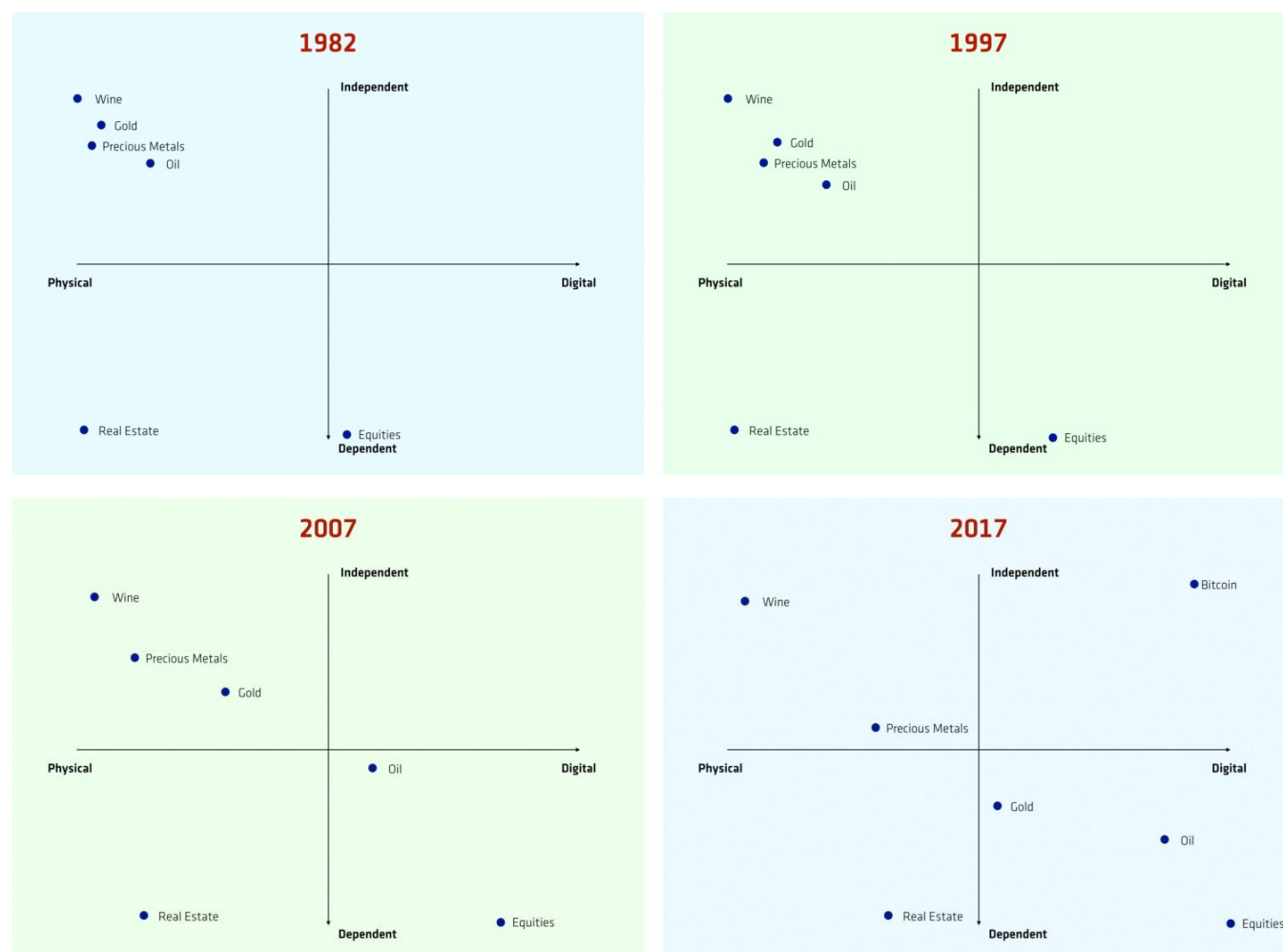
This same evolutionary phenomenon is particularly well illustrated by commodity trading, which saw a quick proliferation of interest in synthetic derivatives compared to the previously dominant physical volume. The below graphs show the relative growth in futures markets versus physical volumes for Gold and Oil.



Please note that while there are many Gold and Oil derivatives, we have used futures as a proxy to represent this digital shift. Had we

included the market for Gold ETPs, this shift would be even harder to deny.

Having plotted dependency and digitalisation on these axes, the changes between years is interesting to track (shown below from 1982–2017):



Representational Figures. CoinShares Research.

Throughout each phase of this trend, it seems that one asset leads, or paves the way, and others follow. I expect bitcoin's emergence as a new type of asset, which lives in the top right quadrant, to have a similar effect and pull other assets in this direction as well.

I believe it is likely this will occur within the 'second layer' infrastructure that is being built on top of the bitcoin blockchain. There is already technology being deployed which facilitates 'tokenisation' of real-world assets, in a format compliant with existing regulations—as my business partner [Danny Masters](#) [has touched on](#).

In the meantime, however, this category represents a tiny fraction of global assets, and in any case has clear potential for substantial growth.

So why does this matter?

Until Bitcoin was introduced, we never had a functional way to operate independently from this web of financial intermediaries in the digital sphere; no way to hedge against financial intermediaries in the same way that we could with our physical offline portfolio (e.g. physical gold, fine art, wine).

Before Bitcoin, digital investments always required a trusted third-party for settlement, clearing, and custody.

Bitcoin's 'why' is that it removes the *need* for intermediaries and provides an alternative choice to the system—not simply a spiffy facade.

That choice is an **evolution** of a trend which dates back over 35+ years now.

If we want consumers to consider adoption, we need to start thinking about how this fits in the larger context—bitcoin does not exist in a vacuum.

One of the most important features of Bitcoin is that it gives users the choice to hold a completely digital bearer asset, and manage the keys for themselves to eliminate counter-party risk.

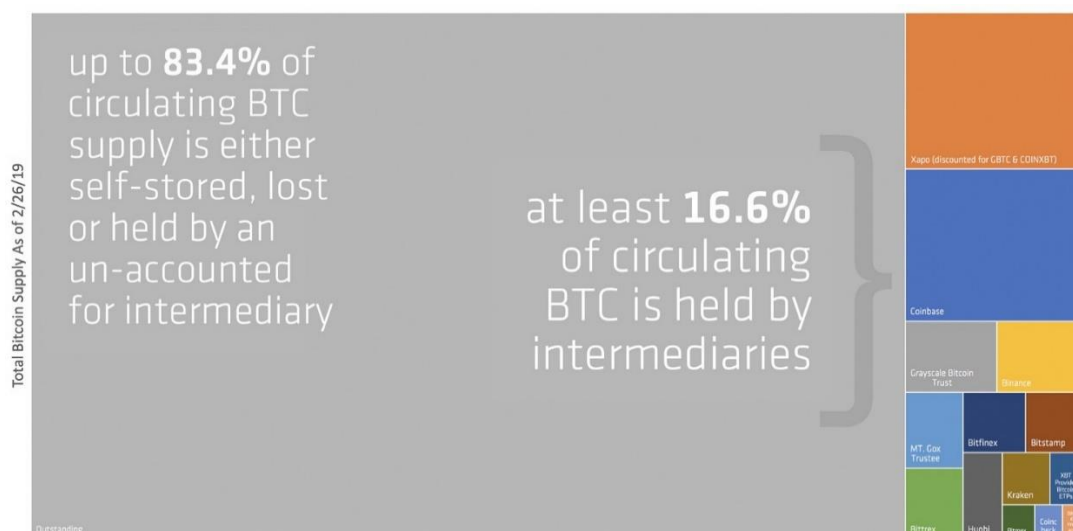
Don't get me wrong—I still expect intermediaries, lots of them in fact.

The business I run on a daily basis acts as an intermediary, offering convenience and a familiar format (ETP) in exchange for control over the underlying assets the product track. Many exchanges offer a similar proposition, acting at least as a temporary custodian for customer funds.

Custodian / Owner / Source	Amount of BTC	Current Value (USD)	% of current bitcoin supply	Date of Ref
Coinbase	856,000	\$3,259,836,320	4.875%	12/19/18
Xapo (discounted for GBTC & COINXBT)	826,997	\$3,149,386,154	4.710%	5/9/18
Grayscale Bitcoin Trust	206,525	\$786,491,342	1.176%	1/31/19
Binance	194,479	\$740,618,398	1.108%	2/26/19
MT. Gox Trustee	137,891	\$525,119,264	0.785%	9/25/18
Bittrex	130,005	\$495,087,451	0.740%	2/26/19
Bitfinex	119,538	\$455,227,307	0.681%	2/26/19
Bitstamp	108,848	\$414,518,197	0.620%	2/26/19
Huobi	108,135	\$411,801,870	0.616%	2/26/19
Kraken	79,103	\$301,239,989	0.451%	2/26/19
XBT Provider Bitcoin ETPs	53,937	\$205,405,162	0.31%	2/26/19
Bitmex	35,482	\$135,123,262	0.202%	2/26/19
Coincheck	29,838	\$113,630,506	0.170%	2/26/19
Bitmex Insurance Fund	21,719	\$82,710,893	0.12%	2/25/19
			TOTALS	
Current BTC Supply (Unknown Custody)	14,649,953		BTC In Other Hands	2,908,497
Current BTC Price (Messari)	\$3,808		Current Value (USD)	\$11,076,196,115
Current BTC Supply (Messari)	17,558,450		% of current supply	16.6%

The above table is only in regard to bitcoin holdings, not other crypto assets. Please feel free to drop a note in the comments of any products we may have missed. [You can also view our full data and sources here.](#)

A quick scan of the publicly reported bitcoin being held by an entity that is not the ultimate beneficial owner shows that at least 17% of the currently circulating bitcoin supply is likely custodied by a third-party.



CoinShares Research

Third-parties offer convenience, alleviate the hassle of key management and custody, and can streamline compliance requirements. Third-parties are not inherently good or bad; they simply offer a service to which users have grown accustomed.

But what is different about Bitcoin and this new digital paradigm is that these users finally have a choice. They have an option to utilise the convenience of these intermediaries, and the security trade-offs (risks) are clear.

*In other words, with Bitcoin the risks are right there in front of you,
and each individual has the opportunity to choose how much of that
risk to take.*

This is a huge leap forward in the evolutionary progression of our digital financial lives, especially when we consider the web of complexity and blind trust that consumers are required to place in our current financial system.

Personally, I could not be more excited for what comes next. But I'll conclude by asking a favour...

Do us all a favour—help Bitcoin, and please STOP SCREAMING ANARCHY AND REVOLUTION. We might just help the world evolve—and drive bitcoin adoption—in the process...

Much credit to many members of the CoinShares team for the contributions, edits and comments — getting this right is always a team effort.

The three core concepts of crypto

By [Anthony Pompliano](#)

Posted March 11, 2019

We are moving into a truly digital world.

In this new world, we need digitally native assets, digitally native contracts, and digitally native accounting. All three concepts are evolutions of traditional assets, contracts, and accounting, but incorporate new technology to be better prepared for the future.

We lived in an analog world with physical assets for thousands of years. In the 1970s we began a shift to the electronic world, which allowed us to transact assets by near-instantaneously moving ones and zeros on a computer screen (representations of the physical assets), but still required multiple days for the physical assets to move and settle the transaction. This shift from the analog to electronic world created enormous value and was the foundation for the world we live in today.

Half a century later, there is another shift underway – the move from the electronic world to the digital world. This transition is driven by (1) the acceleration of technology and (2) the inevitability of algorithms and machines running major aspects of the economy and our lives. In the digital world, legacy assets (and their electronic representations) are outdated technology that are too inefficient and inferior to their digital versions.

Digitally native assets are stocks, bonds, currencies, or commodities that have been created in the digital world and have an aspect of “programmability” to them. These assets have unique features that allow for near-instantaneous settlement times, micro-transactions, low fees, and are compatible with the algorithms and machines that will govern the automated world. (I always joke that “the machines don’t want our paper money!”)

Digitally native contracts (more popularly known as “smart contracts”) are software-based agreements that automatically execute based on previously agreed upon criteria. These are important for two reasons: (1) legacy contracts are incompatible and too slow for the algorithms & machines and (2) the automated world moves counterparty risk from human-led organizations to software code, which requires digitally native contracts to effectively interface with these new counterparties.

Lastly, but potentially most importantly, is digitally native accounting. When you have digital assets, you have to remember that these are simply computer files. An individual can take a computer file (ex: music file), duplicate it, and send the two separate files to two separate individuals. Neither recipient would know whether

they received the original file or the duplicate – this is not a problem when sharing music files, but becomes a big problem (known as “double spend problem”) when transacting money or valuable assets.

Digitally native accounting is a triple entry accounting system that allows for both participants in a transaction, along with a shared public ledger, to keep track of all transactions within a system. Without digitally native accounting (this is what a blockchain does), we would be unable to use digitally native assets.

These three core concepts of crypto (digitally native assets, contracts, and accounting) are accelerating the transition from the electronic world to the digital world. The creation of economic value will dwarf the value created by the shift from the analog world to the electronic world, while also allowing a more global audience to participate in the upside.

The blockchain and crypto industry revolves around a single idea – the digital world needs state-of-the-art assets, contracts, and accounting. Updating these features of the global system on the fly is like switching out airplane parts in a faulty airplane while in mid-air.

No one said it would be easy, but it is necessary. The algorithms and machines don’t want our outdated technology. We have to upgrade our assets, contracts, and accounting, or humans will continue to be the rate limiting factor of innovation and progress.

-Pomp

An Introduction to Blockchain Finality

By [Raul Jordan](#)

Posted March 7, 2019 ·

We do not truly own our digital fiat — banks do, but do we truly own our crypto assets?

Say you log in to your current bank account: you immediately see your checking account balance, your savings, how much you owe on your credit card, etc. You leave the app with a feeling of confidence that money is “yours” and any wire transfer or transactions from your cards will get “settled” by the banks the merchants without much risk. The system “works” and you trust in the system. But, **do you truly own that money?**

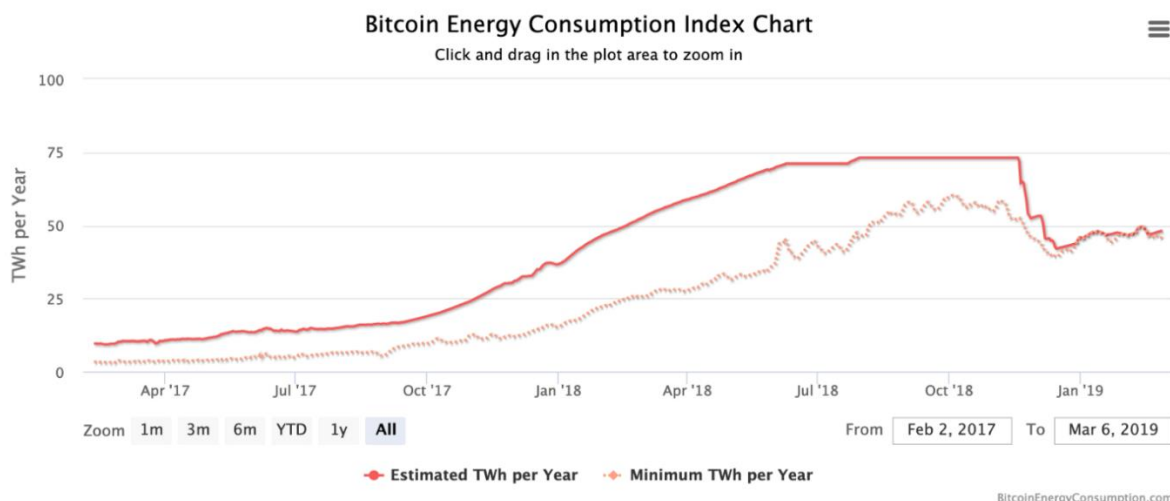
Digital ownership of assets is a concept deeply entrenched in our society since the roots of the Internet revolution. The concepts of a digital password and an email address as an identity have been accepted as standards for what were previously concrete, physical identity credentials. This phenomenon of digital ownership is not only quite artificial in nature, but it is also a highly social concept. Ownership of assets means nothing unless others recognize that ownership—namely, others whom you may wish to transact with.

Blockchain technology has reshaped our notion of what digital ownership signifies. Instead of putting our hard earned assets into the a bank, we have the ability to control the keys to personal freedom, using strong cryptography to give us the ability to move cryptocurrencies in a ledger through our wallets. But even then, do we truly **own** that money? The answer, as is in the legacy financial system, is **no**.

The concept of a blockchain wallet is, indeed, a misnomer. Wallets only store keys which give us the right to transact with a value everyone else in the protocol believes we digitally own. Indeed, users own private keys which give them access to transacting with a blockchain ecosystem, but these keys are only the credentials which unlock access to assets existing in cyberspace, namely, entries in a decentralized ledger.

This report will focus on what ownership in proof of work blockchain protocols means at the lowest level as well as explore its limits. As a first example, the power of a Proof of Work blockchain such as Bitcoin comes down to its security as a monotonically increasing function of time (that is, the security of the network only increases as time goes on). Every block coming in represents the output of a collective race to use the fastest possible machines to find an answer to a cryptographic puzzle: a competition where typically those with the highest, yet most

efficient expenditure have an edge over others. Thousands of machines and mining rigs around the world spend tens of millions in electrical energy and operational costs to participate and earn block rewards from Bitcoin and other cryptoassets.



source: digiconomist.net

The assets miners own then have value by proxy, as there was significant electrical input put into creating any one of them coupled with cryptographically guaranteed scarcity and a global, public competition that every miner agrees to participate in. Every subsequent block created by miners then leads to a cumulative increase in security on previous blocks and transactions, meaning it would require some other miner to create an entire new chain from scratch that is longer than the cumulative work put in by everyone else. This model, Proof of Work, is the basis of the security guarantees of networks such as Bitcoin and Ethereum.

Transaction Settlement: An Introduction to Finality

Participants in the network by default agree that the chain with the highest “difficulty”, or more blocks put into it, is the “canonical ledger”. Having everyone reach consensus on the canonical ledger is what truly drives the trust behind digital ownership in blockchain. If tomorrow, a new ledger is accepted as the true ledger without your transactions or coins on it, you lose out and can no longer participate in the system, as the system no longer recognizes your “ownership” despite you having a local copy.

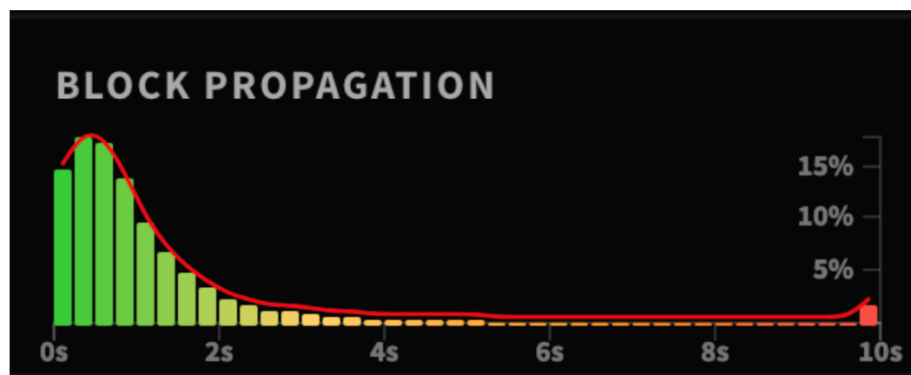
The above holds true for all longest chain variants of blockchain protocols such as Bitcoin and Ethereum as of writing. Despite this, the security guarantees of these protocols are not absolute. In these protocols, there is no **guarantee** your transactions will never get reverted or that a new, longer chain will come along in the Bitcoin protocol. That is, the notion of security in Proof of Work blockchains is

probabilistic. The more time and more blocks come in, the less likely it will be that your transactions will ever get reverted. It's quite obvious that once 50 or even 100 blocks go by the chance of a reversion occurring is neigh impossible, but it isn't entirely obvious if a single or two blocks go by. However, the longer a proof of work chain is, such as Bitcoin, the lower the likelihood its previous transactions will get reverted. This concept is known as **settlement finality**.

Reversions, or chain splits, fall into the greater umbrella of phenomena known as **blockchain forks**, in which a portion of the network has a different collective belief of what the canonical ledger is. Forking can have vast implications for digital ownership, as it is a highly social process that can happen for various reasons. In the Ethereum network, scheduled forks happen in order to upgrade the network and add new features. Sometimes, contentious forks happen in which a vocal group disagrees with decisions made in a protocol and decides to convince some part of the network to split into its own, new chain (for example, Bitcoin Cash was a very contentious fork that split from the Bitcoin Core chain).

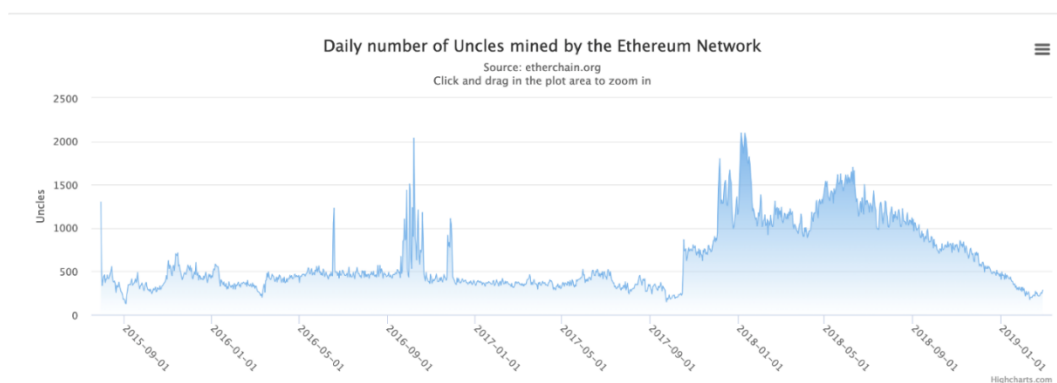
However, forking is not an uncommon, unique scenario. In fact, forking occurs at almost every block interval in Bitcoin due to network conditions. Since not everyone can see broadcast blocks at the same time, two miners might create **perfectly valid blocks**, but only **one** will be rewarded in the end by the protocol.

Blockchain networks are imperfect, as anyone in the world can run a node. With all sorts of Internet connections and latency issues, blocks often take longer to propagate throughout bigger networks, and those offer more time for potential forks to occur in the intervals between consensus.



latest block propagation times of the Ethereum network, source: ethstats.net

Blocks that are valid but fail to be included in the ledger the majority of the network accepts are referred to as **uncle** blocks. In Ethereum, these miners creating orphaned blocks are rewarded a small amount for their efforts, and the rate at which these orphans are created is known as the "uncle rate".



uncle rate peaked after the highest point in the late 2017 hype cycle, source: etherchain.org/charts

This value serves also as a great proxy of network latency and inefficiencies in Ethereum. That is, if blocks are using too much gas (using too much computation), these blocks will be larger in size and take longer to propagate throughout the network, increasing the probability of more uncles happening throughout. In times of high usage, the network becomes congested, and tons of these uncles happen at a higher rate than usual.

Forking and the possibility of chain reorgs are the reasons why exchanges such as Coinbase take a while for you to be able to use coins you receive or send out of the exchange, typically waiting around 30 blocks as a safe confirmation timeframe as exchanges try as much as they can to ensure a high probability their users will not lose ownership of their respective assets.

Alternatives & Tradeoffs

So in Bitcoin and Ethereum as they stand, participants can only increase their likelihood transactions will not get reverted over time, but can never be 100% certain. This concept is baked into the protocol itself, as it depends on the network deciding the “real”, canonical ledger is the one with the most blocks and highest difficulty put into it. **Are the protocols where transactions can reach explicit finality? What are the tradeoffs?**

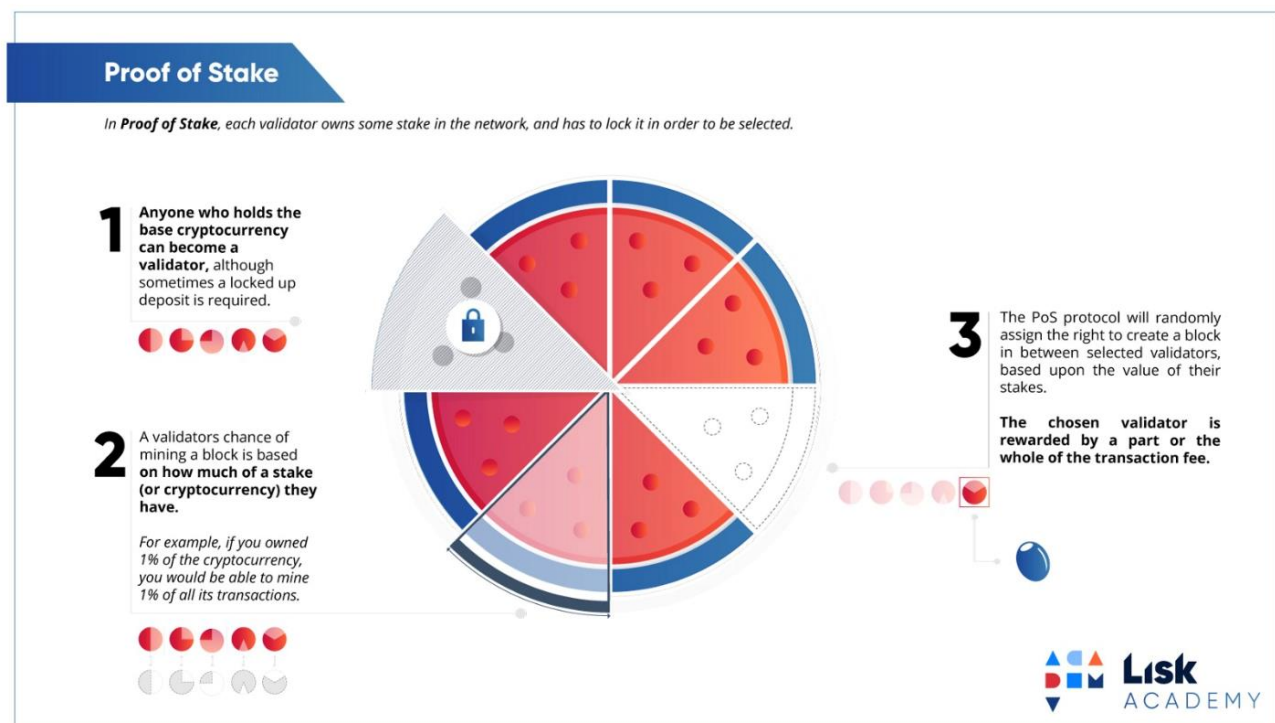
A key alternative to Bitcoin’s proof of work is proof of stake: a mechanism in which participants lock up and “stake” some cryptoasset in order to participate in reaching consensus on a global ledger. If participants act maliciously, they risk losing their full stake or a large portion of it, creating a mechanism that is based on **penalties rather than rewards**. Ethereum has always wanted to transition to proof of stake, and efforts are [well underway](#) to create the next iteration of the Ethereum protocol.

In proof of stake based protocols that are based on a variant of the longest chain decision rule, there is no notion of real world, electrical expenditure required to

create a longer chain, so there are no cryptographic guarantees of when transactions can be considered **final**. Instead, these protocols opt for baking in settlement finality as a fixed parameter. That is, these protocols state that after X blocks, transactions can **never** be reverted, and everyone operates by the rules of that protocol. That also means that there is no incentive to maintain or store the entire history of transactions before every finalized period, which is a major tradeoff of this approach. In Bitcoin, new nodes joining the network independently download and verify the entire ledger since the first block, reaching the same “truth” as the other participants effectively.

How Proof of Stake Systems Achieve Finality

Proof of Stake mechanisms such as Ethereum’s [Casper the Friendly Finality Gadget](#) rely on deposit-weighted votes received by a group of validators (the proof of stake term for miners) to decide on when to finalize a certain sequence of blocks. That is, nodes in the network have a built in protocol which says to disregard blocks before a certain point in time for consensus if certain conditions are met. Typically, this vote threshold is in line with [Byzantine Fault Tolerance](#) to ensure that at least 2/3’s of the validator balances voted in a given period of time as a safety measure.



source: lisk academy

In Proof of Stake based models which have “finality checkpoints”, new nodes that join after a **long period of time** instead only need to verify the state of the ledger since the last finalized checkpoint. That is, if the protocol specifies that every 1000

blocks where a certain threshold of votes was reached, transactions at that point **cannot be reverted**, as new nodes only need to accept the truth from that point on and need not care about preceding blocks. Verification of the state of the world becomes more subjective than objective in this scenario. In fact, Vitalik Buterin [quotes](#) this property of Proof of Stake as **weak subjectivity**.

What Does This Mean for the Average User?

For the average user interacting with the blockchain, similar to how ownership of fiat assets stored in a bank work today, assets on a blockchain are merely records in a ledger. For fiat money in a bank, your ownership of your money exists because there are records in its centralized database attesting your balance. In blockchain, users only own their cryptoassets because the majority of a protocol accepts their ownership as being part of some “hard truth” (i.e. what we call a “canonical” ledger). If tomorrow, the chain gets attacked and a deep block reorg happens without your transactions in it, your private keys and wallet are useless. Even if you “have” the coins, the majority of the protocol thinks you do not. *Digital ownership on a blockchain carries a risk as big as the security flaws of its underlying protocol.*

It is important to remember consensus is a social process, and even in blockchain, settlement finality is not 100% guaranteed. Blockchain finality, however, provides an important, new primitive that helps us question how we reason about digital ownership, security, and the social nature of consensus, both in traditional systems and in the bleeding edge of this new technology.



Privacy and Cryptocurrency, Part I: How Private is Bitcoin?

By [Eric Wall](#)

Posted March 7, 2019

Foreword

The [Human Rights Foundation](#) cares deeply about protecting our civil liberties and privacy in our increasingly digital age, especially in places where people live under authoritarian governments. Without a free press, without local watchdog organizations, and without effective ways to hold governments accountable, the 4 billion people who live under authoritarianism need our help, and technology is one way we can reach out. As we've seen with the evolution of encrypted messaging, virtual private networks, and free knowledge initiatives like the Tor Project, Wikipedia, and Signal, technology can be a liberation tool, if built with the right values in mind. But as we've seen with centralized platforms ranging from Facebook to WeChat, technology will also be a tool of surveillance and even social engineering.

Unless we take a stand now, and help make platforms and protocols with user privacy and decentralization in mind, mass surveillance and social credit may be the inevitable future. To help elevate this conversation, the [Zcash Foundation](#) has provided generous support for HRF to bring Eric Wall on as a Technology Privacy Fellow. Eric will be working with HRF for the next six months, writing five essays on privacy technology, with a special focus on cryptocurrency and how we can preserve privacy in the financial world. We look forward to sharing Eric's work with you, and seeing it inspire fresh conversations with policymakers, philanthropists, investors, students, and the builders of our current and future technology infrastructure.

— Alex Gladstein
Chief Strategy Officer
Human Rights Foundation

Key points:

If you're an activist or a journalist, you may wonder how safe it is to use bitcoin to escape the prying eyes of a government or corporation

Bitcoin is only semi-private; the protocol doesn't know your real name but transactions can still be linked to you in a myriad of ways

Blockchain analytics firms specialize in deanonymizing bitcoin activity and sell this data to corporations and law enforcement agencies

A grasp of how the system works and use of tools such as Tor, coin control, CoinJoin transactions and avoiding address reuse can make a crucial difference in protecting your identity and transactions from being unmasked

This article aims to give the reader a primer on Bitcoin privacy—later articles in the series will look at different wallets, compare different cryptocurrencies and survey exchange platforms in regions with restricted economic and political freedom

Why cryptocurrencies?

It's clear from the onset when observing cryptocurrencies at a protocol level that they are inherently more privacy-oriented than traditional digital payment systems. At the base layer of these protocols, there is typically no mapping between users' cryptographic key pairs and their real-world identities, yet they allow us to store and transfer wealth across the globe with an unprecedented degree of freedom.

The intention of the Human Rights Foundation is to examine these technologies and elucidate on their potential of bringing economic and political freedom to the individual. While there are many angles in the context of money that are within the scope of such an endeavor, we've chosen to focus on the topic of privacy foremost. In that pursuit it's also clear that the degree to which cryptocurrencies enable privacy is not by any means trivial or binary—it varies greatly depending on the user's particular choice of core and ancillary technologies and usage patterns, as well as the capabilities and sophistication of the attacker.

Regardless of that, we can observe that the adoption rate of cryptocurrencies—in particular, bitcoin—is increasing in countries where the economic freedom of the population is limited. While the liberating and democratic aspects of cryptocurrencies are apparent, especially the extent to which they enable censorship-resistant transaction networks and monetary policies impervious to various forms of government sabotage, none of these benefits are particularly helpful as long as authoritarian regimes can deanonymize and prosecute the users of these currencies at will.

Many thanks to Matt Ahlborg for lending us this visualization from his great piece [“Nuanced Analysis of Local Bitcoins Data Suggests Bitcoin is Working as Satoshi Intended”](#) which explains the exact methods used to generate it.

The ambition of this initiative is to cut through the complexity of the cryptocurrency privacy subject by sourcing subject matter expertise from the industry. When we

approach this subject, we recognize that we enter into a complex field, and as in any complex field, experts disagree. We will strive to strip this initiative from personal biases and condense opinions and research into simple practical guidelines.

The product of this research will be an article series of which this is the first piece.

A primer on Bitcoin privacy

Bitcoin is neither completely anonymous nor completely transparent. The Bitcoin privacy conundrum exists in a grey area where the unmasking of a user's financial activity ultimately depends on the capabilities of the adversary and the sophistication of the user and their choice of tools. There is no perfect privacy solution for any activity on the Internet, and in many cases, privacy-conscious choices come with tradeoffs to both cost and ease-of-use where no one-size-fits-all solution exists. Moreover, privacy is never a static thing but evolves continuously and in response to the battle between those who build tools to protect privacy and those who build tools to destroy it.

The Bitcoin protocol itself evolves over time, which can lead to dramatic changes in its privacy properties. Changes to the core protocol are seldom simple choices between privacy and transparency alone, but more often come packed with changes to the security, scalability, and backward-compatibility of the software as well. Historically, the trend and ethos within the Bitcoin community has always favored privacy over transparency, but more conservatively so compared to other cryptocurrencies where privacy is the primary focus.

As a result, activists or journalists who are considering using bitcoin to escape the prying eyes of an authoritarian government or a corporation need to understand what type of traces they leave when they're using it and whether the privacy nature of bitcoin is sufficient for their needs. However, achieving this understanding requires some amount of effort.

Tracing transactions

When you transact on the Bitcoin network you leave two types of traces. These can be categorized into "what's on the blockchain" and "what's not on the blockchain". The information that is on the blockchain reveals no direct link between your identity and your transactions, but it does reveal information that can link your transactions to each other. What does link your identity to your transactions are the things in the second category: "what's not on the blockchain".

What's not on the blockchain

When you transact on the Bitcoin network, you are sometimes sending or receiving money to/from some entity that knows who you are. That entity will then have outside-of-the-blockchain-knowledge that links your identity to a transaction.

When you combine this fact with the other fact that your transactions can be linked to each other, the result is that motivated entities can sometimes figure out how you're using your bitcoins, how much you have and who you've been transacting with.

There are also countless ways you could be linked to a transaction even *without* having transacted with an entity that knows who you are, since Bitcoin transactions are typically sent in unencrypted packets over the Internet and the source IP address can be pinpointed through various means. Bitcoin transactions sent via [full nodes](#) such as Bitcoin Core require some triangulation or targeted traffic sniffing in order for the source IP address to be estimated, whereas other “light” wallets such as mobile wallets (Mycelium, Blockchain Wallet, Coinbase Wallet) will often broadcast transactions through company-run servers that can see your IP address directly and your full transaction history. The same is true for most hardware wallets (Ledger, Trezor) in their out-of-the-box setups.

Geolocation IP databases can often roughly approximate your physical location using your IP address. You can test it out yourself using this [link](#), then enter the coordinates you get into an interface like Google Maps. More importantly, your IP address reveals your Internet Service Provider (ISP), which in turn knows the real-world identity of the owner of your IP address and often has a legal obligation to store this information for several months.

Even if you are using a public WiFi network to transmit your transactions, you could still accidentally associate your real identity with that IP address from the websites you visit and the background services your device connects to. Your Dropbox application will gladly connect to Dropbox's company servers when you start your laptop which will associate that IP address with your Dropbox account in Dropbox's server logs. The same thing will happen when you browse to a personal account on any website. Even if you don't visit any personal web accounts, cookies stored on your laptop can reveal who you are to the website you browse to through your cookie's association to your previous browsing history. Many websites allow third parties to track users like this for analytics purposes—Google alone is estimated to track users across 80% of the sites of the entire web.

Even if you clear your cookies, website operators can track you across their different sites as long as your [browser fingerprint is unique](#) and associate your IP address to your identity that way. And even if you have no services running and avoid browsing altogether, your device's [MAC address](#) could get exposed to the network provider

which could be [linked to your identity using sophisticated methods](#). So, even if your IP address doesn't lead back to you via an ISP record, you might still leave other traces that do when you're using your personal devices.

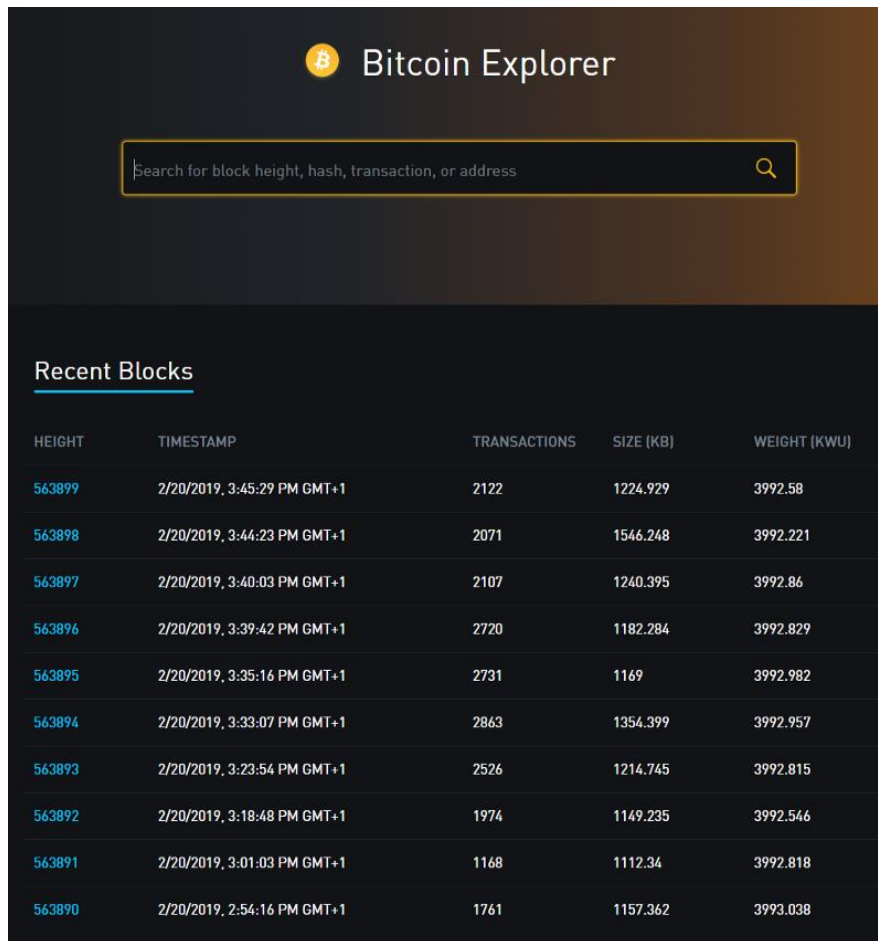
The worst category for privacy is of course when using third-party services that implement know your customer (KYC) practices as your Bitcoin wallet, as these services will keep logs of all your transactions and your real-world identity.

You could also be linked to a Bitcoin address or transaction just by searching for it using web-based tools since there usually aren't that many people other than you who are going to be looking up your transactions on the web for no good reason. Keep this in mind as we move to the next segment. Other data that isn't on the blockchain but can easily be logged about your transaction is the approximate time it was broadcast to the network.

The current known best method to hide your source device and IP address when retrieving information about transactions or when transmitting transactions is to leverage Tor hidden services. Many wallets including Bitcoin Core will provide this as a [configurable option](#) while others have it built-in. The [Tor browser](#) can similarly be a useful tool for your web-based Bitcoin-related activity as it, in addition to hiding your IP address, clears cookies upon each exit, prevents third-party cookies and is immune to most browser fingerprinting techniques.

What's on the blockchain

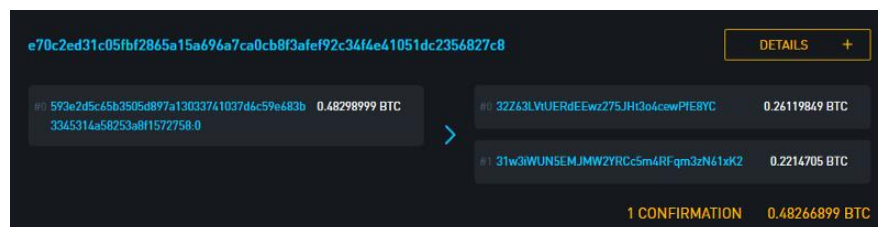
A simple way to begin understanding what type of information is revealed by the Bitcoin blockchain is to use a block explorer. For this exercise, we'll use the open-source explorer [blockstream.info](#).



The screenshot shows the Bitcoin Explorer interface. At the top, there's a search bar with the placeholder text "Search for block height, hash, transaction, or address". Below the search bar, the "Recent Blocks" section is displayed as a table with five columns: HEIGHT, TIMESTAMP, TRANSACTIONS, SIZE (KB), and WEIGHT (KWU). The table lists the most recent blocks, with the top entry being block 563899.

HEIGHT	TIMESTAMP	TRANSACTIONS	SIZE (KB)	WEIGHT (KWU)
563899	2/20/2019, 3:45:29 PM GMT+1	2122	1224.929	3992.58
563898	2/20/2019, 3:44:23 PM GMT+1	2071	1546.248	3992.221
563897	2/20/2019, 3:40:03 PM GMT+1	2107	1240.395	3992.86
563896	2/20/2019, 3:39:42 PM GMT+1	2720	1182.284	3992.829
563895	2/20/2019, 3:35:16 PM GMT+1	2731	1169	3992.982
563894	2/20/2019, 3:33:07 PM GMT+1	2863	1354.399	3992.957
563893	2/20/2019, 3:23:54 PM GMT+1	2526	1214.745	3992.815
563892	2/20/2019, 3:18:48 PM GMT+1	1974	1149.235	3992.546
563891	2/20/2019, 3:01:03 PM GMT+1	1168	1112.34	3992.818
563890	2/20/2019, 2:54:16 PM GMT+1	1761	1157.362	3993.038

The most recent block at the time of writing (#563899) in the Bitcoin blockchain contains 2122 transactions. Let's look at what a randomly chosen transaction reveals.



The screenshot shows the details of a Bitcoin transaction. At the top, the transaction ID is displayed: e70c2ed31c05fbf2865a15a696a7ca0cb8f3afef92c34f4e41051dc2356827c8. Below this, the transaction is broken down into inputs and outputs. The input is a single entry from address 592e2d5c65b3505d897a13033741037d6c59e683b with an amount of 0.48298999 BTC. There are two outputs: one to address 32263LVUERdEEwz275JH3o4cewPIE8YC for 0.26119849 BTC, and another to address 31w3WUN5EMJMWZYRCc5m4RFqm3zN61xdQ2 for 0.2214705 BTC. At the bottom, it shows "1 CONFIRMATION" and a total of 0.48266899 BTC.

Transaction ID: e70c2ed31c05fbf2865a15a696a7ca0cb8f3afef92c34f4e41051dc2356827c8	
Input:	Output:
#0: 592e2d5c65b3505d897a13033741037d6c59e683b 0.48298999 BTC	#0: 32263LVUERdEEwz275JH3o4cewPIE8YC 0.26119849 BTC
3345314a58253a8f11572758-0	#1: 31w3WUN5EMJMWZYRCc5m4RFqm3zN61xdQ2 0.2214705 BTC
1 CONFIRMATION 0.48266899 BTC	

Transactions contain inputs and outputs and are identified by transaction IDs (seen at the top in the image above). If your Bitcoin wallet has sent a transaction, each transaction will be associated with one such identifier.

From a high-level view, what is revealed about this transaction is the following:

- The approximate time the transaction was mined (from the block header)
- The addresses bitcoins were sent to and the amounts sent (i.e. the “transaction outputs”)
- The source of the funds for the transaction (i.e. the inputs)

Let's look at each of these items individually for the transaction shown above, [e70c2ed31c05fbf2865a15a696a7ca0cb8f3afef92c34f4e41051dc2356827c8](#).

Time

Transactions are not timestamped, but blocks are. Block timestamps are not necessarily precisely accurate, but assuming a majority of miners are reporting time honestly, all blocks are bound to be reasonably accurate within a few hours range. For the blocks mined by the honest miners, they'll be precisely accurate. This doesn't mean that the block timestamp is necessarily accurate within a few hours range to *its transactions' broadcast times* however, since it can sometimes take a lot longer for a transaction to be included in a block. Some block explorers complement data this by displaying the time they first saw a transaction on the network to give a more accurate view of transactions' broadcast times.

The approximate time when the transaction above was included in a block can be derived by looking at the block header (in our case it's block #563899 with the timestamp 2019-02-20, 14:45 UTC).

The addresses bitcoins were sent to and the amounts sent

The receiving addresses in this transaction are:

- 1: [32Z63LVtUERdEEwz275JHt3o4cewPfE8YC](#) 0.26119849 BTC
- 2: [31w3iWUN5EMJMW2YRCc5m4RFqm3zN61xK2](#) 0.2214705 BTC

There is more to an address than what meets the eye. It's easy to think of Bitcoin addresses as "hard-to-read email addresses but for bitcoins", but an address isn't always a simple pointer to a certain user's cryptographic key-pair. What addresses are in reality, are cryptographic descriptors of the *spending rules* for the next time someone wants to move those bitcoins.

For example, if you send bitcoins to [37k7toV1Nv4DfmQbmZ8KuZDQCYK9x5KpzP](#), the configuration of this address is such that you're not sending bitcoins to an owner of a particular private key, but rather to a spending rule that releases the coins to [anyone who can provide two different strings that have the same SHA-1 hash](#) (this would mean that the SHA-1 hash function is broken, which it was in 2017— so don't send anything to that address!). What's good to note is that since many address formats used today are [hashed](#) when we send bitcoins to them, we typically can't tell what those spending rules are until someone spends bitcoin from that address, as they need to reveal what was hashed in order to do so.

In our example transaction, the blockchain reveals that bitcoins have been spent from both addresses, so the spending rules for those addresses are known.

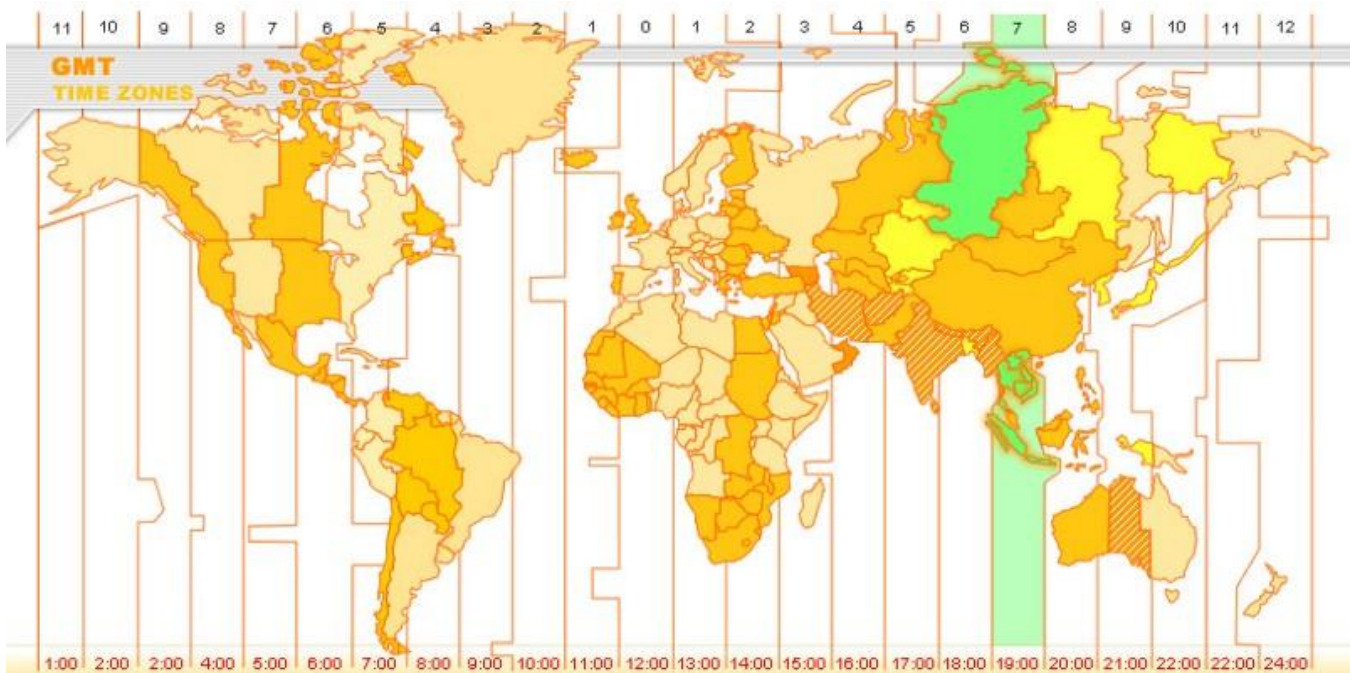
[32Z63LVtUERdEEwz275JHt3o4cewPfe8YC](#) was revealed to be a 2-of-2 [multisignature](#) address when it was spent from in the transaction [f491dfe9867c36e85950116a90a6128060d6070866ad0f3598d70d146750162f](#). We'll look at exactly how that information is revealed in the next section.

Similarly, it was revealed of [31w3iWUN5EMJMW2YRCc5m4RFqm3zN61xK2](#) that it is a frequently used 2-of-3 multisignature address and at the time of writing holds roughly 2,700 bitcoin (US\$10.6m). More advanced blockchain tools such as [oxt.me](#) will even plot the wallet balance over time and display with approximate accuracy which hours of the day it has seen the most activity.



Historical balance and activity relating to the address [31w3iWUN5EMJMW2YRCc5m4RFqm3zN61xK2](#) ([oxt.me](#)).

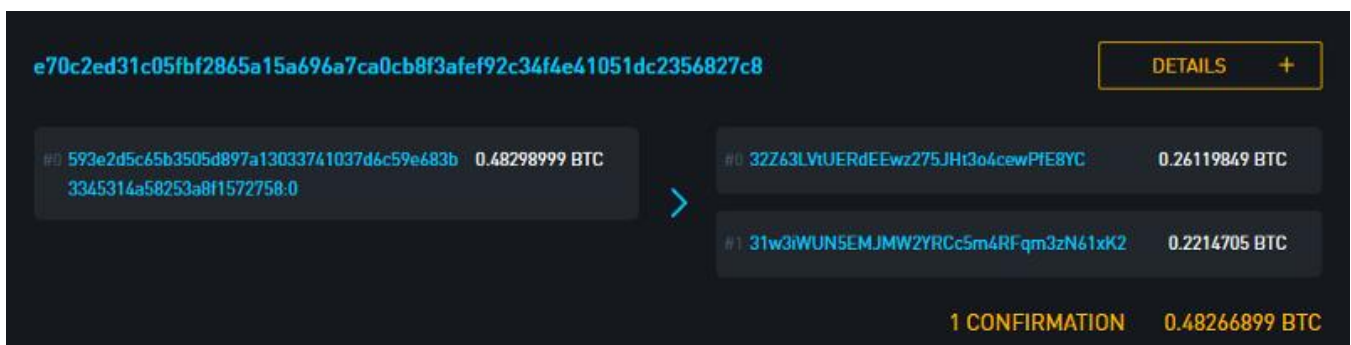
Seeing as 18:00-22:00 UTC are the hours with the least activity for this address, it wouldn't be unreasonable to assume that these hours represent the night-times 01:00-05:00 or 02:00-06:00 in the region where the address is controlled. Given the hours of activity, the volumes and the multisignature setup of this address, one could guess that this address belongs to a cryptocurrency exchange in the GMT+7/8 time zones.



It's considered good privacy hygiene to never reuse a Bitcoin address because it helps to break transaction linkage. That's also a good idea for all users of [P2SH](#) addresses (all addresses starting with a "3" and 62-character addresses starting with "bc") because by the time you reveal what the spending rules are for that address, you've already sent the bitcoins to a new, hashed address for which the spending rules are yet unknown.

Wallets known as [HD wallets](#) can generate many addresses but only require a single back-up seed in order to access the funds. These wallets will also automatically generate a fresh address for you every time you've received a transaction.

Now let's look at the transaction again to see what else we can reveal about the sent coins.



Bitcoin transactions are regularly directed towards two addresses where one of the transaction outputs is the actual payment and the other is what is known as a "change output" going back to the sender. It's similar to when you pay for a \$3 item

with a \$5 bill, it creates two payments; one of \$3 to the merchant and one with the change of \$2 going back to the one paying.

Identifying a transaction output as a change output requires the use of [heuristics](#). Examples of heuristics that can be used to discern a change output from the other payment are; the usage of round numbers (in the bitcoin amount or in the fiat currency value of the amount at the time of the transaction), the order of the outputs in the transaction body and so on. In our chosen transaction, it's easy to detect the change output because it's going back to the same address that was used to receive the bitcoins that were spent, as we'll see below.

In principle, Bitcoin wallets behave somewhat differently from each other and leave different traces on the blockchain—similar to how browsers reveal pieces of information about themselves when they browse the web. Because of this, it is sometimes possible to identify certain transactions as originating from a certain kind of Bitcoin wallet application.

If your adversary knows which wallet application you're using then that knowledge can contribute to mapping your identity to one of your transactions, which would weaken your privacy. Every little piece of information helps an adversary paint a picture of who you are and what you are doing.

The source of funds for the transaction

In Bitcoin transactions, the “source of funds” is always other “unspent” transactions, or to be precise, unspent transaction outputs (known as UTXOs). It's good to keep in mind that what is seen in a block explorer is a combination of decoded raw blockchain data and *derived* data. One block explorer might choose to display the transaction like this:

e70c2ed31c05fb2865a15a696a7ca0cb8f3afe92c34f4e41051dc2356827c8		
31w3iWUN5EMJMW2YRCc5m4RFqm3zN61xK2 (0.48298999 BTC - Output)	➡ 32Z63LVtUERdEEwz275JHt3o4cewPFE8YC - (Spent) 31w3iWUN5EMJMW2YRCc5m4RFqm3zN61xK2 - (Spent)	0.26119849 BTC 0.2214705 BTC
		0.48266899 BTC

From blockchain.com.

Here the “source of funds” is displayed as an address. Blockstream's explorer chooses to display it like this, where the source of funds is displayed as a transaction:

e70c2ed31c05fbf2865a15a696a7ca0cb8f3afef92c34f4e41051dc2356827c8

DETAILS +

#0 593e2d5c65b3505d897a13033741037d6c59e683b3345314a58253a8f1572758.0 0.48298999 BTC

#0 32Z63LVtUERdEEwz275JHt3o4cewPFE8YC 0.26119849 BTC

#1 31w3iWUN5EMJMW2YRCc5m4RFqm3zN61xK2 0.2214705 BTC

1 CONFIRMATION 0.48266899 BTC

The reason why Blockstream's explorer doesn't show an address as the source of funds is that addresses aren't technically a part of the inputs to a transaction and it isn't always possible to infer the notion of an originating address ([example](#)). Moreover, since address reuse is discouraged, it's good to break inherited mental models from traditional payment systems and not further cement the idea that money could or should be sent back to the recipient at the same address by showing addresses as senders.

Let's get more technical for a moment and look at the decoded raw data of the transaction, which you can fetch from your own local copy of the Bitcoin blockchain if you run a [full node](#) ([or by using a trusted web-based interface](#)). Here's what it looks like:

```

1 $ bitcoin-cli getrawtransaction e70c2ed31c05fbf2865a15a696a7ca0cb8f3afef92c34f4e41051dc2356827c8
2 {
3   "version": 2,
4   "locktime": 0,
5   "vin": [
6     {
7       "txid": "593e2d5c65b3505d897a13033741037d6c59e683b3345314a58253a8f1572758",
8       "vout": 0,
9       "scriptSig": "0020fa28dc1e5eb22055e90f8cade9bcd13ca9ddab7a5ed029e27d41a736f7455ce",
10      "txinwitness": [
11        "",
12        "304402204d969f7102fd24009c21533e65c506f2083e0c372994a5e724c2ba831ce42f1
13        10220623958a13694d19b7c3a65553d862d04d67dec565969594c1a2cd26afb8de9801",
14        "30440220235ec716247a2a2dfae4aeae6c16bac3be4055b70c7585f4cf25a77b30775d
15        5022011771761f11dd8f040c9a2dcd15e1e0ef88f0cfb7b4b1f7037d384622e4bef7501",
16        "5221027111c0d6cbc3a40c6e6197ed234bd6e59f277c88094fd33297b1e0a3787a5b7d2
17        102e71711c9840d68e6401d4bd5df78f1850e25ae41f082f4b38ceec37d60cab5442103
18        eeae18900c0d12046f644b960a1ef84589f7f4f71d07914006d550bf85c576e153ae"
19      ],
20      "sequence": 4294967294
21    }
22  ],
23  "vout": [
24    {
25      "value": 0.26119849,
26      "scriptPubKey": "OP_HASH160 09783c21e42b639f4f91819706aa42949361762c OP_EQUAL",
27    },
28    {
29      "value": 0.22147050,
30      "scriptPubKey": "OP_HASH160 02a751dc8c10e35fed2c6eddc2575c9af2c71d23 OP_EQUAL",
31    },
32  ],
33  }
34 }
35

```

[e70c2ed31c05fbf2865a15a696a7ca0cb8f3afef92c34f4e41051dc2356827c8](#) decoded (manually trimmed).

The source of funds is described by the `vin`-array. It doesn't refer to an address specifically. Instead, it refers to the output of a previous transaction;

[593e2d5c65b3505d897a13033741037d6c59e683b3345314a58253a8f1572758](#), where `vout: 0` refers to that transaction's *first* output (`vout: 1` would mean its second output, and so on). This unspent transaction output (UTXO) is the *source of funds*.

To clarify what this means, the source of funds for a transaction is not an address, nor is it a transaction. The source of funds is a specific *output* of a specific previous transaction. Knowing this will help you protect your privacy when using bitcoin, as we'll see in later sections.



The source of funds for

[e70c2ed31c05fbf2865a15a696a7ca0cb8f3afef92c34f4e41051dc2356827c8](#).

We can further decode parts of this transaction from the decoded raw data such as what's in `txinwitness` to find out more about the source of funds. The last hexadecimal string in `txinwitness` reveals the 2-of-3 multisignature script, which allowed us to deduce that it's likely to be an exchange wallet.

```
1 $ bitcoin-cli decodescript
2 5221027111c0d6cbc3a40c6e6197ed234bd6e59f277c88094fd33297b1e0a3787a5b7d
3 2102e71711c9840d68e6401d4bd5df78f1850e25ae41f082f4b38ceec37d60cab54421
4 03eeae18900c0d12046f644b960a1ef84589f7f4f71d07914006d550bf85c576e153ae
5
6 {
7   "result": {
8     "asm": "2 027111c0d6cbc3a40c6e6197ed234bd6e59f277c88094fd33297b1e0a3787a5b7d
9           02e71711c9840d68e6401d4bd5df78f1850e25ae41f082f4b38ceec37d60cab544
10          03eeae18900c0d12046f644b960a1ef84589f7f4f71d07914006d550bf85c576e1
11          3 OP_CHECKMULTISIG",
12     "reqSigs": 2,
13     "type": "multisig",
14     "addresses": [
15       "164GApvfW9FkteXYS2J6RsSp262dEBxF6H",
16       "1A4PaXs5CJRy2BLN5wXxqYKpjvia9T8v8c",
17       "1Q55L1VQ616mCdrQD9jwUSqZGeiSDhRBs9"
18     ],
19   },
20 }
```

The two other hexadecimal strings we saw in the `txinwitness` are just the signatures fulfilling this 2-of-3 multisignature condition.

Now that we've identified the source of funds, we can see in this example that it's a 0.48298999 bitcoin output (~US\$1850), even though the sent payment was just one of ~US\$1000. This has an undesirable consequence: imagine a situation in which a friend pays you \$10 but the transaction reveals that he's the owner of a million dollars and has immediate access to send the full amount— obviously not very good for privacy. If you are worried about disclosing information about your bitcoin wealth when you are sending a payment to someone, you need to be aware of which inputs are used in your transactions (more on this below).

Combining the knowledge

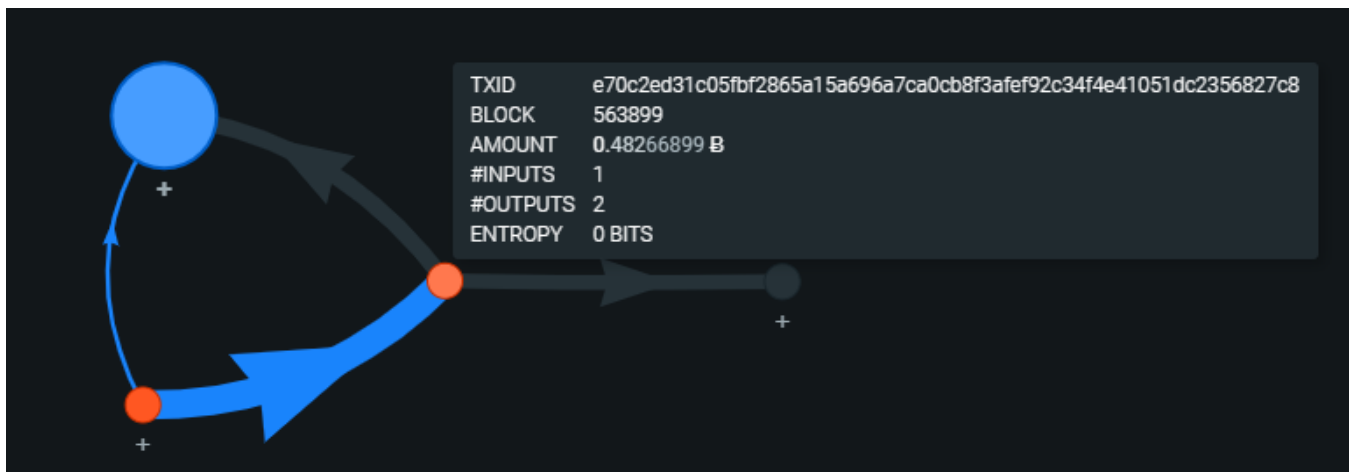
Because transactions always need to provide the source of funds, transactions become linked together, producing what's known as a transaction graph. If you pay a friend in bitcoin, not only will your friend see the inputs you used in the transaction, but you will also be able to see when your friend spends those coins and to which addresses the coins are sent.

Some addresses are known in the Bitcoin space, such as the [Bitfinex cold wallet](#) or the [seized Silk Road coins](#). An address can become known because an entity—for example, a business or a charity—advertently exposes their deposit or donation addresses on their website, or inadvertently because a forum post or a law enforcement record publicly reveals the connection. Blockchain analytics firms will scrape the web regularly to find such information.

Other addresses become exposed via association through a technique called clustering.

Clustering

Let's go back to our example transaction from the previous examples, [e70c2ed31c05fbf2865a15a696a7ca0cb8f3afef92c34f4e41051dc2356827c8](#). Here, we can immediately see that both the source of funds of our transaction and our transaction (red dots) have been used to jointly fund a third transaction (big blue dot).

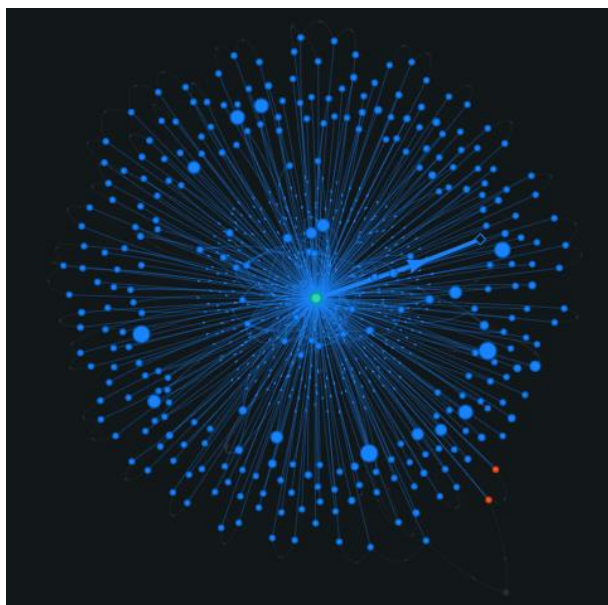


Transaction graph for [e70c2ed31c05fbf2865a15a696a7ca0cb8f3afef92c34f4e41051dc2356827c8](https://oxt.me/e70c2ed31c05fbf2865a15a696a7ca0cb8f3afef92c34f4e41051dc2356827c8) (oxt.me).

Particularly, it's the [second output of the funding transaction](#) and the [first output of our transaction](#) that are involved in funding this transaction. They were previously sent to the addresses:

[3Qt1YaJwQwtHMB4mjJ41DZVawWXih9LGMq](#)
[32Z63LVtUERdEEwz275JHt3o4cewPfE8YC](#)

On the surface, these appear to be two separate addresses with just one innocuous-looking incoming and outgoing transaction each. But because their private keys have both been used to sign the big blue dot transaction, these addresses now all belong to the same *cluster* (along with 407 other addresses involved in the inputs to the transaction), which we can make assumptions about having the same owner. This heuristic has gone under a couple of different names in the past, the most recent one being the [common-input-ownership-heuristic](#).



Transaction graph for “the big blue dot” transaction [f491dfe9867c36e85950116a90a6128060d6070866ad0f3598d70d146750162f](https://oxt.me/f491dfe9867c36e85950116a90a6128060d6070866ad0f3598d70d146750162f) (oxt.me).

Blockchain analytics firms will use such heuristics to create giant clusters. The blockchain explorer WalletExplorer has pinned the two addresses to belong to a cluster of [162787 addresses](#) in total. Analytics firms label such clusters with all identities (IP addresses, user accounts, organizations, real names) they’re able to pin to the cluster in order to map out the Bitcoin transaction ecosystem. They then sell access to these data sets to law enforcement agencies and other companies.

Many blockchain analytics firms receive information about transactions directly from their own customers, such as cryptocurrency exchanges. However, two of the largest analytics firms, Chainalysis and Elliptic, have stated that they do not trace back transactions to specific individuals in the data they receive, but only to the exchanges or other business entities ([1](#), [2](#)).

It only takes the deanonymization of one address in a cluster to deanonymize an entire cluster.

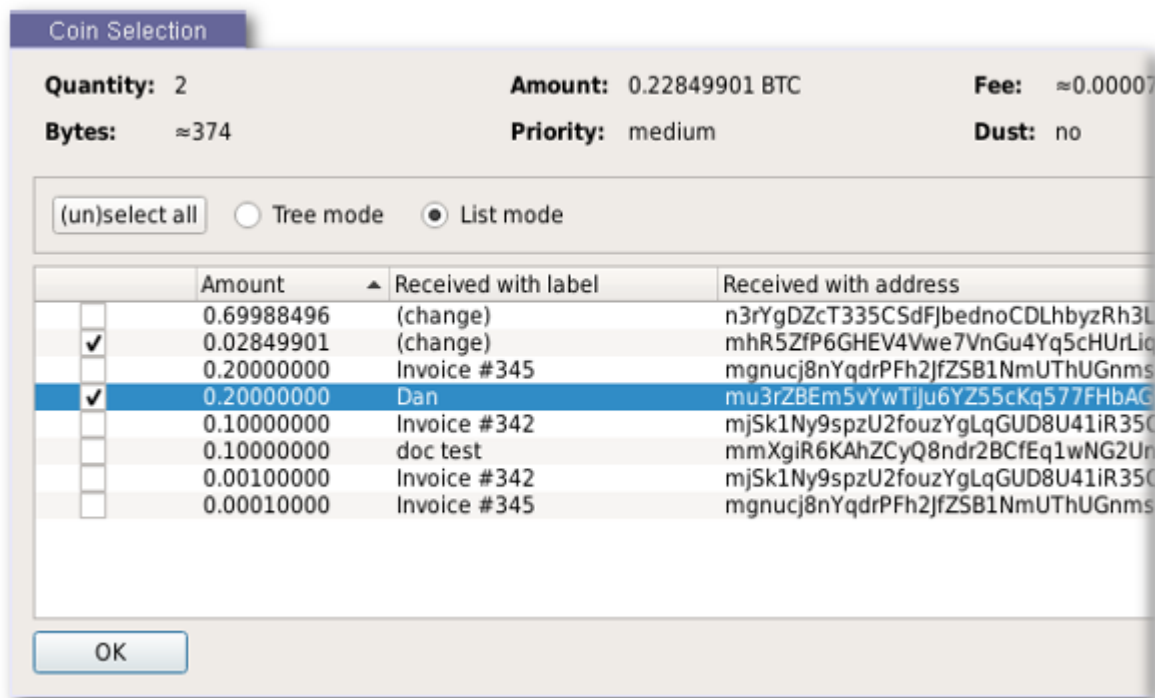
Breaking the heuristics

We’ve seen now that there are a multitude of ways your identity can be linked to a certain Bitcoin address or transaction and yet another multitude of ways your Bitcoin transactions can be linked to each other. When put together, these information leaks in combination can unmask our entire financial privacy.

Some Bitcoin users intentionally try to make this kind of analysis difficult by using tools and techniques to break the heuristics analytics companies employ. Some techniques decrease the effectiveness of the heuristics through distortive methods while others attempt to avoid the heuristics altogether. Bitcoin wallets can assist users by automating some of these techniques or make them available through a user interface.

Here's a non-exhaustive list of some examples:

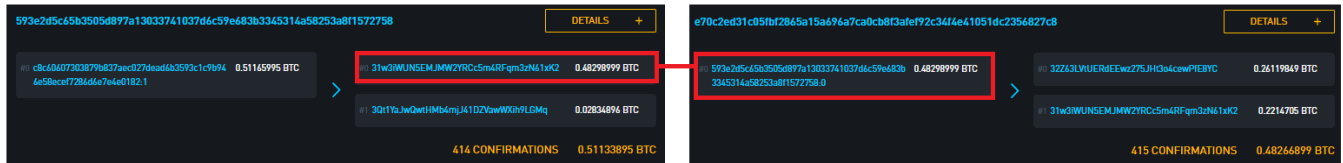
- Randomizing the order of outputs when creating transactions to decrease change output detection accuracy ([example](#)).
- Avoiding address reuse via [HD wallets](#).
- A [PayNym](#) is a publicly sharable ID which allows you to receive payments at different unassociated addresses you control that only become known to you and the sender. The PayNym allows a new address to be derived for each payment without you having to manually present a new address each time, which is great if you want to conveniently receive, say, donations online using bitcoin.
- Coin selection/coin control—wallets can be designed to prioritize clustering fewer addresses together when possible by selecting inputs for transactions more carefully ([example](#)), or allow users to select inputs for transactions manually to avoid revealing ownership of certain coins ([example](#)).



Coin control in Bitcoin Core—user can manually choose the source of funds for a transaction.

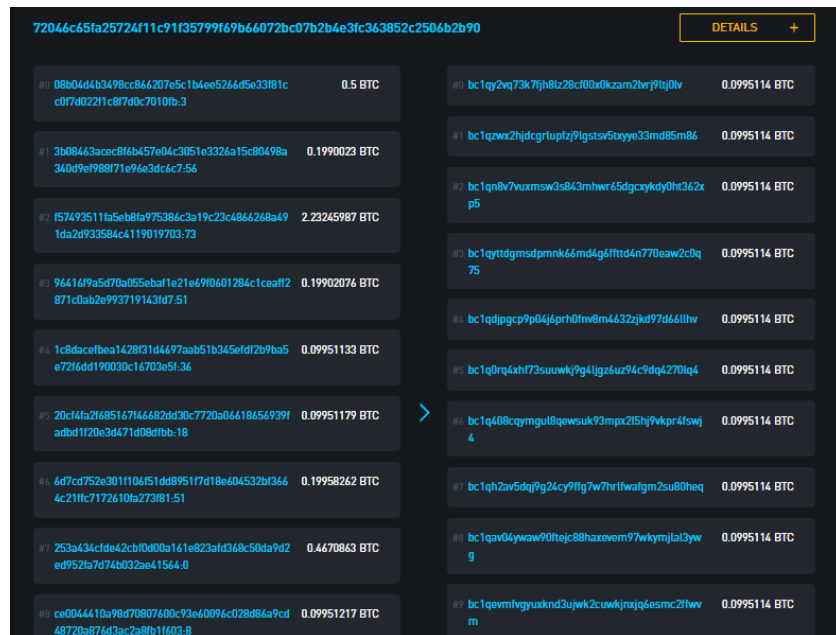
A more advanced example of a privacy-enhancement technique is **CoinJoin** transactions. CoinJoins are a scheme which adds many inputs from many different users into a joint transaction before the transaction is broadcast.

In our example, we saw how the input of a transaction always references a *specific* output of a previous transaction, rather than the whole transaction:



The source of funds for
[e70c2ed31c05fbf2865a15a696a7ca0cb8f3afef92c34f4e41051dc2356827c8](#).

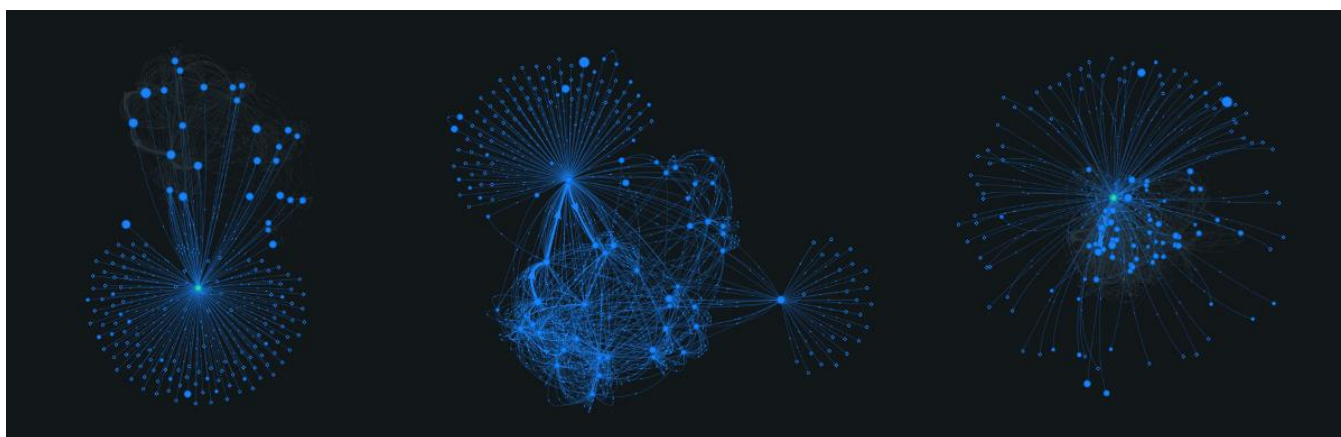
But the inputs and the outputs *within* each individual transaction don't reference each other in any way; transactions are valid as long as there's enough bitcoin in the inputs to cover all the outputs.



A CoinJoin transaction
([72046c65fa25724f11c91f35799f69b66072bc07b2b4e3fc363852c2506b2b90](#)) created by the [Wasabi Wallet](#).

Here, the outputs are chopped up into many equal-amount chunks, so you can't be sure which input funds which payment. The result is that a payment can have a plethora of possible "source of funds" indiscernible from one another, as well as a plethora of possible destinations. This technically doesn't *hide* the source of funds or the destination, but it mixes it so that it becomes difficult to prove what actually funded a particular payment and who's bitcoins went where.

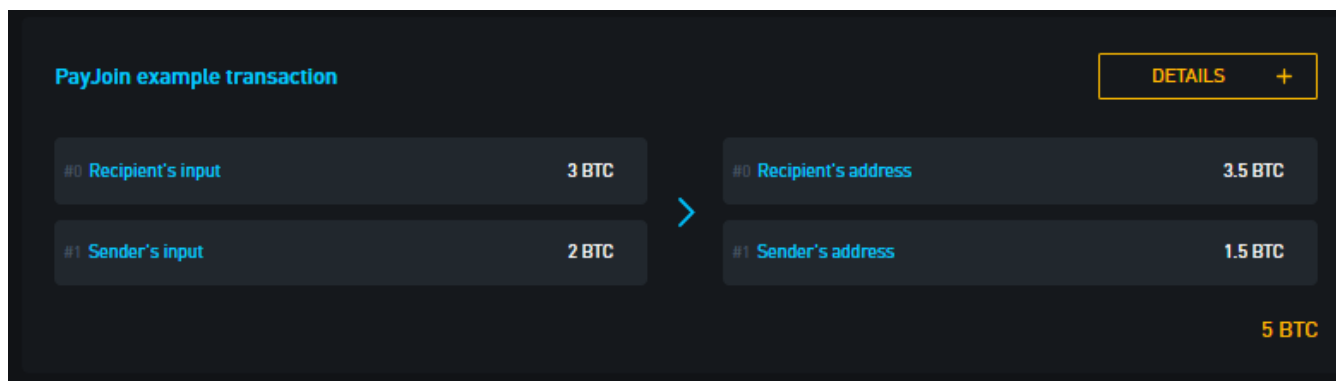
What's also interesting about these kinds of transactions is that they complicate the idea of the common-input-ownership-heuristic. These inputs would all get flagged as belonging to the same owner, which in this transaction they aren't. The images below show false clusters of independent payments as a result of CoinJoin transactions.



CoinJoin transactions created by the [Wasabi Wallet](#). Transaction IDs from left to right: [72046c65fa25724f11c91f35799f69b66072bc07b2b4e3fc363852c2506b2b90](#), [d7a428a8e3d69f236519cb999dbcb47b3b283548875371da567259be806e35ea](#), [20cf4fa2f685167f46682dd30c7720a06618656939fadbdf20e3d471d08dfbb](#) ([oxt.me](#)).

But because these transactions all have the odd look of equal-amount outputs, they're rather easy to spot and can be eliminated from the clustering analytics tools. Equal-amount CoinJoin transactions are best understood as *mixers* to be used when one wishes to obfuscate the source of funds for a payment and the destination to which a payment is sent.

However, the same principle is used to create transactions that are indistinguishable from normal transactions in a recent invention called a **PayJoin** or **Pay-to-EndPoint (P2EP)**. This emerging transaction type mixes inputs from the payer and the recipient and pays the recipient by shifting over the payment amount from the sender's output and to the recipient's output during a real payment for something.



A PayJoin transaction template where the sender pays 0.5 bitcoin to the recipient, mixing inputs with each other in the process.

This transaction doesn't do a lot of mixing—but it does trigger the common-input-ownership heuristic erroneously. More importantly, it triggers the heuristic without leaving any clues for the analytics firms to *not* cluster the inputs together, which they would need to in order to avoid giving false positives. If the usage of PayJoins becomes widespread, the portion of false common-input-ownership positives could become so great that the heuristic itself becomes unreliable, which would be a massive setback for the blockchain analytics tools.

The Lightning Network

The Lightning Network is a beta technology that is being developed on top of the Bitcoin protocol to facilitate low-cost, instant payments. The Lightning Network is accessible to users of [Lightning wallets](#). Lightning transactions differ from base-layer transactions in many ways which make them advantageous from a privacy perspective:

- Lightning transactions are not stored on a public ledger.
- Lightning transactions use [onion routing](#) which doesn't disclose who the final recipient is to the rest of the network.
- Lightning transactions don't mix inputs and can't be clustered together.

The Lightning Network is a system of channels which require liquidity; the current set of merchants and users that accept Lightning payments today are a small subset of the total set of Bitcoin users in the system, and not all payments (especially larger ones) can propagate through the channel system, although that is expected to improve over time. This also means that while Lightning can provide improved privacy for the transactions in its channel system, those channels still need to be funded by regular Bitcoin transactions, which are subject to the privacy concerns in this post.

Another problem is that unlike base-layer Bitcoin payment recipients, recipients of Lightning payments are required to have a Lightning node running. Your node communicates with other Lightning nodes using TCP/IP. Whenever your node interacts with the network (sending, receiving or routing other payments) someone will learn about the existence of your node, its public key and its IP address. From your public key, it's trivial to find out which channels are open between you and other nodes, and how many bitcoins you each have committed to those channels upon opening them. For private channels, the IP address is only revealed to the ones you have an open channel with, but for public channels, it's revealed to the entire network and it's even possible for someone to probe the channels' current balances to figure out if you're a target worth attacking.

When you run a Lightning node, you should assume that your channel balances are known and that they can be linked to your IP address. For this reason, running your Lightning node over Tor is a good option to protect your privacy.

The Lightning Network is currently under quite rapid development and many of its properties might be subject to change in the near future.

Protocol changes

There are several privacy-enhancing technologies that are in development for the base-layer Bitcoin protocol. Here are a few examples:

Schnorr signatures—a signature scheme which, among other improvements, makes multisignature addresses indistinguishable from single-signature addresses

Scriptless scripts—a method by which to use scripts without disclosing the actual spending rules

Taproot—a technique with the potential of making transactions of all types of spending rules indistinguishable from each other

Conclusion

This article aims to give a primer to how privacy works in Bitcoin. The pseudonymous but transparent nature of the Bitcoin blockchain creates an environment where the privacy of the system ultimately hinges on the tools employed by the user and the spying entity. Users who take few precautions for protecting their privacy will most likely leak enough financial information in order for it to be dangerous, assuming that the spying entity is analyzing the blockchain.

The next step is to get acquainted with how different Bitcoin wallet applications can help with privacy, and what to expect when using them. This will be covered in the

next article in this series. In later articles, we will look at different cryptocurrencies and survey available exchange platforms in regions with restricted economic and political freedom.

Further reading

To completely understand what is going on under the hood of Bitcoin, [Andreas Antonopoulos' Mastering Bitcoin](#) is an excellent resource [which is translated into several languages](#).

More specifically, the [Privacy page on the Bitcoin Wiki](#) goes into much more depth on several of these topics and was very recently updated by Chris Belcher. The [Blockstream block explorer](#) was also patched recently to show “privacy ratings” for transactions and is now a good resource to learn more about what conclusions can be derived from transactions’ information.

Special thanks to Adam Gibson, Tomislav Dugandzic and Simon Bohlin for their thoughts and feedback to this article.

***The essays in this series will form the basis for a report to be published by Coin Center, the leading cryptocurrency policy research and advocacy group based in Washington, DC.*

****The Zcash Foundation contributed funding for the project. The Zcash Foundation exists to build and support tools that enable privacy and autonomy, particularly with respect to people’s transactions and financial information. Privacy is important for numerous reasons — personal, medical, political, and more. For this reason, Zcash pioneers the use of zk-SNARKs, a novel form of zero-knowledge cryptography with strong privacy guarantees. Ultimately, the Zcash Foundation’s impact will come from serving the needs and workflows of real people, including those from many backgrounds and locations.*

Thanks to [Human Rights Foundation](#).

Tweetstorm: Developer Activity

By @avichal

Posted March 6, 2019

1/ We [@ElectricCapital](#) fingerprinted more than 20,000 code repos and 16M commits to create a Dev Report on crypto. Analyzed by [@MariaShen](#) (better known internally as "Maria Meeker"). Data powered by [@jubos](#). Here are the highlights ⚡

2/ Number of developers working on public coins has doubled in 2 years. Today, 4,000+ developers/month contribute code across 2.8k coins.

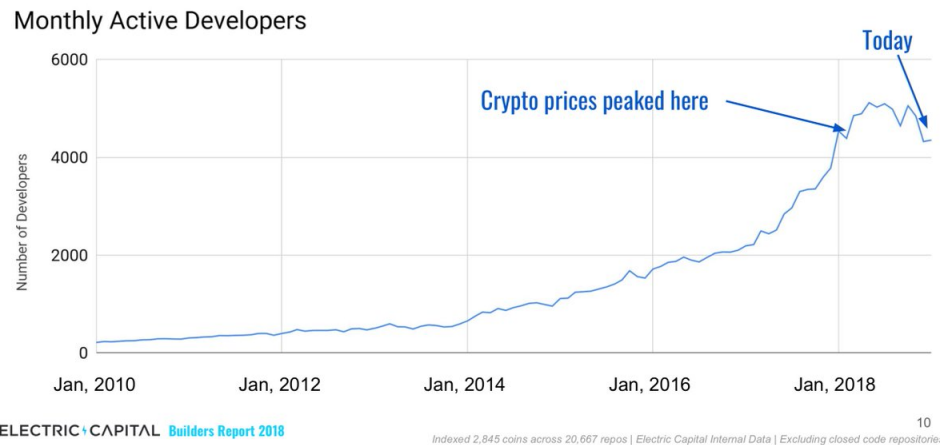
Reminder: this is undercounting. Some of most active projects are private ([@binance](#)), un-launched ([@CodaProtocol](#)), or not a coin ([@lightning](#))

The number of developers working on public coins has roughly doubled in 2 years



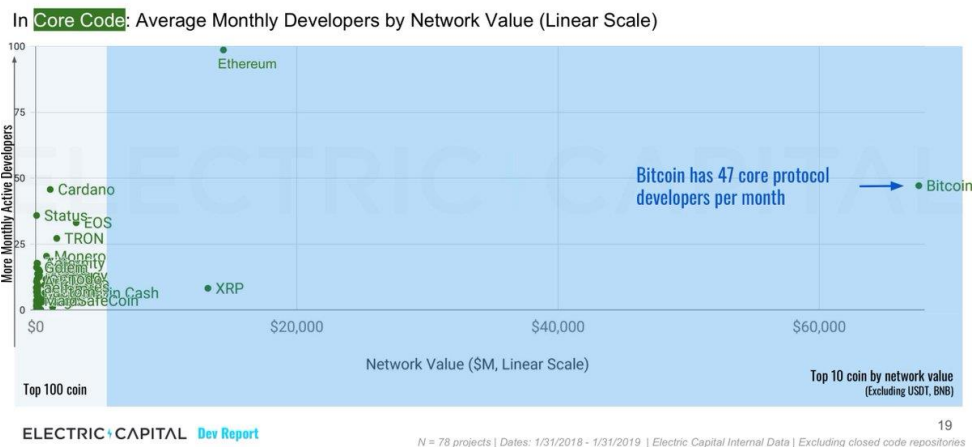
3/ Number of monthly active developers fell 4% while the markets fell more than 80%. Developers who entered the crypto ecosystem have continued to build despite market conditions 🙌

From Jan 2018 to Jan 2019, monthly devs only fell 4% while crypto markets fell 80%



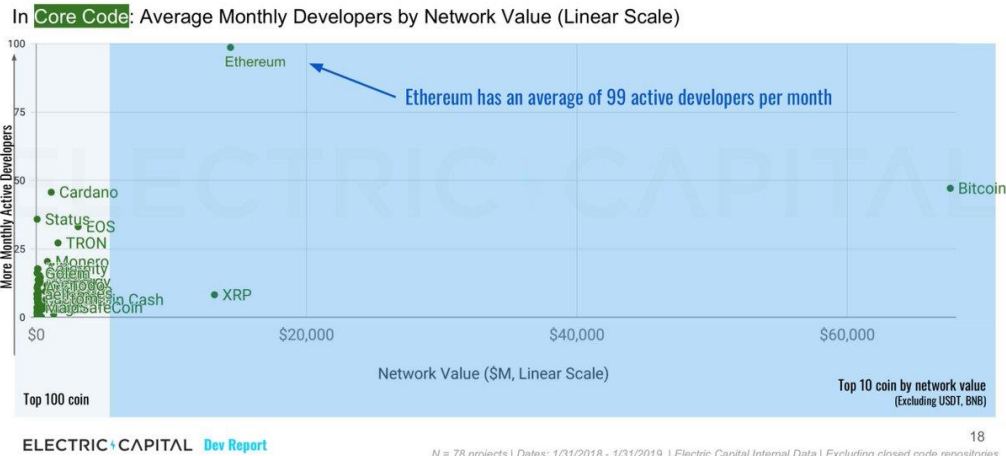
4/ [#Bitcoin](#) has the 2nd biggest team of developers working on core protocol, 10+ years after founding. An average of 47 developers per month work on Bitcoin's core protocol 🏠

Bitcoin has the 2nd highest number of core protocol devs 10+ years after founding



5/ [@Ethereum](#) attracts the biggest developer team in crypto. Average 99 unique developers/month working on ETH's core protocol alone!

Ethereum has the highest number of developers working on core protocol

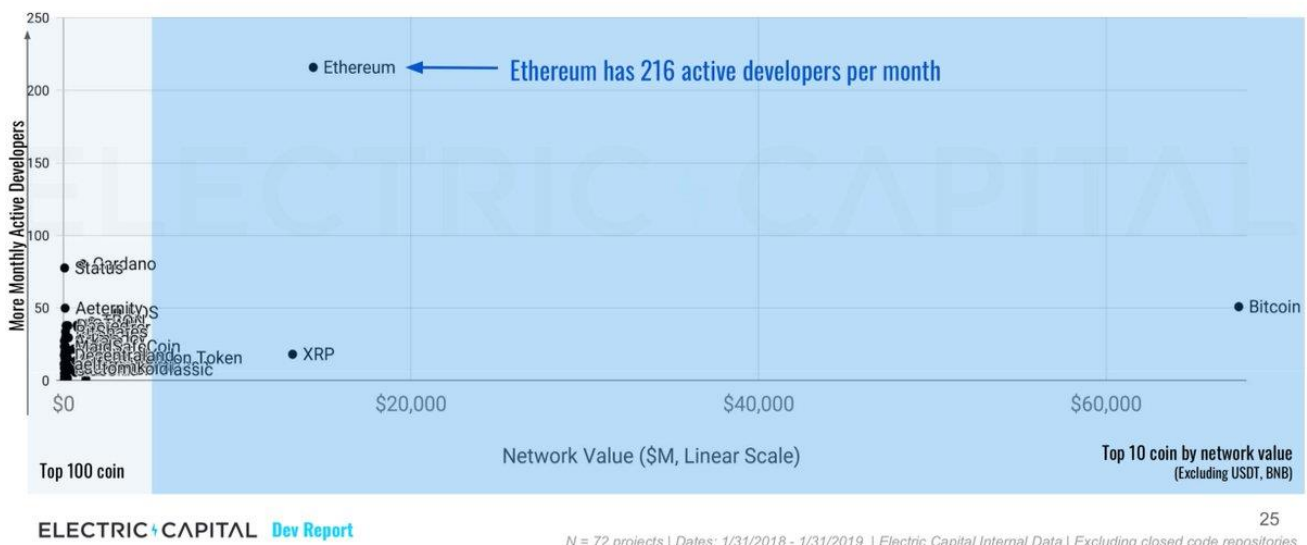


6/ If you consider TOTAL code developers (protocol + wallets, docs, APIs, etc...), [@Ethereum](#) still has the most developers. More than 200 developers/month are working on Ethereum.

Reminder: this is an undercount as it doesn't include ecosystem devs like those working on [@Truffle](#).

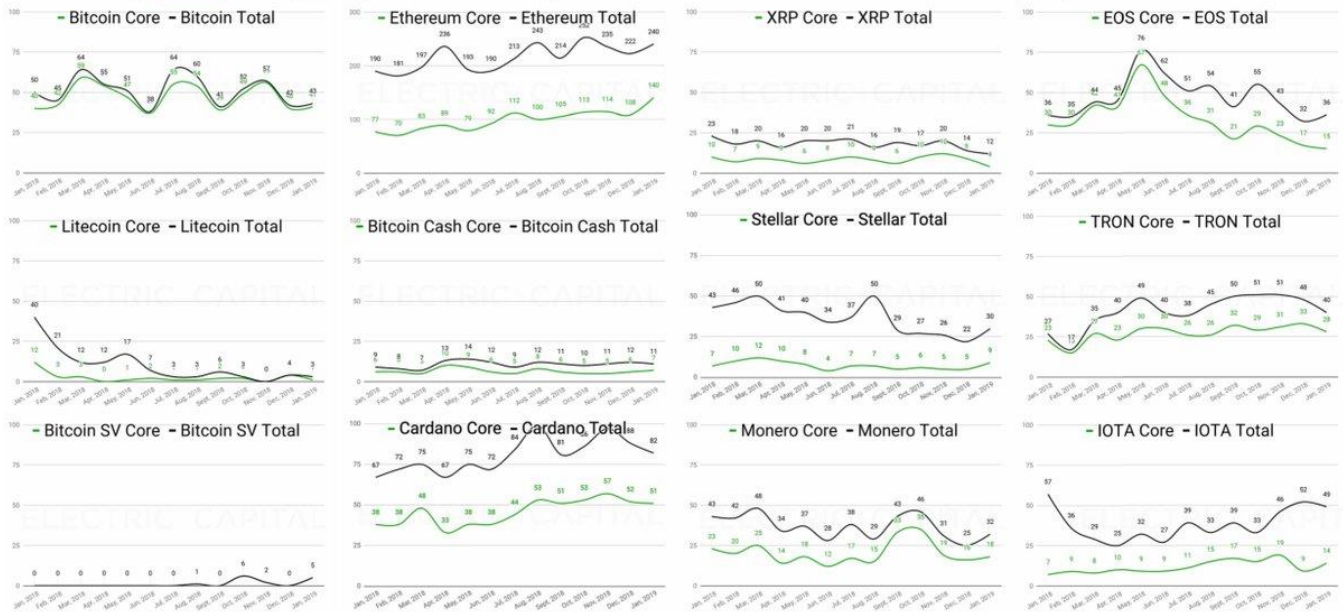
...Ethereum (again) has the most developers

In **Total Code**: Average Monthly Developers by Network Value (Linear Scale)



7/ Let's dive into monthly developer counts of the top projects by network value... [#Bitcoin](#), [@ethereum](#), [@Ripple](#), [#EOS @block_one_](#), [@litecoin](#), [#bitcoincash](#), [@StellarOrg](#), [@Tronfoundation](#), [#BitcoinSV](#), [@Cardano](#), [@monero](#), [@iotatoken](#)

Monthly **core** and **total** devs in the past year across most valuable projects....



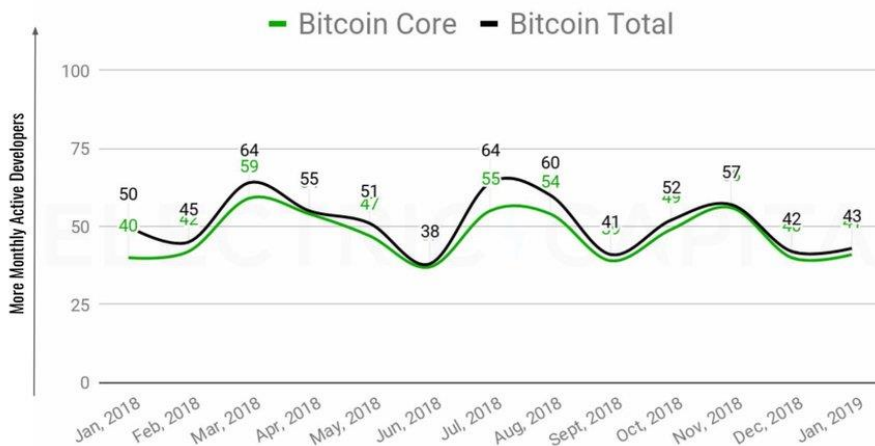
ELECTRIC CAPITAL Dev Report

32
Dates: 1/31/2018 - 1/31/2019 | Electric Capital Internal Data

8/ [#Bitcoin](#) hasn't fallen below 35 developers in the past year. Its developer ecosystem is in top health.

Bitcoin has not fallen below 35 developers in the past year

Number of Active Developers by Month

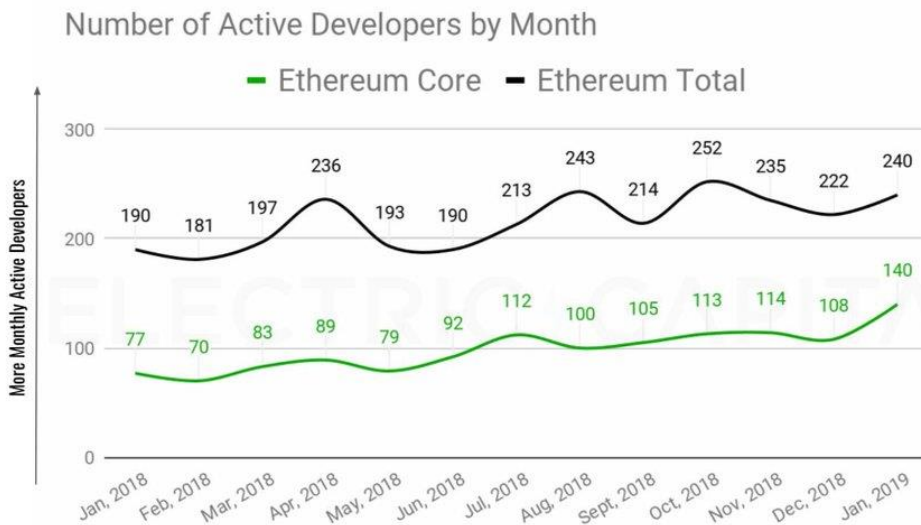


ELECTRIC CAPITAL Dev Report

33
Dates: 1/31/2018 - 1/31/2019 | Electric Capital Internal Data

9/ [@Ethereum](#) grew from 190 total developer per month to 240 total developers per month over 2018 ☒

Ethereum has strong, consistent developer growth



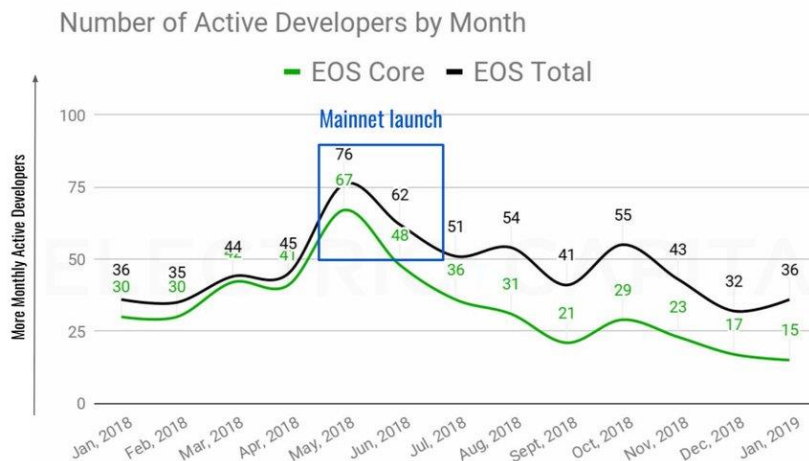
ELECTRIC+CAPITAL Dev Report

34
Dates: 1/31/2018 - 1/31/2019 | Electric Capital Internal Data

10/ [#EOS](#) total developers spiked to 76 leading up to its mainnet launch, then flattened.

[@block_one](#)

EOS developer growth increased around its launch, then flattened



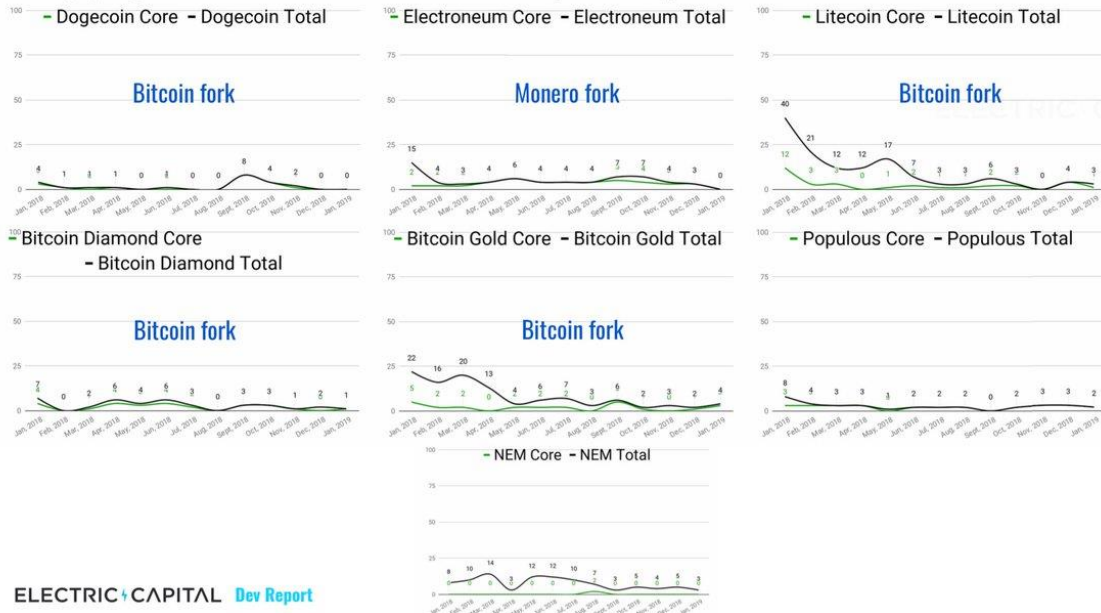
ELECTRIC+CAPITAL Dev Report

35
Dates: 1/31/2018 - 1/31/2019 | Electric Capital Internal Data

11/ Low activity projects tend to be forks

[@Dogecoin](#) is abandoned, [@Litecoin](#) lost almost all its developers in 2018, and forks like [@BitcoinDiamond](#) and [@bitcoingold](#) have fewer than 5 developers working on them a month (perspective: Bitcoin itself has ~50 developers a month)

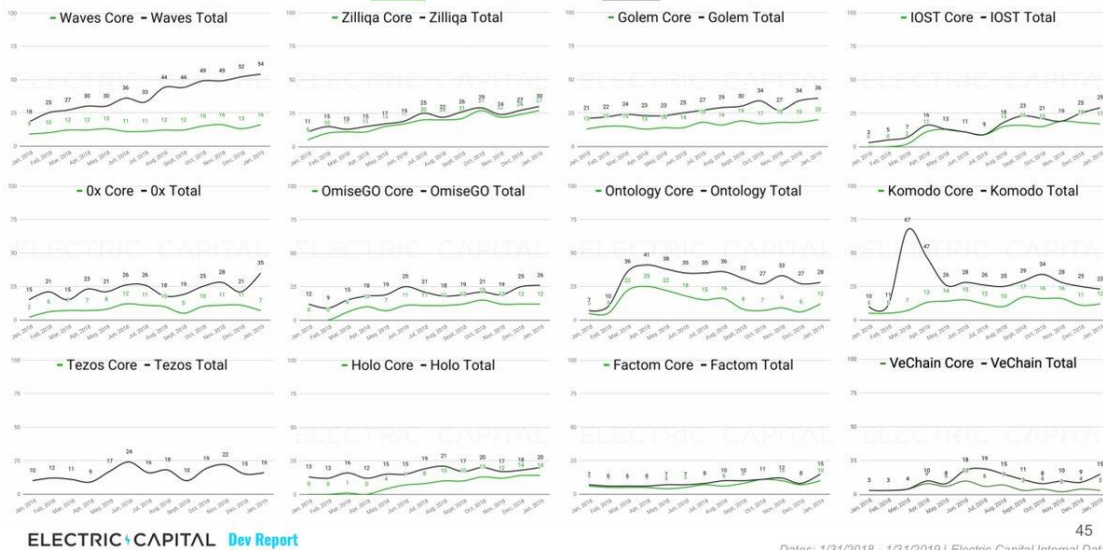
Many projects with fewer than 5 monthly developers are forks



41

12/ High network value coins w/ high developer gains... [@waves](#), [@zilliqa](#), [@golemproject](#), [@IOStoken](#), [@OxProject](#), [@omise_go](#), [@OntologyNetwork](#), [@KomodoPlatform](#), [@tezos](#), [@holochain](#), [@factom](#), [@vechainofficial](#)

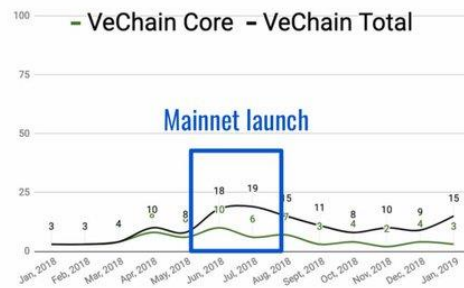
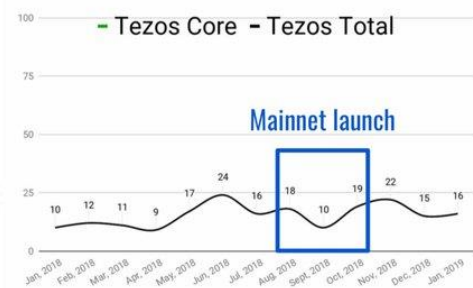
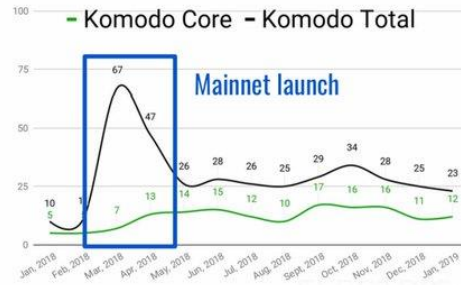
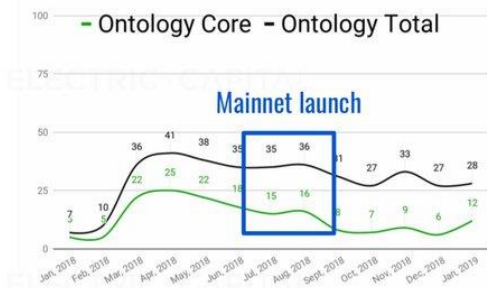
In Top 100, biggest gains in **core** developers & **total** developers



45

13/ Number of developers increase as projects get close to major releases
[@OntologyNetwork](#), [@KomodoPlatform](#), [@tezos](#), [@vechainofficial](#)

Predictably, developers increase leading up to major releases

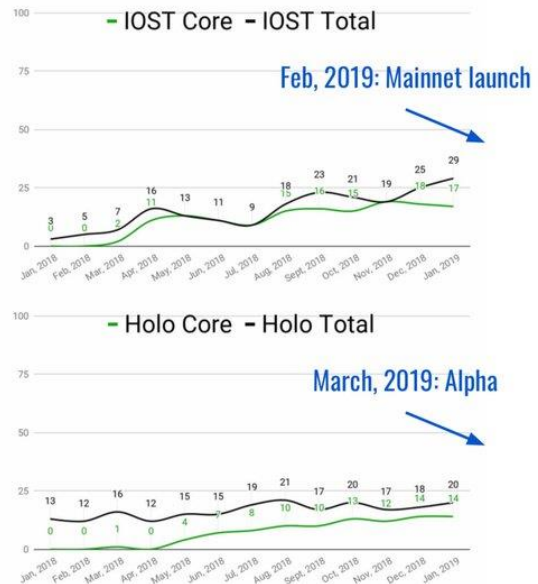
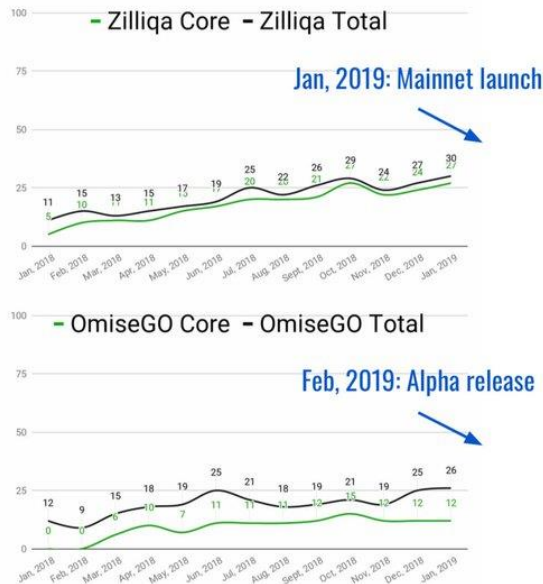


ELECTRIC CAPITAL Dev Report

46

14/ Some projects that have been steadily gaining developers over 2018 have been gearing up for major releases early 2019 [@zilliqa](#), [@IOStoken](#), [@omise_go](#), [@holochain](#)

Some projects were gearing up for major releases



ELECTRIC CAPITAL Dev Report

47
Dates: 1/31/2018 - 1/31/2019 | Electric Capital Internal Data

15/ ...and way more charts here:

[Dev Report - Electric Capital - Medium](https://medium.com/@ElectricCapital/dev-report-476df4ff1fd2) We fingerprinted 20,000+ code repos and 16M commits to create this Q1 2019 Dev Report. We are excited to introduce this as the first of a series of reports that dig in to where crypto developers are...
<https://medium.com/@ElectricCapital/dev-report-476df4ff1fd2>

If you spot an error/missing project, let us know👉

Methodology: de-duped commit data to eliminate forks, open source libraries, and separated the "core" protocol code from "total" updates from website, wallets, and docs

Oops, I meant [@trufflesuite](https://twitter.com/trufflesuite) :)

HOW DID WE MISS A CHANCE TO INCLUDE THIS AT THE TOP OF REPORT?!?!?

On Value Capture At Layers 1 and 2

By [Kyle Samani](#)

Posted March 14, 2019

Among the crypto development and investor communities, the most popular term is “protocol,” and for good reason. Everyone is building a protocol (and presumably these protocols offer investors and employees some way to generate returns).

A protocol is not a thing; it’s an abstract concept, a set of rules. It is by definition impossible to invest in a protocol, as there is nothing to invest in. Crypto investors don’t actually invest in protocols, but in scarce assets that are necessary to make certain kinds of protocols work.

Some protocols’ native assets capture value. Others don’t.

In this essay, we’ll examine layer 1 and layer 2 protocols in the context of value capture, and propose value capture frameworks for each layer.

Value Capture At Layer 1

Layer 1 tokens exist for only one reason: to secure the chain against 51% attacks.

Let’s explore this idea.

One of the more popular visions among crypto enthusiasts is the idea that there will be many chains—thousands or even millions. Some chains will run the same protocol (e.g. many small chains using the vanilla [ethermint](#) protocol), and others will run unique protocols (e.g. Solana, Dfinity, Algorand, Ethereum, Bitcoin, Monero, etc.).

However, the number of chains that can persist in the long run is finite. We already have evidence that supports this hypothesis: [13 chains](#) have been 51% attacked. And it’s not just the long tail of assets. Ethereum Classic, Bitcoin Gold, and Verge were 51% attacked when they were in the top 20 coins by market cap. These chains are limping along and not yet dead. However, they have a near 0% probability of recovery.

Given this: why would users choose to store their wealth in a chain that’s been 51% attacked when they can choose to store their wealth in a chain that hasn’t been?

The breakthrough that made Bitcoin possible was not in technology, cryptography, or distributed systems, but in game theory. The breakthrough of Bitcoin was the

proof of work (POW) consensus algorithm in which miners are compensated for maintaining the ledger by receiving newly minted Bitcoin and the incentives are structured as such that independent miners act in the best interest of the network because of the value of those mined Bitcoin.

We can compare the security of blockchains by measuring the cost of conducting a 51% attack. To conduct a 51% attack, an attacker needs to spend more than the chain's security budget (SB). We can quantify SB in USD terms as follows:

$$SB = \text{aggregate network value} * \text{inflation rate} + \text{transaction fees}$$

Note that this provides a floor, not a ceiling, for network security. There may be supply constraints in the ASIC market for POW coins making it even more difficult to conduct a 51% attack.

To keep the math simple, let's say the market cap of Bitcoin is \$100B. Today, inflation in Bitcoin is about 4% annually. For simplicity, let's round transaction fees down to 0 (in practice, miners generate [the vast majority](#) of their revenues from inflation, not transaction fees). It's thus rational for honest, economically motivated miners to spend up to \$4B (\$100B * 4%) per year to mine Bitcoin. We can therefore say the SB of Bitcoin is \$4B / year.

It's clear from this simple math that security is primarily a function of network value because there is unlikely to be high inflation in the largest blockchain networks. While there are valid arguments for 0%, 1%, and 2% inflation, it's extremely unlikely that people will opt into a global, state-free money that inflates > 5% annually in the long run.

Because security is primarily a function of network value, there is a natural [network effect](#): the more valuable a chain is, the more secure it is. The more secure it is, the easier it becomes for the next marginal user to justify storing their wealth in that chain.

This is why it's not possible to maintain an equilibrium in the medium or long run in which more than a handful of chains exist. Why would users choose to store their wealth in the 7th most valuable/secure chain?

Given the intrinsic differences between proof of work and proof of stake systems, we should expect for the foreseeable future to have a few chains, if for no other reason than they have unique consensus algorithms. Going all-in on a single consensus model at this stage is premature given how young these systems are.

Interoperability Chains

This naturally begs the question: what about interoperability chains like Cosmos (ATOM) and Polkadot (DOT)? Both chains relay messages between other chains, and charge a fee to users for doing so. Additionally, Polkadot provides consensus safety to its parachains for a fee.

Thus ATOMs and DOTs are yield-generating assets, and can be valued as a function of cash flows. Both the Cosmos and Polkadot teams have expressed that they don't expect their respective native tokens to be used as currencies in their respective ecosystems. We agree, and do not expect ATOMs and DOTs to become money either.

Given that 1) the native tokens for interoperability chains are unlikely to be money 2) the only purpose of a chain is to secure itself against 51% attacks, and 3) the [largest market](#) that a native token can strive to be is global, state-free money, it's not clear if interoperability chains can survive in the long run.

We do however expect Cosmos and Polkadot to thrive in the coming years as the [Web3 Stack](#) is clearly becoming more heterogeneous rather than homogenous as developers run experiments and explore different trade-offs at every layer of the stack.

Value Capture At Layer 2

The only way a layer 2 protocol can capture value is if it stores some sort of external and valuable state.

This is an abstract concept. To best understand this, let's compare a few layer 2 assets:

- [Ox](#) (\$ZRX)
- [Basic Attention Token](#) (\$BAT)
- [Augur](#) (\$REP)
- [Livepeer](#) (\$LPT)

The Ox protocol is among the most widely *used* protocols built on the Ethereum blockchain. It allows any two parties to trustlessly trade digital assets without relying on a 3rd party.

Excluding the token balances of ZRX holders, on the surface it does not appear that the asset-exchange function of the Ox contract stores any state. Either a trade happens, or it doesn't. After processing a transaction, the state of the Ox asset-swap contract remains unchanged.

Beyond the actual asset-swap contract, the OX protocol stores a few pieces of [external state](#) about user preferences and network-level governance. While these pieces of state are external to the protocol, they are not valuable pieces of state. That is, the state being stored does not have measurable, market value.

There is at least one way that the OX protocol can capture value: governance. This is an explicit decision to create extra-protocol state (coin holder votes). Governance becomes more interesting as others build higher level protocols and applications on top of the core OX protocol. If these external protocols come to rely on the OX protocol meaningfully, and are economically motivated to see the protocol evolve in a specific direction (or not evolve), they may actively participate in governance, or they may fork away, as [DDEX recently did](#).

While this is an interesting hypothesis, it remains to be seen if governance is fundamentally value-able. At least on a theoretical basis, it can be, although we are skeptical.

BAT is an effectively stateless protocol. The core protocol itself does not store any state about the network other than the account balances of BAT owners. BAT is a proprietary payment currency, which will if not redesigned ultimately be subject to the [velocity problem](#).

Although the BAT protocol is effectively stateless in the Ethereum network, it's not stateless outside of the Ethereum network. That is, the [Brave browser](#), which has more than 5M monthly active users, only supports BAT, and the Brave team is economically incentivized not to change this because they own a lot of BAT. As the number of Brave users grows, the extra-protocol state of BAT grows. This extra-protocol state is un-forkable, so BAT can't be forked out.

Brave is an interesting case study. On an abstract basis, BAT should not capture any value. On the other hand, BAT benefits from a large exogenous effort of the Brave team. Absent changes in the token mechanics, we don't expect BAT will capture value in the long run, but the existence of this extra-protocol state does justify some value, at least for now.

Augur stores two kinds of valuable state. The first is obvious: there is capital locked in the Augur contracts for all open markets. If someone were to fork Augur, it would be impossible to fork the ETH that's locked in open Augur markets.

The second form of valuable state that Augur stores is a bit more nuanced, but actually more important in the long run. Augur is both a global, censorship-resistant prediction market and a decentralized oracle. These functions go hand-in-hand.

Augur is a radical concept. There really is nothing like it in the world. That also means it's untested, and it can fail. Each market that successfully resolves is another proof point that the system works. In order to support billions of dollars of volume, prediction market participants *need* to know that the system will not implode, and the only way to know that is to see that every market has resolved honestly.

If someone were to fork Augur and change the token distribution, then market participants should question the motivations of the fork. The whole point of REP is that it's valued by rational market actors who want to report off-chain events honestly. If someone forks REP and changes the token distribution, one should think adversarially and assume that the person/team/company who forked it has malicious intentions.

Furthermore, the history of Augur gives credibility to the future accuracy of the Augur protocol. That is, many market participants will not risk capital on a platform with such a radical dispute resolution system until they've seen it work in practice. This is valuable state that cannot be forked out, creating more defensibility and value capture for REP.

Next let's examine Livepeer, a layer 2 [work token](#) that powers a network of video transcoders. I wanted to include a work token specifically because many in the crypto community perpetuate the idea that layer 2 work-token networks cannot capture value. This is simply untrue.

Livepeer is a network that enables distributed transcoding for live streaming videos. In order to gain the right to perform work in the Livepeer network, transcoders must purchase and stake LPT. In exchange for doing so, streamers pay the transcoders in ETH or a stablecoin such as DAI or USDC. As such, LPT can be valued as a function of cash flows using a discounted cash flow (DCF) model.

Livepeer, like all layer 2 work token networks, requires that all workers register themselves in an on-chain registry by staking LPT. The more demand there is for services on the Livepeer network, the more revenue will be paid to LPT holders, justifying a higher LPT price. The more demand for Livepeer's transcoding services, the more honest transcoders should compete for that demand, making the network as a whole more secure. If someone were to fork Livepeer and create their own token, that token would be worth a fraction of the LPT because the fork would not bring the same community of demand-side (streamers) and supply-side (transcoders) participants with it.

The purpose of a layer 2 work token is to secure the network against malicious actors. Like in the case of layer 1 networks, there is a natural network effect. Why would users want to use a forked network with lower security if they could use a larger network with more security at the same cost? (the Livepeer protocol does not impose any

taxes on users, so there isn't an opportunity to undercut the original network in terms of price)

All layer 2 work-token networks—for example [Keep](#), [The Graph](#), and [SKALE](#)—benefit from this economic security network effect, not just Livepeer.

Final Thoughts

Given that all of the code that powers crypto networks is open-source, the only source of defensibility is network effects.

While there are many ways to bootstrap network effects for layer 1 assets, in the long run, we will see consolidation as price volatility between chains is ultimately value-destructive. Layer 2 assets, on the other hand, don't need to defend themselves against 51% attacks. Instead, they build network effects through the value of the state they contain.

Hat tip to [Jesse Walden](#) and [Denis Nazarov](#) for conversations that inspired this post.

Disclaimer: Multicoin Capital is a thesis-driven hedge fund that may hold some of the assets discussed in this post.

Links

- <https://github.com/cosmos/ethermint>
- https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3290016
- <https://fork.lol/reward/feepct>
- <https://multicoin.capital/2018/05/09/on-the-network-effects-of-stores-of-value/>
- <https://multicoin.capital/2018/10/09/100-trillion/>
- <https://multicoin.capital/2018/07/10/the-web3-stack/>
- <https://twitter.com/willwarren89/status/1074430379224776705>
- <https://medium.com/hydro-protocol/why-we-are-forking-0x-97dc48ee0426>
- <https://multicoin.capital/2017/12/08/understanding-token-velocity/>
- <https://brave.com/>
- <https://multicoin.capital/2018/02/13/new-models-utility-tokens/>
- <https://keep.network/>
- <https://thegraph.com/>
- <https://skalelabs.com/>
- <https://twitter.com/jessewldn>
- <https://twitter.com/literature>

Disclaimer:

THANK YOU, CREATORS.

WORDS

Please note that this Journal is provided on the basis that the person who is reading it accepts the following conditions relating to the provision of the same (including on behalf of their respective organization). This Journal does not contain or purport to be, financial promotion(s) of any kind.

This Journal does not contain reference to any of the investment products or services currently offered by members of the any specific business, that means any business I am associated with. Bitcoin, shitcoins, and related technologies can be volatile, Don't fuck around with this stuff because you might get burned.

Bitcoin has paved the way for some VERY radical technology AND it's very confusing. Read more. Ask questions. The purpose of this Journal is to provide archive and curate the best commentary and culture in the bitcoin space.

This Blog Post fairly represents the opinions and sentiments of its author at the date of publishing but it should be noted that such opinions and sentiments may be revised from time to time, for example in light of experience and further developments, and the blog post may not necessarily be updated to reflect the same.

Nothing within this Journal constitutes investment, legal, tax or other advice. This Journal should not be used as the basis for any investment decisions which a reader may be considering. Any potential investor in bitcoin or shitcoins, even if experienced and affluent, is strongly recommended to seek independent financial advice upon the merits of the same in the context of their own unique circumstances.

This journal is subject to copyright with all rights reserved. Just kidding. I didn't write these articles so I can't really copyright them. If you want permission to use the contents of this journal, contact the original author.

DYOR | BTFD | HOLD