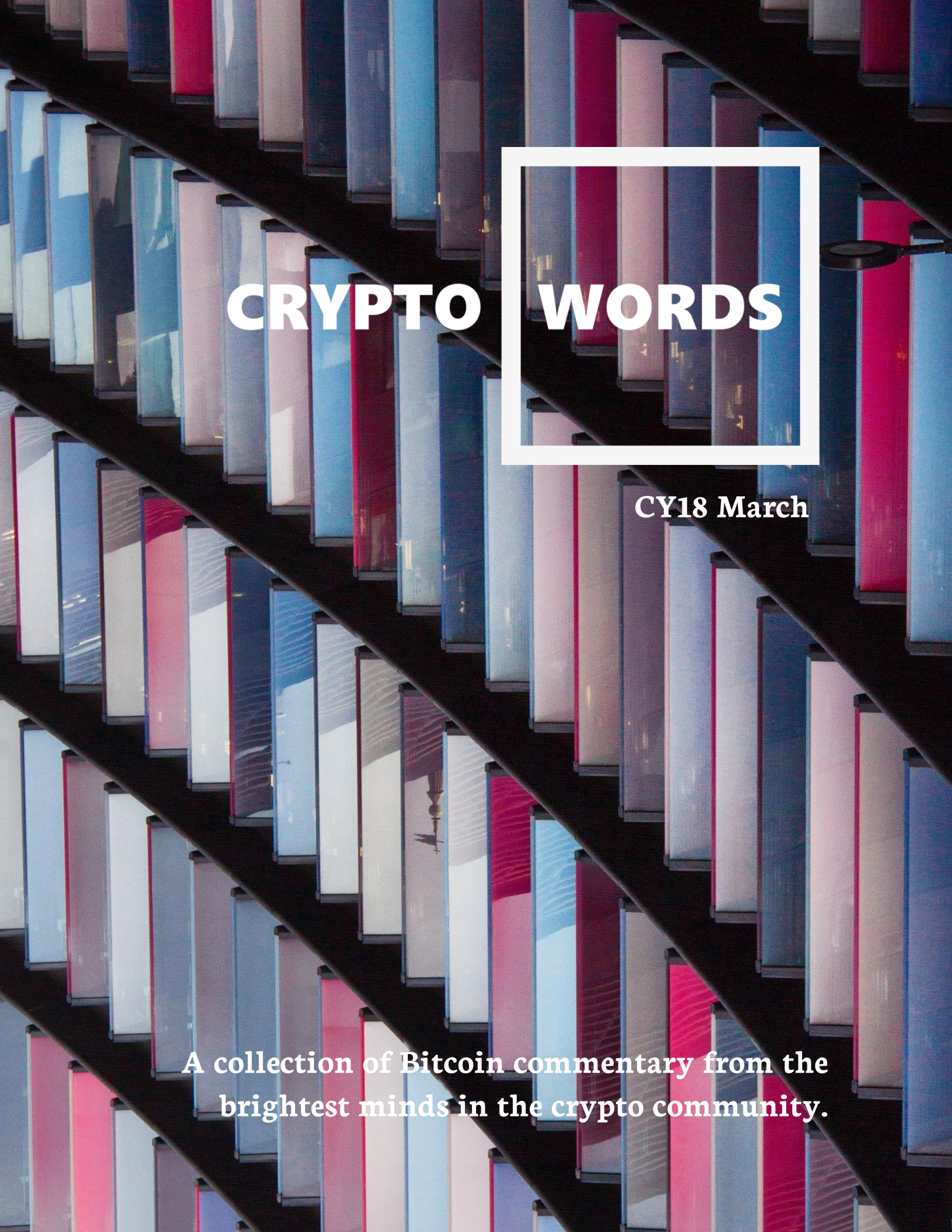


CY18 March

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

Contents

Goals and Scope

Crypto Words is a journal of Bitcoin commentary, established February 13, 2019. Its purpose is to document and advance commentary and research in disciplines of particular interest to the Bitcoin 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 Bitcoin space for current and future researchers. *Crypto Words 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 Bitcoin publishing. For authors with commentary and scholarly papers on topic, 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 Bitcoin 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 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.

Support Crypto Words

The posts and journals published here have been carefully curated and crafted as a true labor of love. If you've found any of this content useful here's how to show your thanks and keep the project going.

Send Bitcoin | tippin.me | Send CashApp | Send PayPal

Spread the word

Have a website or use social networking sites like Twitter, Facebook, or LinkedIn? Please consider sharing the content found on Crypto Words or linking to https://cryptowords.github.io.

Follow us on social media

We post regularly on Twitter and use it as our main form of communication. — We don't rapid fire posts but add commentary where we see fit. Posts are typically links to our content here, trolling nocoiners, sarcastic remarks, and other things regarding development of this site.

If these sorts of things interest you, follow along on:

Twitter

Subscribe to our newsletter

We publish our journal monthly and share it via Twitter and via newsletter. Consider subscribing to the newsletter. If you're not on Twitter all day, it might make sense to subscribe so you never miss a publication.

Our pledge

- We will never sell you out.
- We will never shill you shitcoins.
- We will only deliver what is promised.

Subscribe

Seven Myths of Bitcoin

By George Kikvadze

Posted March 2, 2018

First they ignore you. Then they laugh at you. Then they fight you. Then you win.
Mahatma Gandhi

Bitcoin has been around for almost 10 years; and right now, the cryptocurrency is clearly in its "fight" stage. This is both understandable and expected. Every "trusted" third-party intermediary has everything to lose. And the myths about bitcoin that these intermediaries have been disseminating need to be addressed.

Myth # 1: Bitcoin is criminal money.

The Bitcoin Blockchain is a transparent, digital ledger on which each and every transaction is registered, time stamped and visible to anybody who wishes to view it. If you give someone a $100 note, no one has any idea where that note has been since its minting by the Federal Reserve. No wonder a study by Harvard highlights the preponderance of large bills used by criminal organizations. But with bitcoin, the movement is tracked from inception and available for viewing on the Bitcoin Blockchain. In its 110-page annual report on money laundering and terrorist financing, the UK Treasury considers bitcoin a significantly lower risk in money laundering and terrorism financing than cash. And as Jason Weinstein, co-Founder of Blockchain Alliance and former head of the U.S. Justice Department's cybercrime division, put it: "Criminals should run, not just walk away, from bitcoin."

Table 1.A: National risk assessment on money laundering

National risk assessment on money laundering						
Thematic area	Total vulnerabilities score	Total likelihood score	Structural risk	Structural risk level	Risk with mitigation grading	Overall risk level
Banks	34	6	211	High	158	High
Accountancy service providers	14	9	120	High	90	High
Legal service providers	17	7	112	High	84	High
Money service businesses	18	7	119	High	71	Medium
Trust or company service providers	11	6	64	Medium	64	Medium
Estate agents	11	7	77	Medium	58	Medium
High value dealers	10	6	56	Low	42	Low
Retail betting (unregulated gambling)	10	5	48	Low	36	Low
Casinos (regulated gambling)	10	3	32	Low	24	Low
Cash	21	7	147	High	88	High
New payment methods (e-money)	10	6	60	Medium	45	Medium
Digital currencies	5	3	15	Low	11	Low

Myth # 2: Bitcoin consumes a lot more electricity.

If you consider the aggregate energy demanded by the "old rails" of finance and government services such as notaries and registrars, it's easy to understand that bitcoin is actually much more efficient than the systems it aims to disintermediate. The amount of energy spent every year to mine copper, nickel and other minerals around the globe — transporting them, turning them into coins, storing, distributing and securing those coins — you get the idea. Or consider the process of cutting forests to produce paper required for contemporary systems of titling, registration and certification. The Bitcoin Blockchain — the new "World Wide Ledger" will gradually update paper-based systems and with that the inefficient energy accompanying them. Coin Center — a D.C. based crypto-currency advocacy group — has produced an insightful report on the topic, with a more detailed study on its way.

Myth # 3 Bitcoin is a Bubble.

In recent months, bitcoin has been attacked by economists, central bankers and various “experts.” But the qualifications of these crypto critics are few and irrelevant. Would you listed to a doctor advising on stock markets or a car mechnic commenting on blood presure ?

When critics compared the cryptocurrency to the 17th century tulip mania, Naval Ravikant, founder of Angelist, explained the flawed juxtaposition this way: “Tulips are not durable, not scarce, not programmable, not fungible, not verifiable, not divisible and hard to transfer… but tell me more about your analogy.”

When it comes to bitcoin, I’m betting with technologists and coders. And in regards to sceptics, I expect many will reevaluate their ambivalence about the significance of this technology. This has happened with internet. It will happen with bitcoin. Meanwhile, my advice to them is to go out; to acquire and to use bitcoin. See what it is all about.

Myth # 4 I love Blockchain; just not bitcoin.

This is similar to saying I love the Internet; just not the TCP/IP protocol. Bitcoin is one of the fundamental applications of blockchain technology. It’s the protocol that makes blockchain secure and safe. Without bitcoin, blockchains are just databases. We have those already.

Myth # 5 Bitcoin can't process large numbers of transactions.

Bitcoin is still in the early stages of development. Remember the dial-up service in early 90s whereas 10kbp/s was an achievement? Back then we would have never predicted that anyone, anywhere would be able to stream anything on their phone. Bitcoin will likely mature in a similar fashion; Segwit, Schnorr Singatures, Sidechains, and the Lightning Network are a few of the proposals that will facilitate the evolution and scaling of the Bitcoin Blockchain over the coming years. And the potential to scale is significant — Lightning, for example, can process up to 100,000 transactions per second which is much more than what Visa can do. Be patient. And remember — thousands of developers are working tirelessly to enhance the protocol.

Myth #6 Bitcoin is a solution looking for a problem.

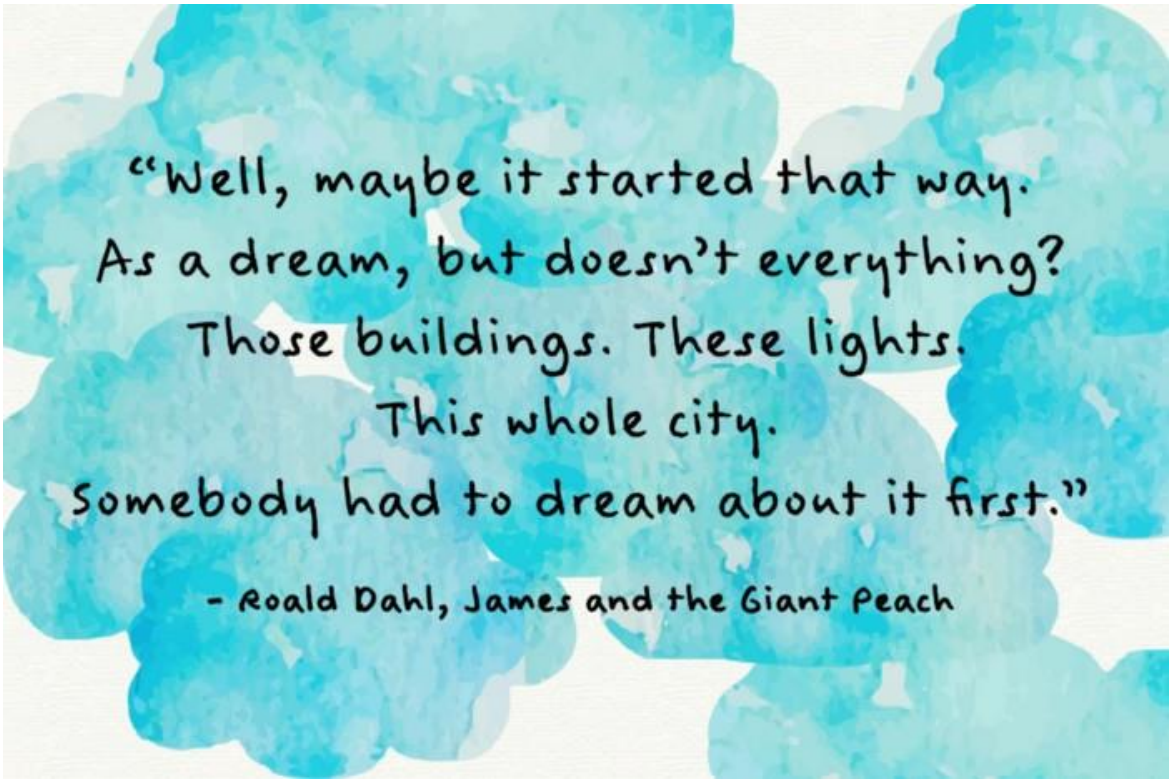
It's difficult for someone living in Manhattan or Mayfair to comprehend the utility of bitcoin. Indeed, the payment rails in most of the OECD countries function pretty well. However, lets admit it, the global trust of citizens in the systems is broken. And you don't need to look at Edelman Trust Barometer to feel it. In frontier markets the friction related to moving money can be significant. The friction of registering and securely storing your assets is even more stifling. Around the globe, some two billion adults are unbanked while over billion live in countries with double-digit inflation. Another friction that bitcoin addresses is micro-payments. It is not attractive for the existing payment rails to be sending amounts at less than a $1. But the trillions of transactions that fall into this category may one day be processed on bitcoin blockchain with minimal fees via the Lightning network. And IoT opens an even more expansive world of opportunity. Those devices will have digital wallets with digital currency programmed to execute smart contracts systematically. We are moving into digital age where digital currency and digital wallets make so much more sense.

Myth #7 Bitcoin will be shut down by governments.

Bitcoin is an open-source movement. And perhaps the risks of bitcoin being shut down in certain places, like North Korea, still exist. Hint, they ll have to shut down the internet first. But, in my opinion, that risk is minimal in Democratic places like Japan, EU, USA and others. At this stage, the greatest barrier to progress is ignorance and misinformation. This is both a great challenge and a great opportunity for the ecosystem to engage and educate decision-makers and regulators. Organizations like Coin Center, the Blockchain Alliance, the Global Blockchain Business Council (GBBC) and others are leading this effort across the world. However there is much more to be done.

Historically, innovation has been met with skepticism and scorn. From lightbulbs to laptops, cameras to cars — the initial reception to change is never warm. But eventually these innovations became commonplace — essential tools powering our everyday lives. One day, bitcoin will fall into this category. And as there are still candles

and horses, there will still be banks and notaries. But their role will evolve, transformed by the open source technology of the future — bitcoin.



---

https://www.reddit.com/r/Bitcoin/comments/bzoy78/the_seven_myths_of_bitcoin_by_george_kikvadze/

If you liked this piece, you may enjoy my other blogs — linked below.

- Bitcoin as a Security Layer
- On the Price of Bitcoin
- Blockchain for the Global Finance Trade Gap
- Investing in Bitcoin for the Non-Technical Investor
- **Bitcoin & The Point of No Return**
- The Global Blockchain Business Council Returns to the Blockchain Summit
- Less Conference, More Conversation: Our Fifth Annual Blockchain Summit

---

The Bullish Case for Bitcoin

By Vijay Boyapati

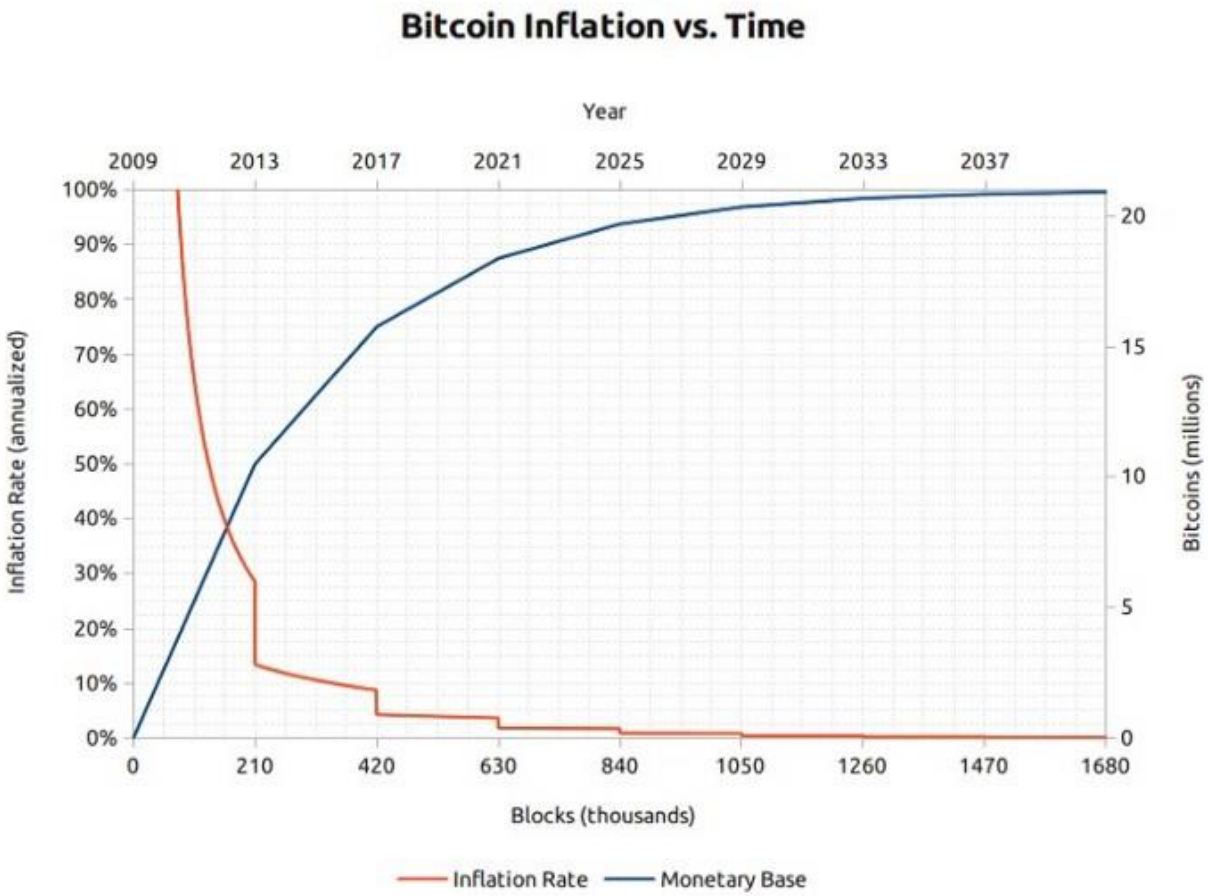
Posted March 2, 2018

With the price of a bitcoin surging to new highs in 2017, the bullish case for investors might seem so obvious it does not need stating. Alternatively it may seem foolish to invest in a digital asset that isn't backed by any commodity or government and whose price rise has prompted some to compare it to the tulip mania or the dot-com bubble. Neither is true; the bullish case for Bitcoin is compelling but far from obvious. There are significant risks to investing in Bitcoin, but, as I will argue, there is still an immense opportunity.

Genesis

Never in the history of the world had it been possible to transfer value between distant peoples without relying on a trusted intermediary, such as a bank or government. In 2008 Satoshi Nakamoto, whose identity is still unknown, published a 9 page solution to a long-standing problem of computer science known as the Byzantine General's Problem. Nakamoto's solution and the system he built from it — Bitcoin — allowed, for the first time ever, value to be quickly transferred, at great distance, in a completely trustless way. The ramifications of the creation of Bitcoin are so profound for both economics and computer science that Nakamoto should rightly be the first person to qualify for both a Nobel prize in Economics *and* the Turing award.

For an investor the salient fact of the invention of Bitcoin is the creation of a new scarce digital good — bitcoins. Bitcoins are transferable digital tokens that are created on the Bitcoin network in a process known as "mining". Bitcoin mining is roughly analogous to gold mining except that production follows a designed, predictable schedule. By design, only 21 million bitcoins will ever be mined and most of these already have been — approximately 16.8 million bitcoins have been mined at the time of writing. Every four years the number of bitcoins produced by mining halves and the production of new bitcoins will end completely by the year 2140.



Bitcoins are not backed by any physical commodity, nor are they guaranteed by any government or company, which raises the obvious question for a new bitcoin investor: why do they have any value at all? Unlike stocks, bonds, real-estate or even commodities such as oil and wheat, bitcoins cannot be valued using standard discounted cash flow analysis or by demand for their use in the production of higher order goods. Bitcoins fall into an entirely different category of goods, known as monetary goods, whose value is set game-theoretically. I.e., each market participant values the good based on their appraisal of whether and how much other participants will value it. To understand the game-theoretic nature of monetary goods, we need to explore the origins of money.

The Origins of Money

In the earliest human societies, trade between groups of people occurred through barter. The incredible inefficiencies inherent to barter trade drastically limited the scale and geographical scope at which trade could occur. A major disadvantage with barter based trade is the double coincidence of wants problem. An apple grower may desire trade with a fisherman, for example, but if the fisherman does not desire apples at the same moment, the trade will not take place. Over time humans evolved a desire to hold certain collectible items for their rarity and symbolic value (examples include shells, animal teeth and flint). Indeed, as Nick

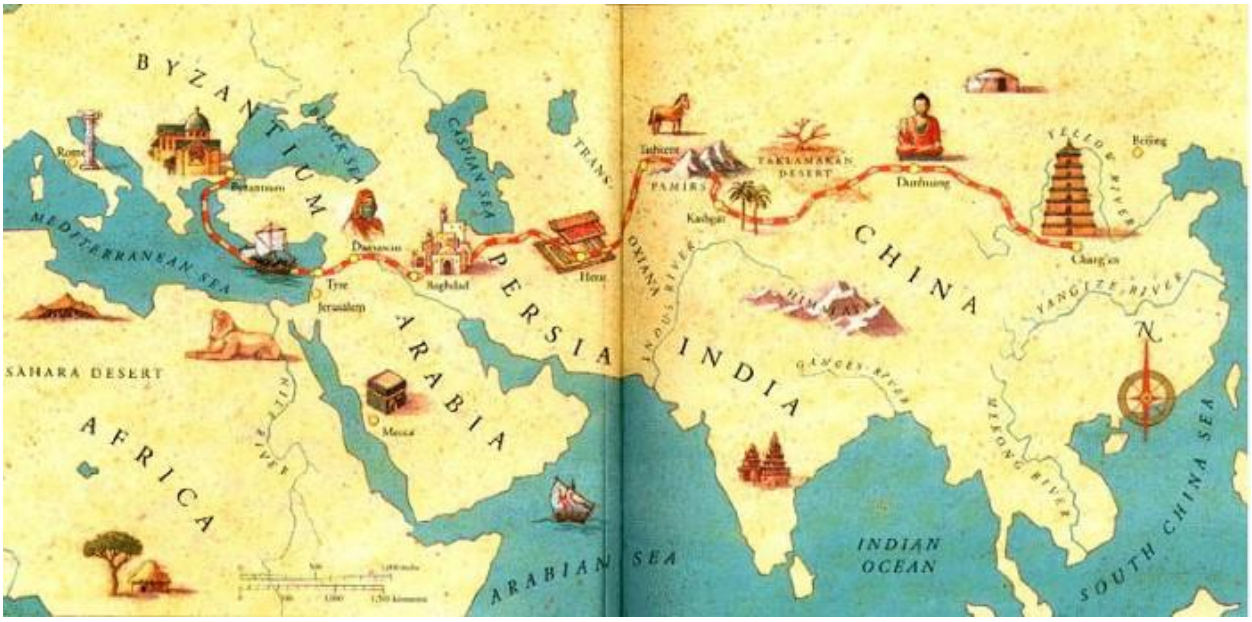
Szabo argues in his brilliant essay on the origins of money, the human desire for collectibles provided a distinct evolutionary advantage for early man over his nearest biological competitors, *Homo neanderthalensis*.

The primary and ultimate evolutionary function of collectibles was as a medium for storing and transferring wealth.

Collectibles served as a sort of "proto-money" by making trade possible between otherwise antagonistic tribes and by allowing wealth to be transferred between generations. Trade and transfer of collectibles were quite infrequent in paleolithic societies, and these goods served more as a "store of value" rather than the "medium of exchange" role that we largely recognize modern money to play. Szabo explains:

Compared to modern money, primitive money had a very low velocity — it might be transferred only a handful of times in an average individual's lifetime. Nevertheless, a durable collectible, what today we would call an heirloom, could persist for many generations and added substantial value at each transfer — often making the transfer even possible at all.

Early man faced an important game-theoretic dilemma when deciding which collectibles to gather or create: which objects would be desired by other humans? By correctly anticipating which objects might be demanded for their collectible value, a tremendous benefit was conferred on the possessor in their ability to complete trade and to acquire wealth. Some Native American tribes, such as the Narragansetts, specialized in the manufacture of otherwise useless collectibles simply for their value in trade. It is worth noting that the earlier the anticipation of future demand for a collectible good, the greater the advantage conferred to its possessor; it can be acquired more cheaply than when it is widely demanded and its trade value appreciates as the population which demands it expands. Furthermore, acquiring a good in hopes that it will be demanded as a future store of value hastens its adoption for that very purpose. This seeming circularity is actually a feedback loop that drives societies to quickly converge on a single store of value. In game-theoretic terms, this is known as a "Nash Equilibrium". Achieving a Nash Equilibrium for a store of value is a major boon to any society, as it greatly facilitates trade and the division of labor, paving the way for the advent of civilization.



Over the millennia, as human societies grew and trade routes developed, the stores of value that had emerged in individual societies came to compete against each other. Merchants and traders would face a choice of whether to save the proceeds of their trade in the store of value of their own society or the store of value of the society they were trading with, or some balance of both. The benefit of maintaining savings in a foreign store of value was the enhanced ability to complete trade in the associated foreign society. Merchants holding savings in a foreign store of value also had an incentive to encourage its adoption within their own society, as this would increase the purchasing power of their savings. The benefits of an imported store of value accrued not only to the merchants doing the importing, but also to the societies themselves. Two societies converging on a single store of value would see a substantial decrease in the cost of completing trade with each other and an attendant increase in trade-based wealth. Indeed, the 19th century was the first time when most of the world converged on a single store of value — gold — and this period saw the greatest explosion of trade in the history of the world. Of this halcyon period, Lord Keynes wrote:

What an extraordinary episode in the economic progress of man that age was … for any man of capacity or character at all exceeding the average, into the middle and upper classes, for whom life offered, at a low cost and with the least trouble, conveniences, comforts, and amenities beyond the compass of the richest and most powerful monarchs of other ages. The inhabitant of London could order by telephone, sipping his morning tea in bed, the various products of the whole earth, in such quantity as he might see fit, and reasonably expect their early delivery upon his doorstep

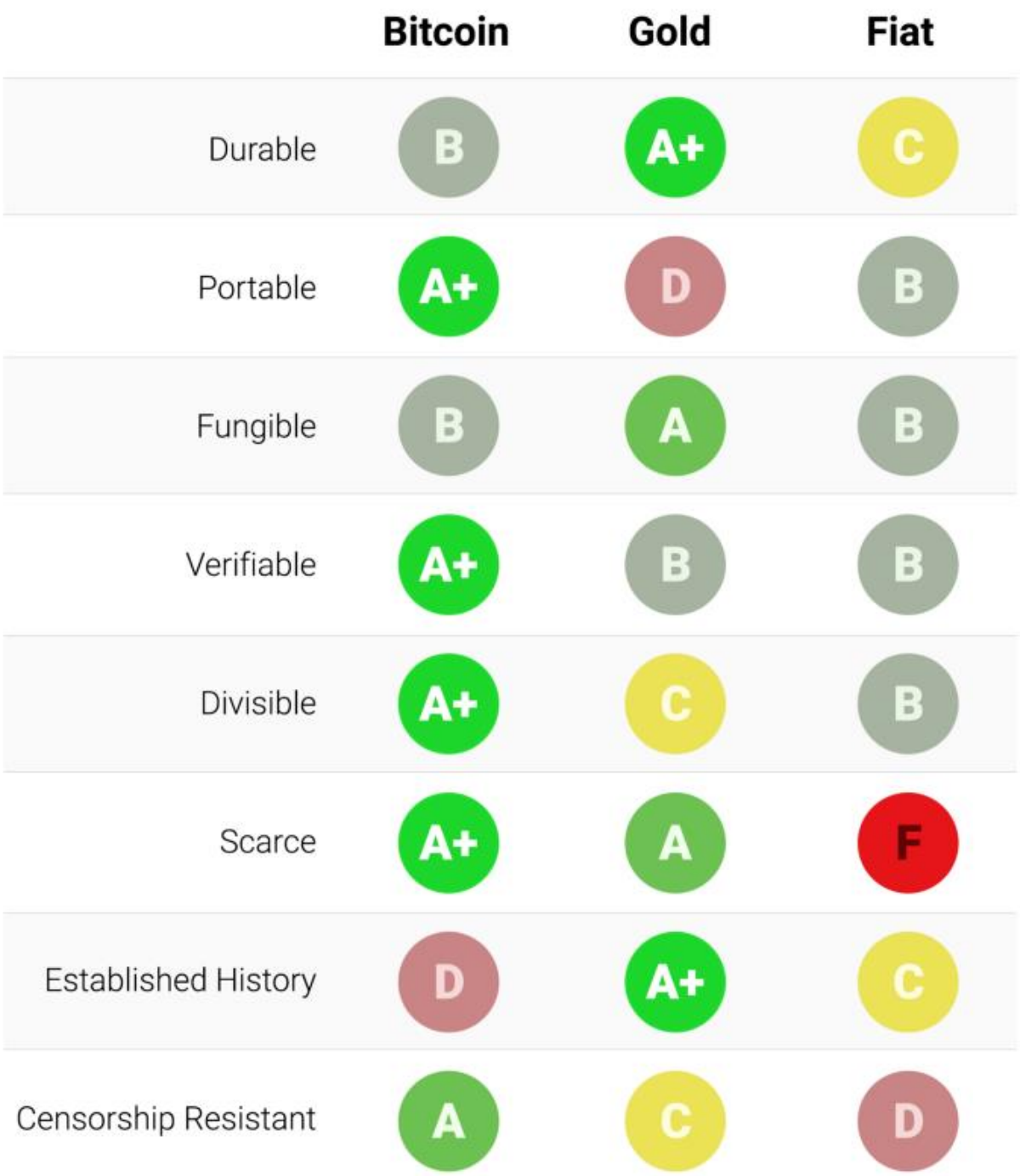
The attributes of a good store of value

When stores of value compete against each other, it is the specific attributes that make a good store of value that allows one to out-compete another at the margin

and increase demand for it over time. While many goods have been used as stores of value or "proto-money", certain attributes emerged that were particularly demanded and allowed goods with these attributes to out-compete others. An ideal store of value will be:

- Durable: the good must not be perishable or easily destroyed. Thus wheat is not an ideal store of value
- Portable: the good must be easy to transport and store, making it possible to secure it against loss or theft and allowing it to facilitate long-distance trade. A cow is thus less ideal than a gold bracelet.
- Fungible: one specimen of the good should be interchangeable with another of equal quantity. Without fungibility, the coincidence of wants problem remains unsolved. Thus gold is better than diamonds, which are irregular in shape and quality.
- Verifiable: the good must be easy to quickly identify and verify as authentic. Easy verification increases the confidence of its recipient in trade and increases the likelihood a trade will be consummated.
- Divisible: the good must be easy to subdivide. While this attribute was less important in early societies where trade was infrequent, it became more important as trade flourished and the quantities exchanged became smaller and more precise.
- Scarce: As Nick Szabo termed it, a monetary good must have "unforgeable costliness". In other words, the good must not be abundant or easy to either obtain or produce in quantity. Scarcity is perhaps the most important attribute of a store of value as it taps into the innate human desire to collect that which is rare. It is the source of the original value of the store of value.
- Established history: the longer the good is perceived to have been valuable by society, the greater its appeal as a store of value. A long-established store of value will be hard to displace by a new upstart except by force of conquest or if the arriviste is endowed with a significant advantage among the other attributes listed above.
- Censorship-resistant: a new attribute, which has become increasingly important in our modern, digital society with pervasive surveillance, is censorship-resistance. That is, how difficult is it for an external party such as a corporation or state to prevent the owner of the good from keeping and using it. Goods that are censorship-resistant are ideal to those living under regimes that are trying to enforce capital controls or to outlaw various forms of peaceful trade.

The table below grades Bitcoin, gold and fiat money (such as dollars) against the attributes listed above and is followed by an explanation of each grade:



Durability:

Gold is the undisputed King of durability. The vast majority of gold that has ever been mined or minted, including the gold of the Pharaohs, remains extant today and will likely be available a thousand years hence. Gold coins that were used as money in antiquity still maintain significant value today. Fiat currency and bitcoins are

fundamentally digital records that may take physical form (such as paper bills). Thus it is not their physical manifestation whose durability should be considered (since a tattered dollar bill may be exchanged for a new one), but the durability of the institution that issues them. In the case of fiat currencies, many governments have come and gone over the centuries, and their currencies disappeared with them. The Papiermark, Rentenmark and Reichsmark of the Weimar Republic no longer have value because the institution that issued them no longer exists. 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, despite prominent instances of nation-states attempting to regulate Bitcoin and years of attacks by hackers, the network has continued to function, displaying a remarkable degree of "anti-fragility".

Portability:

Bitcoins are the most portable store of value ever used by man. Private keys representing hundreds of millions of dollars can be stored on a tiny USB drive and easily carried anywhere. Furthermore, equally valuable sums can be transmitted between people on opposite ends of the earth near instantly. Fiat currencies, being fundamentally digital, are also highly portable. However, government regulations and capital controls mean that large transfers of value usually take days or may not be possible at all. 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. It is no wonder that the majority of bullion is never transported. 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. Transmitting physical gold across large distances is costly, risky and time-consuming.

Fungibility:

Gold provides the standard for fungibility. When melted down, an ounce of gold is essentially indistinguishable from any other ounce, and gold has always traded this way on the market. 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. The demonetization caused 500 and 1000 rupee notes to trade at a discount to their face value, making them no longer truly fungible with their lower denomination sibling notes. 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. Without improvements to the privacy and anonymity of Bitcoin's network protocol, bitcoins cannot be considered as fungible as gold.

Verifiability:

For most intents and purposes, both 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 mathematical certainty. Using cryptographic signatures, the owner of a bitcoin can publicly prove she owns the bitcoins she says she does.

Divisibility:

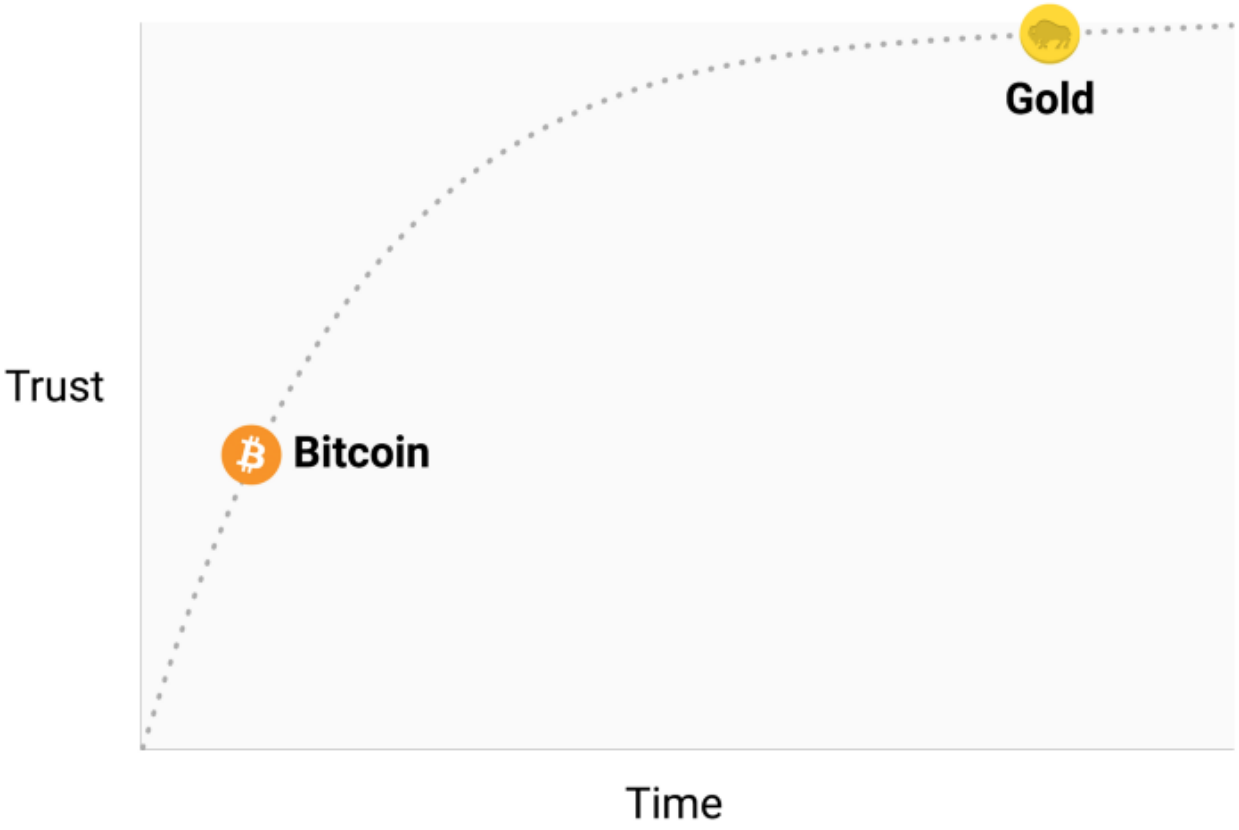
Bitcoins can be divided down to a hundred millionth of a bitcoin and transmitted at such infinitesimal amounts (network fees can, however, make transmission of tiny amounts uneconomic). Fiat currencies are typically divisible down to pocket change, which has little purchasing power, making fiat divisible 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.

Scarcity:

The attribute that most clearly distinguishes Bitcoin from fiat currencies and gold is its predetermined scarcity. By design, at most 21 million bitcoins can ever be created. This gives the owner of bitcoins a known percentage of the total possible supply. For instance, an owner of 10 bitcoins would know that at most 2.1 million people on earth (less than 0.03% of the world's population) could ever have as many bitcoins as they had. 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 (examples include 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. Nations-states have shown a persistent proclivity to inflate their money supply to solve short-term political problems. The inflationary tendencies of governments across the world leave the owner of a fiat currency with the likelihood that their savings will diminish in value over time.

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 few states in history have been able to resist. If the 20th century, in which fiat monies came to dominate the global monetary order, established any economic truth, it is that fiat money cannot be trusted to maintain its value over the long or even medium term. 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. In other words, the societal trust of a new monetary good is asymptotic in nature, as is illustrated in the graph below:



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 resistance:

One of the most significant sources of early demand for bitcoins was their use in the illicit drug trade. Many subsequently surmised, mistakenly, that the primary demand for bitcoins was due to their ostensible anonymity. Bitcoin, however, is far from an anonymous currency; every transaction transmitted on the Bitcoin network is forever recorded on a public blockchain. The historical record of transactions allows for later forensic analysis to identify the source of a flow of funds. It was such an analysis that led to the apprehending of a perpetrator of the infamous MtGox heist. While it is true that a sufficiently careful and diligent person can conceal their identity when using Bitcoin, this is not why Bitcoin was so popular for trading drugs. 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. 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.

Bitcoin excels across the majority of attributes listed above, allowing it to outcompete modern and ancient monetary goods at the margin and providing a strong incentive for its increasing adoption. In particular, the potent combination of censorship resistance and absolute scarcity has been a powerful motivator for wealthy investors to allocate a portion of their wealth to the nascent asset class.

The Evolution of Money

There is an obsession in modern monetary economics with the medium of exchange role of money. In the 20th century, states have monopolized the issuance of money and continually undermined its use as a store of value, creating a false belief that money is primarily defined as a medium of exchange. Many have criticized Bitcoin as being an unsuitable money because its price has been too volatile to be suitable as a medium of exchange. This puts the cart before the horse, however. Money has always evolved in stages, with the store of value role preceding the medium of exchange role. One of the fathers of marginalist economics, William Stanley Jevons, explained that:

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.

Using modern terminology, money always evolves in the following four stages:

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. In the earliest days of Bitcoin, many people did not appreciate the huge opportunity cost of using bitcoins as a medium of exchange, rather than as an incipient store of value. The famous story of a man trading 10,000 bitcoins (worth approximately $94 million at the time of this article's writing) for two pizzas illustrates this confusion.
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. It is a common misconception that bitcoin prices are available for many goods today. For example, while a cup of coffee might be available for purchase using bitcoins, the price listed is not a true bitcoin price; rather it is the dollar price desired by the merchant translated into bitcoin terms at the current USD/BTC market exchange rate. If the price of bitcoin were to drop in dollar terms, the number of bitcoins requested by the merchant would increase commensurately. Only when merchants are willing to accept bitcoins for payment without regard to the bitcoin exchange rate against fiat currencies can we truly think of Bitcoin as having become a unit of account.

Monetary goods that are not yet a unit of account may be thought of as being "partly monetized". Today gold fills such a role, being a store of value but having been stripped of its medium of exchange and unit of account roles by government intervention. It is also possible that one good fills the medium of exchange role of money while another good fills the other roles. This is typically true in countries with dysfunctional states, such as Argentina or Zimbabwe. In his book Digital Gold, Nathaniel Popper writes:

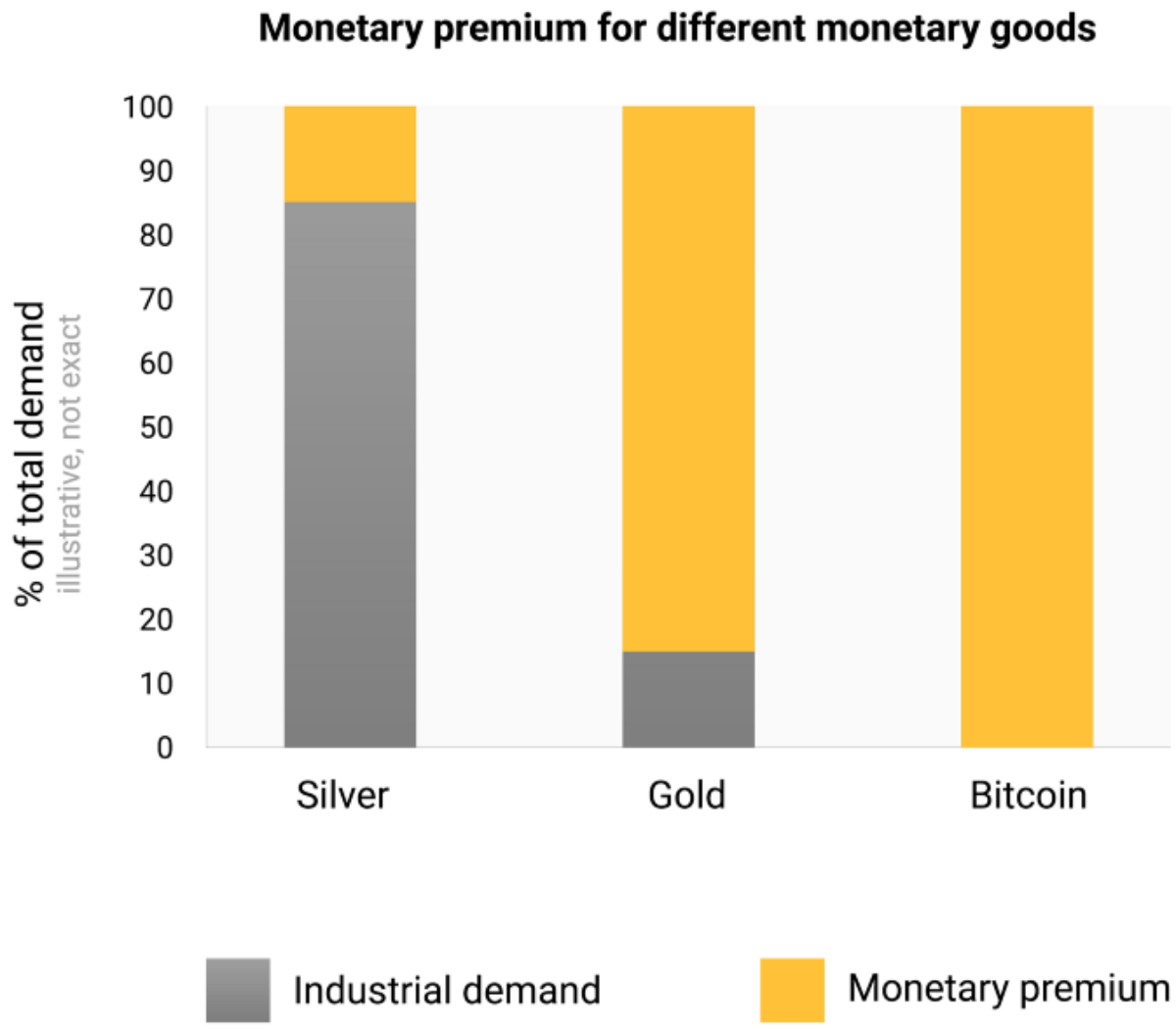
In America, the dollar seamlessly serves the three functions of money: providing a medium of exchange, a unit for measuring the cost of goods, and an asset where value can be stored. In Argentina, on the other hand, while the peso was used as a medium of exchange — for daily purchases — no one used it as a store of value. Keeping savings in the peso was equivalent to throwing away money. So people exchanged any pesos they wanted to save for dollars, which kept their value better

than the peso. Because the peso was so volatile, people usually remembered prices in dollars ,which provided a more reliable unit of measure over time.

Bitcoin is currently transitioning from the first stage of monetization to the second stage. It will likely be several years before Bitcoin transitions from being an incipient store of value to being a true medium of exchange, and the path it takes to get there is still fraught with risk and uncertainty. It is striking to note that the same transition took many centuries for gold. No one alive has seen the real-time monetization of a good (as is taking place with Bitcoin), so there is precious little experience regarding the path this monetization will take.

Path dependence

In the process of being monetized, a monetary good will soar in purchasing power. Many have commented that the increase in purchasing power of Bitcoin creates the appearance of a "bubble". While this term is often using disparagingly to suggest that Bitcoin is grossly overvalued, it is unintentionally apt. A characteristic that is common to all monetary goods is that their purchasing power is higher than can be justified by their use-value alone. Indeed, many historical monies had no use-value at all. The difference between the purchasing power of a monetary good and the exchange-value it could command for its inherent usefulness can be thought of as a "monetary premium". As a monetary good transitions through the stages of monetization (listed in the section above), the monetary premium will increase. The premium does not, however, move in a straight, predictable line. A good X that was in the process of being monetized may be outcompeted by another good Y that is more suitable as money, and the monetary premium of X may drop or vanish entirely. The monetary premium of silver disappeared almost entirely in the late 19th century when governments across the world largely abandoned it as money in favor of gold.



Even in the absence of exogenous factors such as government intervention or competition from other monetary goods, the monetary premium for a new money will not follow a predictable path. Economist Larry White observed that:

the trouble with [the] bubble story, of course, is that [it] is consistent with *any* price path, and thus gives no explanation for a particular price path

The process of monetization is game-theoretic; every market participant attempts to anticipate the aggregate demand of other participants and thereby the future monetary premium. Because the monetary premium is unanchored to any inherent usefulness, market participants tend to default to past prices when determining whether a monetary good is cheap or expensive and whether to buy or sell it. The connection of current demand to past prices is known as "path dependence" and is perhaps the greatest source of confusion in understanding the price movements of monetary goods.

When the purchasing power of a monetary good increases with increasing adoption, market expectations of what constitutes "cheap" and "expensive" shift accordingly. Similarly, when the price of a monetary good crashes, expectations can switch to a general belief that prior prices were "irrational" or overly inflated. The path dependence of money is illustrated by the words of well-known Wall Street fund manager Josh Brown:

I bought [bitcoins] at like $2300 and had an immediate double on my hands. Then I started saying "I can't buy more of it," as it rose, even though that's an anchored opinion based on nothing other than the price where I originally got it. Then, as it fell over the last week because of a Chinese crackdown on the exchanges, I started saying to myself, "Oh good, I hope it gets killed so I can buy more."

The truth is that the notions of "cheap" and "expensive" are essentially meaningless in reference to monetary goods. The price of a monetary good is not a reflection of its cash flow or how useful it is but, rather, is a measure of how widely adopted it has become for the various roles of money.

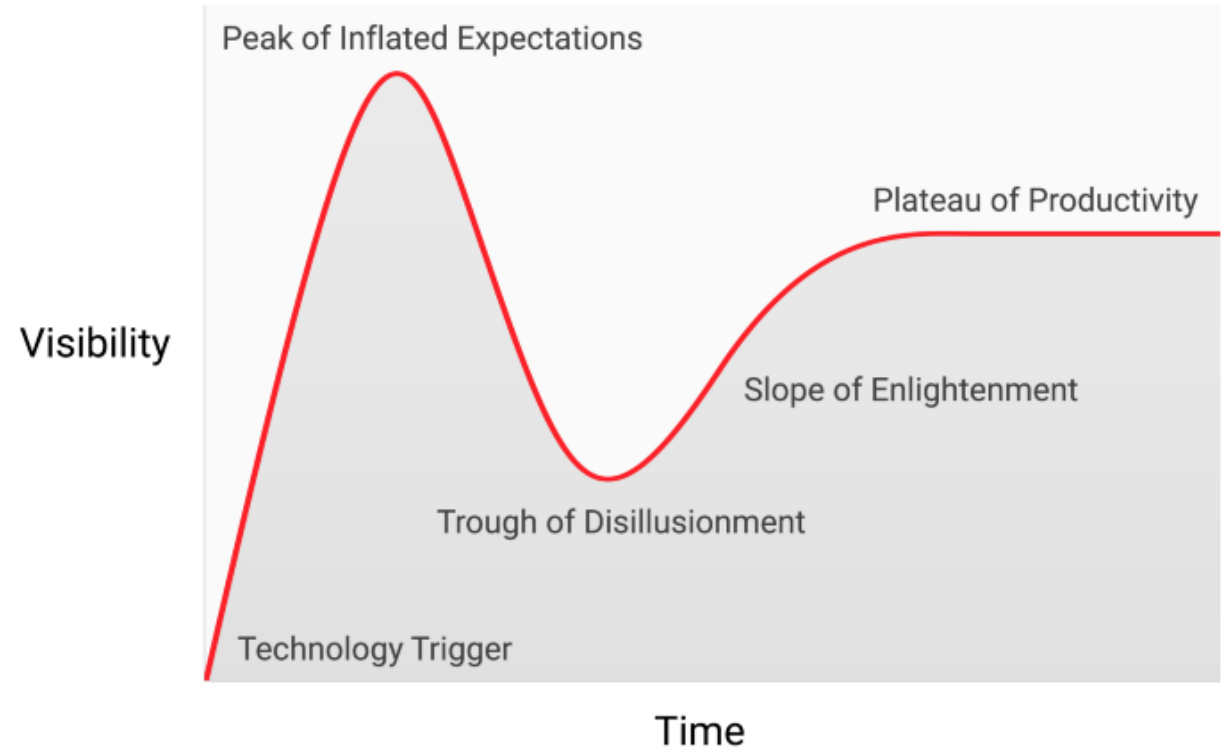
Further complicating the path-dependent nature of money is the fact that market participants do not merely act as dispassionate observers, trying to buy or sell in anticipation of future movements of the monetary premium, but also act as active evangelizers. Since there is no objectively correct monetary premium, proselytizing 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.

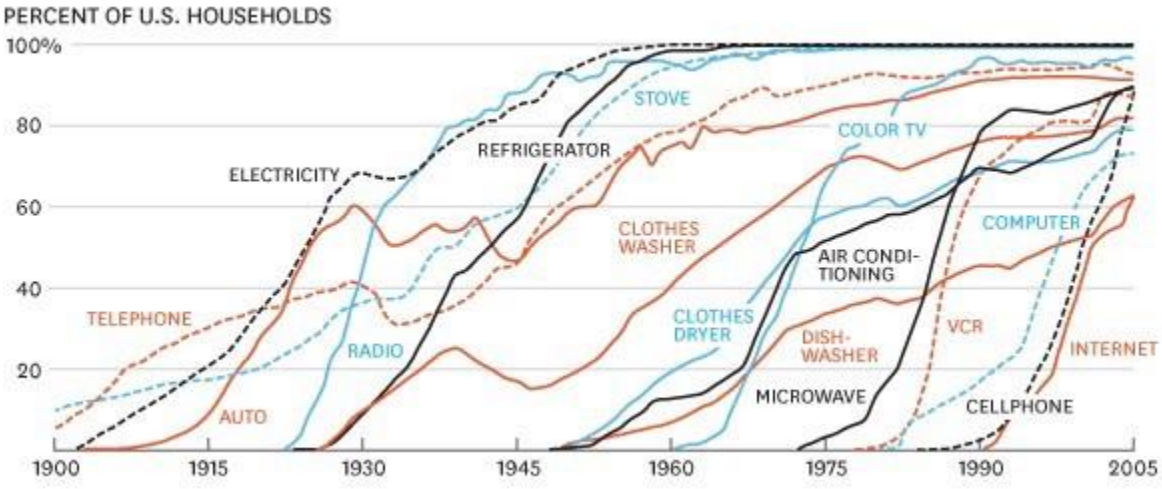
While the comparison to religion may give Bitcoin an aura of irrational faith, it is entirely rational for the individual owner to evangelize for a superior monetary good and for society as a whole to standardize on it. Money acts as the foundation for all trade and savings, so the adoption of a superior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

The shape of monetization

While there are no *a priori* rules about the path a monetary good will take as it is monetized, a curious pattern has emerged during the relatively brief history of Bitcoin's monetization. Bitcoin's price appears to follow a fractal pattern of increasing magnitude, where each iteration of the fractal matches the classic shape of a Gartner hype cycle.



In his article on the Speculative Bitcoin Adoption/Price Theory, Michael Casey posits that the expanding Gartner hype cycles represent phases of a standard S-curve of adoption that was followed by many transformative technologies as they become commonly used in society.



Each Gartner hype cycle begins with a burst of enthusiasm for the new technology, and the price is bid up by the market participants who are "reachable" in that iteration. The earliest buyers in a Gartner hype cycle typically have a strong conviction about the transformative nature of the technology they are investing in. Eventually the market reaches a crescendo of enthusiasm as the supply of new participants who can be reached in the cycle is exhausted and the buying becomes

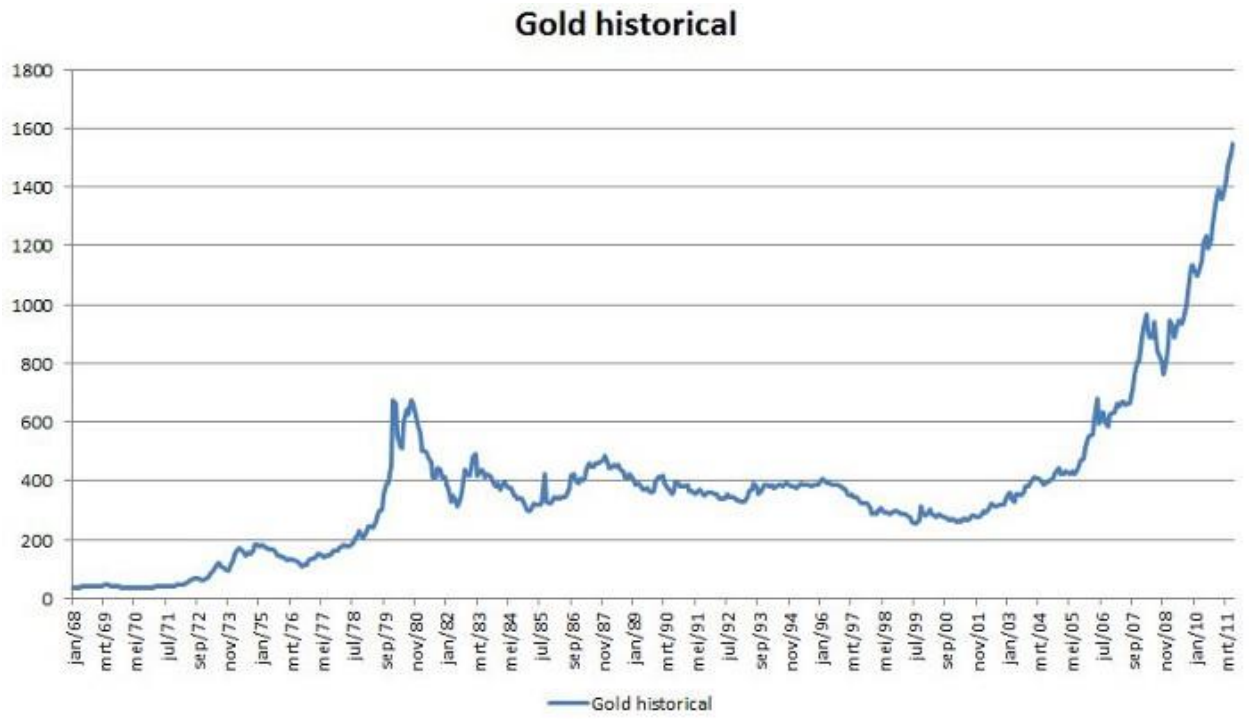
dominated by speculators more interested in quick profits than the underlying technology.

Following the peak of the hype cycle, prices rapidly drop and the speculative fervor is replaced by despair, public derision and a sense that the technology was not transformative at all. Eventually the price bottoms and forms a plateau where the original investors who had strong conviction are joined by a new cohort who were able to withstand the pain of the crash and who appreciated the importance of the technology.

The plateau persists for a prolonged period of time and forms, as Casey calls it, a "stable, boring low". During the plateau, public interest in the technology will dwindle but it will continue to be developed and the collection of strong believers will slowly grow. A new base is then set for the next iteration of the hype cycle as external observers recognize the technology is not going away and that investing in it may not be as risky as it seemed during the crash phase of the cycle. The next iteration of the hype cycle will bring in a much larger set of adopters and be far greater in magnitude.

Very few people participating in an iteration of a Gartner hype cycle will correctly anticipate how high prices will go in that cycle. Prices usually reach levels that would seem absurd to most investors at the earliest stages of the cycle. When the cycle ends, a popular cause it typically attributed to the crash by the media. While the stated cause (such as an exchange failure) may be a precipitating event, it is not the fundamental reason for the cycle to end. Gartner hype cycles end because of an exhaustion of market participants reachable in the cycle.

It is telling that gold followed the classic pattern of a Gartner hype cycle from the late 1970s to the early 2000s. One might speculate that the hype cycle is an inherent social dynamic to the process of monetization.



Gartner cohorts

Since the inception of the first exchange traded price in 2010, the Bitcoin market has witnessed four major Gartner hype cycles. With hindsight we can precisely identify the price ranges of previous hype cycles in the Bitcoin market. We can also qualitatively identify the cohort of investors that were associated with each iteration of prior cycles.

$0– **$1** (2009–March 2011): The first hype cycle in the Bitcoin market was dominated by cryptographers, computer scientists and cypherpunks who were already primed to understand the importance of Satoshi Nakamoto's groundbreaking invention and who were pioneers in establishing that the Bitcoin protocol was free of technical flaws.

$1– **$30** (March 2011–July 2011): The second cycle attracted both early adopters of new technology and a steady stream of ideologically motivated investors who were dazzled by the potential of a stateless money. Libertarians such as Roger Ver were attracted to Bitcoin for the anti-establishment activities that would become possible if the nascent technology became widely adopted. Wences Casares, a brilliant and well-connected serial entrepreneur, was also part of the second Bitcoin hype cycle and is known to have evangelized Bitcoin to some of the most prominent technologists and investors in Silicon Valley.

$250– **$1100** (April 2013–December 2013): The third hype cycle saw the entrance of early retail and institutional investors who were willing to brave the horrendously complicated and risky liquidity channels from which bitcoins could be bought. The primary source of liquidity in the market during this period was the Japan-based

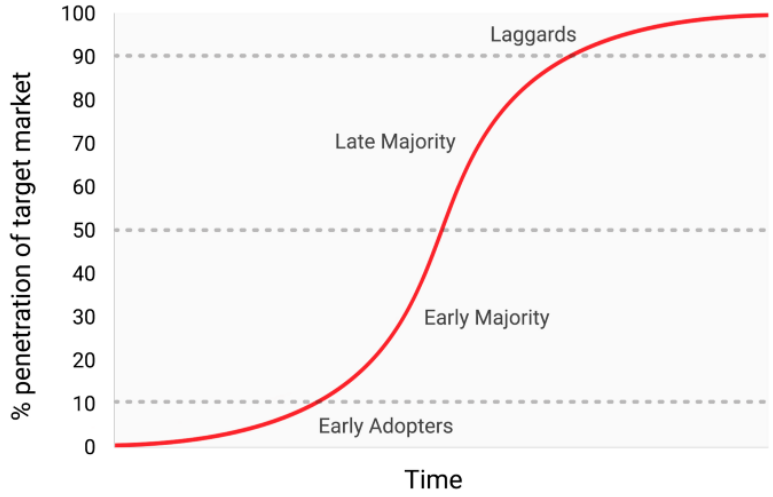
MtGox exchange that was run by the notoriously incompetent and malfeasant Mark Karpeles, who later saw prison time for his role in the collapse of the exchange.

It is worth observing that the rise in Bitcoin's price during the aforementioned hype cycles was largely correlated with an increase in liquidity and the ease with which investors could purchase bitcoins. In the first hype cycle, there were no exchanges available, and acquisition of bitcoins was primarily through mining or by direct exchange with someone who had already mined bitcoins. In the second hype cycle, rudimentary exchanges became available, but obtaining and securing bitcoins from these exchanges remained too complex for all but the most technologically savvy investors. Even in the third hype cycle, significant hurdles remained for investors transferring money to MtGox to acquire bitcoins. Banks were reluctant to deal with the exchange, and third party vendors who facilitated transfers were often incompetent, criminal, or both. Further, many who did manage to transfer money to MtGox ultimately faced loss of funds when the exchange was hacked and later closed.

It was only after the collapse of the MtGox exchange and a two-year lull in the market price of Bitcoin that mature and deep sources of liquidity were developed; examples include regulated exchanges such as GDAX and OTC brokers such as Cumberland mining. By the time the fourth hype cycle began in 2016 it was relatively easy for retail investors to buy bitcoins and secure them.

$1100– $19600? (2014– ?):

At the time of writing, the Bitcoin market is undergoing its fourth major hype cycle. Participation in the current hype cycle has been dominated by what Michael Casey described as the "early majority" of retail and institutional investors.



As sources of liquidity have deepened and matured, major institutional investors now have the opportunity to participate through regulated futures markets. The availability of a regulated futures market paves the way for the creation of a Bitcoin

ETF, which will then usher in the "late majority" and "laggards" in subsequent hype cycles.

Although it is impossible to predict the exact magnitude of the current hype cycle, it would be reasonable to conjecture that the cycle reaches its zenith in the range of $20,000 to $50,000. Much higher than this range and Bitcoin would command a significant fraction of gold's entire market capitalization (gold and Bitcoin would have equivalent market capitalizations at a bitcoin price of approximately $380,000 at the time of writing). A significant fraction of gold's market capitalization comes from central bank demand and it's unlikely that central banks or nation states will participate in this particular hype cycle.

The entrance of nation-states

Bitcoin's final Gartner hype cycle will begin when nation-states start accumulating it as a part of their foreign currency reserves. The market capitalization of Bitcoin is currently too small for it to be considered a viable addition to reserves for most countries. However, as private sector interest increases and the capitalization of Bitcoin approaches 1 trillion dollars it will become liquid enough for most states to enter the market. The entrance of the first state to officially add bitcoins to their reserves will likely trigger a stampede for others to do so. The states that are the earliest in adopting Bitcoin would see the largest benefit to their balance sheets if Bitcoin ultimately became a global reserve currency. Unfortunately, it will probably be the states with the strongest executive powers — dictatorships such as North Korea — that will move the fastest in accumulating bitcoins. The unwillingness to see such states improve their financial position and the inherently weak executive branches of the Western democracies will cause them to dither and be laggards in accumulating bitcoins for their reserves.

There is a great irony that the US is currently one of the nations most open in its regulatory position toward Bitcoin, while China and Russia are the most hostile. The US risks the greatest downside to its geopolitical position if Bitcoin were to supplant the dollar as the world's reserve currency. In the 1960s, Charle de Gaulle criticized the "exorbitant privilege" the US enjoyed from the international monetary order it crafted with the Bretton Woods agreement of 1944. The Russian and Chinese governments have not yet awoken to the geo-strategic benefits of Bitcoin as a reserve currency and are currently preoccupied with the effects it may have on their internal markets. Like de Gaulle in the 1960s, who threatened to reestablish the classical gold standard in response to the US's exorbitant privilege, the Chinese and Russians will, in time, come to see the benefits of a large reserve position in a non-sovereign store of value. With the largest concentration of Bitcoin mining power residing in China, the Chinese state already has a distinct advantage in its potential to add bitcoins to its reserves.

The US prides itself as a nation of innovators, with Silicon Valley being a crown jewel of the US economy. Thus far, Silicon Valley has largely dominated the conversation toward regulators on the position they should take vis-à-vis Bitcoin. However, the

banking industry and the US Federal Reserve are finally having their first inkling of the existential threat Bitcoin poses to US monetary policy if it were to become a global reserve currency. The Wall Street Journal, known to be a mouth-piece for the Federal Reserve, published a commentary on the threat Bitcoin poses to US monetary policy:

There is another danger, perhaps even more serious from the point of view of the central banks and regulators: bitcoin might not crash. If the speculative fervor in the cryptocurrency is merely the precursor to it being widely used as an alternative to the dollar, it will threaten the central banks' monopoly on money.

In the coming years there will be a great struggle between entrepreneurs and innovators in Silicon Valley, who will attempt to keep Bitcoin free of state control, and the banking industry and central banks who will do everything in their power to regulate Bitcoin to prevent their industry and money-issuing powers from being disrupted.

The transition to a medium of exchange

A monetary good cannot transition to being a generally accepted medium of exchange (the standard economic definition of "money") before it is widely valued, for the tautological reason that a good that is not valued will not be accepted in exchange. In the process of becoming widely valued, and hence a store of value, a monetary good will soar in purchasing power, creating an opportunity cost to relinquishing it for use in exchange. Only when the opportunity cost of relinquishing a store of value drops to a suitably low level can it transition to becoming a generally accepted medium of exchange.

More precisely, a monetary good will only be suitable as a medium of exchange when the sum of the opportunity cost and the transactional cost of using it in exchange drops below the cost of completing a trade without it.

In a barter-based society, the transition of a store of value to a medium of exchange can occur even when the monetary good is increasing in purchasing power because the transactional costs of barter trade are extremely high. In a developed economy, where transactional costs are low, it is possible for a nascent and rapidly appreciating store of value, such as Bitcoin, to be used as a medium of exchange, albeit in a very limited scope. An example is the illicit drug market where buyers are willing to sacrifice the opportunity of holding bitcoins to minimize the substantial risk of purchasing the drugs using fiat currency.

There are, however, major institutional barriers to a nascent store of value becoming a *generally* accepted medium of exchange in a developed society. States use taxation as a powerful means to protect their sovereign money from being displaced by competing monetary goods. Not only does a sovereign money enjoy the advantage of a constant source of demand, by way of taxes being remittable only in it, but competing monetary goods are taxed whenever they are exchanged

at an appreciated value. This latter kind of taxation creates significant friction to using a store of value as a medium of exchange.

The handicapping of market-based monetary goods is not an insurmountable barrier to their adoption as a generally accepted medium of exchange, however. If faith is lost in a sovereign money, its value can collapse in a process known as hyperinflation. When a sovereign money hyperinflates, its value first collapses against the most liquid goods in the society, such as gold or a foreign money like the US dollar, if they are available. When no liquid goods are available or their supply is limited, a hyperinflating money collapses against real goods, such as real estate and commodities. The archetypal image of a hyperinflation is a grocery store emptied of all its produce as consumers flee the rapidly diminishing value of their nation's money.

Eventually, when faith is completely lost during a hyperinflation, a sovereign money will no longer be accepted by anyone, and the society will either devolve to barter or the monetary unit will be completely replaced as a medium of exchange. An example of this process was the replacement of the Zimbabwe dollar with the US dollar. The replacement of a sovereign money with a foreign one is made more difficult by the scarcity of the foreign money and the absence of foreign banking institutions to provide liquidity.

The ability to easily transmit bitcoins across borders and absence of a need for a banking system make Bitcoin an ideal monetary good to acquire for those afflicted by hyperinflation. In the coming years, as fiat monies continue to follow their historical trend toward eventual worthlessness, Bitcoin will become an increasingly

popular choice for global savings to flee to. When a nation's money is abandoned and replaced by Bitcoin, Bitcoin will have transitioned from being a store of value in that society to a generally accepted medium of exchange. Daniel Krawisz coined the term "hyperbitcoinization" to describe this process.

Common misconceptions

Much of this article has focused on the monetary nature of Bitcoin. With this foundation we can now address some of the most commonly held misconceptions about Bitcoin.

Bitcoin is a bubble

Bitcoin, like all market-based monetary goods, displays a monetary premium. The monetary premium is what gives rise to the common criticism that Bitcoin is a "bubble". However, *all* monetary goods display a monetary premium. Indeed, it is this premium (the excess over the use-demand price) that is the defining characteristic of all monies. In other words, money is always and everywhere a bubble. Paradoxically, a monetary good is both a bubble and may be undervalued if it's in the early stages of its adoption for use as money.

Bitcoin is too volatile

Bitcoin's price volatility is a function of its nascency. In the first few years of its existence, Bitcoin behaved like a penny-stock, and any large buyer — such as the

Winklevoss twins — could cause a large spike in its price. As adoption and liquidity have increased over the years, Bitcoin's volatility has decreased commensurately. When Bitcoin achieves the market capitalization of gold, it will display a similar level of volatility. As Bitcoin surpasses the market capitalization of gold, its volatility will decrease to a level that will make it suitable as a widely used medium of exchange. As previously noted, the monetization of Bitcoin occurs in a series of Gartner hype cycles. Volatility is lowest during the plateau phase of the hype cycle, while it is highest during the peak and crash phases of the cycle. Each hype cycle has lower volatility than the previous ones because the liquidity of the market has increased.

Transaction fees are too high

A recent criticism of the Bitcoin network is that the increase in fees to transmit bitcoins makes it unsuitable as a payment system. However, the growth in fees is healthy and expected. Transaction fees are the cost required to pay bitcoin miners to secure the network by validating transactions. Miners can either be paid by transaction fees or by block rewards, which are an inflationary subsidy borne by current bitcoin owners.

Given Bitcoin's fixed supply schedule — a monetary policy which makes it ideally suited as a store of value — block rewards will eventually decline to zero and the network must ultimately be secured with transaction fees. A network with "low" fees is a network with little security and prone to external censorship. Those touting the low fees of Bitcoin alternatives are unknowingly describing the weakness of these so-called "alt-coins".

The specious root of the criticism of Bitcoin's "high" transaction fees is the belief that Bitcoin should be a payment system first and a store of value later. As we have seen with the origins of money, this belief puts the cart before the horse. Only when Bitcoin has become a deeply established store of value will it become suitable as a medium of exchange. Further, once the opportunity cost of trading bitcoins is at a level at which it is suitable as a medium of exchange, most trades will not occur on the Bitcoin network itself but on "second layer" networks with much lower fees. Second layer networks, such as the Lightning network, provide the modern equivalent of the promissory notes that were used to transfer titles for gold in the 19th century. Promissory notes were used by banks because transferring the underlying bullion was far more costly than transferring the note that represented title to the gold. Unlike promissory notes, however, the Lightning network will allow the transfer of bitcoins at low cost while requiring little or no trust of third parties such as banks. The development of the Lightning network is a profoundly important technical innovation in Bitcoin's history and its value will become apparent as it is developed and adopted in the coming years.

Competition

As an open-source software protocol, it has always been possible to copy Bitcoin's software and imitate its network. Over the years, many imitators have been created, ranging from ersatz facsimiles, such as Litecoin, to complex variants like Ethereum that promise to allow arbitrarily complex contractual arrangements using a distributed computational system. A common investment criticism of Bitcoin is that it cannot maintain its value when competitors can be easily created that are able to incorporate the latest innovations and software features.

The fallacy in this argument is that the scores of Bitcoin competitors that have been created over the years lack the "network effect" of the first and dominant technology in the space. A network effect — the increased value of using Bitcoin simply because it is already the dominant network — is a feature in and of itself. For any technology that possesses a network effect, it is by far the most important feature.

The network effect for Bitcoin encompasses the liquidity of its market, the number of people who own it, and the community of developers maintaining and improving upon its software and its brand awareness. Large investors, including nation-states, will seek the most liquid market so that they can enter and exit the market quickly without affecting its price. Developers will flock to the dominant development community which has the highest-calibre talent, thereby reinforcing the strength of that community. And brand awareness is self-reinforcing, as would-be competitors to Bitcoin are always mentioned in the context of Bitcoin itself.

A fork in the road

A trend that became popular in 2017 was not only to imitate Bitcoin's software, but to copy the entire history of its past transactions (known as the blockchain). By copying Bitcoin's blockchain up to a certain point and then splitting off into a new network, in a process known as "forking", competitors to Bitcoin were able to solve the problem of distributing their token to a large user base.

The most significant fork of this kind occurred on August 1st, 2017 when a new network known as Bitcoin Cash (BCash) was created. An owner of N bitcoins before August 1st, 2017, would then own both N bitcoins and N BCash tokens. The small but vocal community of BCash proponents have tirelessly attempted to expropriate Bitcoin's brand recognition, both through the naming of their new network and a campaign to convince neophytes in the Bitcoin market that Bcash is the "real" Bitcoin. These attempts have largely failed, and this failure is reflected in the market capitalizations of the two networks. However, for new investors, there remains an apparent risk that a competitor might clone Bitcoin and its blockchain and succeed in overtaking it in market capitalization, thus becoming the de facto Bitcoin.

An important rule can be gleaned from the major forks that have happened to both the Bitcoin and Ethereum networks. The majority of the market capitalization will settle on the network that retains the highest-calibre and most active developer community. For although Bitcoin can be viewed as a nascent money, it is also a computer network built on software that needs to be maintained and improved upon. Buying tokens on a network which has little or inexperienced developer support would be akin to buying a clone of Microsoft Windows that was not supported by Microsoft's best developers. It is clear from the history of the forks that occurred in 2017 that the best and most experienced computer scientists and cryptographers are committed to developing for the original Bitcoin and not any of the growing legion of imitators that have been created from it.

Real risks

Although the common criticisms of Bitcoin found in the media and economics profession are misplaced and based on a flawed understanding of money, there are real and significant risks to investing in Bitcoin. It would be prudent for a prospective Bitcoin investor to understand and weigh these risks before considering an investment in Bitcoin.

Protocol risk

The Bitcoin protocol and the cryptographic primitives that it is built upon could be found to have a design flaw, or could be made insecure with the development of quantum computing. If a flaw is found in the protocol, or some new means of computation makes possible the breaking of the cryptography underpinning Bitcoin, the faith in Bitcoin may be severely compromised. The protocol risk was highest in the early years of Bitcoin's development, when it was still unclear, even to seasoned cryptographers, that Satoshi Nakamoto had actually found a solution to the Byzantine Generals' Problem. Concerns about serious flaws in the Bitcoin protocol have dissipated over the years, but given its technological nature, protocol risk will always remain for Bitcoin, if only as an outlier risk.

Exchange shutdowns

Being decentralized in design, Bitcoin has shown a remarkable degree of resilience in the face of numerous attempts by various governments to regulate it or shut it down. However, the exchanges where bitcoins are traded for fiat currencies are highly centralized and susceptible to regulation and closure. Without these exchanges and the willingness of the banking system to do business with them, the process of monetization of Bitcoin would be severely stunted, if not halted completely. While there are alternative sources of liquidity for Bitcoin, such as over-the-counter brokers and decentralized markets for buying and selling Bitcoins (like localbitcoins.com), the critical process of price discovery happens on the most liquid exchanges, which are all centralized.

Mitigating the risk of exchange shutdowns is jurisdictional arbitrage. Binance, a prominent exchange that started in China, moved to Japan after the Chinese government halted its operations in China. National governments are also wary of smothering a nascent industry that may prove as consequential as the Internet, thereby ceding a tremendous competitive advantage to other nations.

Only with a coordinated global shutdown of Bitcoin exchanges would the process of monetization be halted completely. The race is on for Bitcoin to become so widely adopted that a complete shutdown becomes as politically infeasible as a complete shutdown of the Internet. The possibility of such a shutdown is still real, however, and must be factored into the risks of investing in Bitcoin. As was discussed in the prior section on the entrance of nation-states, national governments are finally

awakening to the threat that a non-sovereign, censorship-resistant, digital currency poses to their monetary policies. It is an open question whether they will act on this threat before Bitcoin becomes so entrenched that political action against it proves ineffectual.

Fungibility

The open and transparent nature of the Bitcoin blockchain makes it possible for states to mark certain bitcoins as being "tainted" by their use in proscribed activities. Although Bitcoin's censorship resistance at the protocol level allows these bitcoins to be transmitted, if regulations were to appear that banned the use of such tainted bitcoins by exchanges or merchants, they could become largely worthless. Bitcoin would then lose one of the critical properties of a monetary good: fungibility.

To ameliorate Bitcoin's fungibility, improvements will need to be made at the protocol level to improve the privacy of transactions. While there are new developments in this regard, pioneered in digital currencies such as Monero and Zcash, there are major technological tradeoffs to be made between the efficiency and complexity of Bitcoin and its privacy. It remains an open question whether privacy-enhancing features can be added to Bitcoin in a way that doesn't compromise its usefulness as money in other ways.

Conclusion

Bitcoin is an incipient money that is transitioning from the collectible stage of monetization to becoming a store of value. As a non-sovereign monetary good, it is possible that at some stage in the future Bitcoin will become a global money much like gold during the classical gold standard of the 19th century. The adoption of Bitcoin as global money is precisely the bullish case for Bitcoin, and was articulated by Satoshi Nakamoto as early as 2010 in an email exchange with Mike Hearn:

If you imagine it being used for some fraction of world commerce, then there's only going to be 21 million coins for the whole world, so it would be worth much more per unit.

This case was made even more trenchantly by the brilliant cryptographer Hal Finney, the recipient of the first bitcoins sent by Nakamoto, shortly after the announcement of the first working Bitcoin software:

[I]magine that Bitcoin is successful and becomes the dominant payment system in use throughout the world. Then the total value of the currency should be equal to the total value of all the wealth in the world. Current estimates of total worldwide household wealth that I have found range from $100 trillion to $300 trillion. With 20 million coins, that gives each coin a value of about $10 million.

Even if Bitcoin were not to become a fully fledged global money and were simply to compete with gold as a non-sovereign store of value, it is currently massively undervalued. Mapping the market capitalization of the extant above-ground gold

supply (approximately 8 trillion dollars) to a maximum Bitcoin supply of 21 million coins gives a value of approximately $380,000 per bitcoin. As we have seen in prior sections, for the attributes that make a monetary good suitable as a store of value, Bitcoin is superior to gold along every axis except for established history. As time passes and the Lindy effect takes hold, established history will no longer be a competitive advantage for gold. Thus, it is not unreasonable to expect that Bitcoin will approach, and perhaps surpass, gold's market capitalization in the next decade. A caveat to this thesis is that a large fraction of gold's capitalization comes from central banks holding it as a store of value. For Bitcoin to achieve or surpass gold's capitalization, some participation by nation-states will be necessary. Whether the Western democracies will participate in the ownership of Bitcoin is unclear. It is more likely, and unfortunate, that tin-pot dictatorships and kleptocracies will be the first nations to enter the Bitcoin market.

If no nation-states participate in the Bitcoin market, there still remains a bullish case for Bitcoin. As a non-sovereign store of value used only by retail and institutional investors, Bitcoin is still early in its adoption curve — the so-called "early majority" are now entering the market while the late majority and laggards are still years away from entering. With broader participation from retail and especially institutional investors, a price level between $100,000 and $200,000 is feasible.

Owning bitcoins is one of the few asymmetric bets that people across the entire world can participate in. Much like a call option, an investor's downside is limited to 1x, while their potential upside is still 100x or more. Bitcoin is the first truly global bubble whose size and scope is limited only by the desire of the world's citizenry to protect their savings from the vagaries of government economic mismanagement. 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.

Beyond the financial case for Bitcoin, its rise as a non-sovereign store of value will have profound geopolitical consequences. A global, non-inflationary reserve currency will force nation-states to alter their primary funding mechanism from inflation to direct taxation, which is far less politically palatable. States will shrink in size commensurate to the political pain of transitioning to taxation as their exclusive means of funding. Furthermore, global trade will be settled in a manner that satisfies Charles de Gaulle's aspiration that no nation should have privilege over any other:

We consider it necessary that international trade be established, as it was the case, before the great misfortunes of the World, on an indisputable monetary base, and one that does not bear the mark of any particular country.

50 years from now, that monetary base will be Bitcoin.

Translations

This article has been translated into:

- English podcast by Heardit.
- English podcast by Cryptoconomy.
- Podcast interview about the article with Peter McCormack.
- Deutsche by Daniel Schnurr,Simon Lutz and Arlene Roa Aillaud.
- Österreichisches Deutsch by Bernie Eder.
- Korean by Hyungmok joh (part 1,part 2,part 3,part 4).
- Traditional Chinese by Flora Sun (part 1,part 2,part 3,part 4)
- Simplified Chinese by Flora Sun (part 1,part 2,part 3,part 4)
- Español by Iñigo and Carlos Beltrán (part 1,part 2,part 3,part4).
- Nederlandse by Wim, edited by Koen Swinkels (part 1,part 2,part 3,part 4).
- Française by Greg Guittard (part 1,part 2,part 3,part 4).
- Italiano by Ryan DeLongpre.
- Português by Allex Fer (part 1,part 2,part 3,part 4).
- Tamil by Balaji Vaidyanath and Mahadevan Vaidyanath (part 1).
- русский/Russian by CoinSpot (part 1,part 2,part 3,part 4).
- Bulgarian by Bo Mirchev (part 1,part 2,part 3,part 4).

About me

I'm a former Google engineer who's interested in Austrian economics. I'm also a husband and loving father of Addie and Will. Follow me on Twitter.

Acknowledgements

I want to thank Alex Morcos, John Pfeffer, Pierre Rochard, Mat Balez, Ray Boyapati, Daniel Coleman, Koen Swinkels, Patri Friedman, Ardian Tola, Michael Flaxman and Michael Hartl for their valuable feedback on earlier drafts of this series of articles. Sanjay Mavinkurve generously provided his brilliant design skills to create some of the charts.

Disclaimer

The views presented in this article and any errors herein are my own.

This article is for information purposes only. It is not intended to be investment advice. Seek a duly licensed professional for investment advice.

How Blockchains Will Enable Privacy

By Shaan Ray

Posted March 3, 2018

Technology has eroded our privacy protections. Most things individuals or organizations do are now in the public domain. Third-parties monitor, store, and use personal and organizational data, patterns, preferences, and activities. Many emerging business models rely on the collection, organization, and resale of our personal data.

Technology has also made it easier to link data back to an individual, even if that individual opts out of social networking platforms. For example, breakthroughs in facial recognition technology have found broad application in commerce and security, especially in China and Russia.

Blockchain technology could potentially limit the impact of this erosion of privacy, while still releasing personal information when it is useful. For example, a user could store personal information on a blockchain and release parts of it temporarily to receive services. Bitcoin and other blockchain-based digital currencies have demonstrated that trusted and transparent computing is possible using a peer-to-peer decentralized network and a public ledger.

This essay explores the impact that data generation by individuals and organizations is having on privacy. It also briefly considers how blockchain-enabled systems could help put users back in charge of their data.

Part 1: The Individual

Individuals

Privacy is important to individuals because their personal information is valuable to organizations, marketers and other individuals. A common saying among internet users is: if you aren't paying for the product, you are the product. This means that for companies that offer free services, such as social networking platforms, personal information is valuable.

Constitutional Protections

In the US, privacy is important for the exercise of various constitutional rights, including the rights to free speech, free association, free press, protection from unreasonable searches and seizures, and protection from self-incrimination. A lack of privacy from state actors imperils these rights. Knowing that their statements will be attributed to them in the public domain, an individual may not speak up about just causes, especially if their opinion or the subject is controversial or unpopular. Since many important opinions are unpopular or controversial, self-censorship should be of serious concern to society. Knowing you are being watched may also prevent you from meeting with like-minded people. Whistleblowers and others who expose organizational wrongdoing are less likely to do so if they cannot remain anonymous. As technology has advanced, courts have outlined limits on state behavior.

Health Information

If information is power, protecting that information can help a person negotiate with organizations. For example, health insurers can use negative health information to charge particular individuals higher premiums, or to deny coverage. An individual therefore has an incentive to prevent such information from entering the public domain. Public release of health information can also be awkward or embarrassing to a person's social or professional life.

Financial Information

Financial information is another realm in which personal information empowers its possessor. An individual may not want a financial institution to be aware of a poor credit record from several years ago, and certainly would not want nefarious actors to use the individual's personal information to commit identity theft or financial fraud.

While people have to disclose personal financial information frequently, for example to pay taxes, or to obtain a mortgage, if such information enters the public domain, it is of interest to various actors. Corporations seeking customers, charities seeking donors, and political candidates seeking donations are all interested in knowing an individual's personal financial information. Though these actors are largely benign, people have varying preferences for whom they want to share personal financial information with, and what they want it to be used for.

For example, people may not want their financial information used by companies to determine the maximum amount they would be willing and able to pay for something which is generally available for a lower price. Yet, Orbitz showed the same hotel rooms to Mac users for higher prices than to PC users. This shows that even a little personal information, such as whether a person uses a PC or a Mac, can be useful to marketers in gauging the financial capacity of a person, in a way that most people would find uncomfortable.

Personal Behavior

Studies have shown that people act differently when they know they are being watched. So, at a more fundamental level, privacy enables a person to act in an inspired, intimate, or silly manner, without fear. Just as people intuitively close or lock their front doors, they desire privacy in their interactions with technology. As discussed above, there are many good reasons for organizations to collect personal information (ranging from convenience in using a product or service in the future, to ease of future interaction, to researching consumer preferences to create better products or services). Savvy organizations make efforts not to violate individuals' expectations of personal privacy, because personal privacy is inherently valuable: it allows people to be themselves and act in an uninhibited manner.

Anonymity and Pseudonymity

There is a paradox at the heart of the internet: people expect it to be an open and transparent forum to exchange ideas, information, goods, and services, and yet they also expect to surf the internet anonymously. As a prominent New Yorker cartoon caption put it: on the internet, nobody knows you're a dog. Expectations of privacy on the internet vary by interest group and by country. For example, due to government regulation, South Koreans have lower expectations of internet privacy than Americans. In early 2015, China's government passed new regulations requiring internet users to use their real names when blogging or using social media in the future. The situations in which anonymity and pseudonymity are desirable on the internet are subject to debate. For example, while it would be reasonable for a college student to expect to be anonymous on the internet, the same cannot be said for someone using the internet to plot a violent crime. People have different opinions on whether professors should be allowed to write under a pseudonym.

Though interesting, the debate on when anonymity or pseudonymity should be respected risks becoming moot as new technology poses new and unprecedented challenges to personal privacy.

Social Media and the On-Demand economy require disclosure of personal data

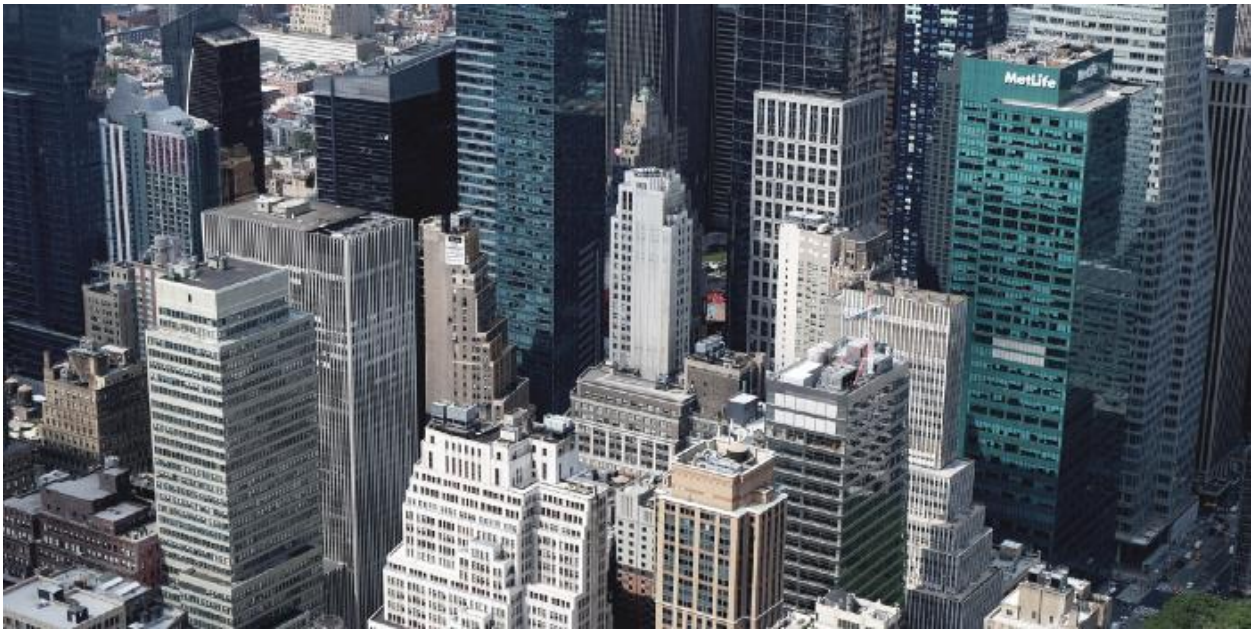
The rise of Facebook, Twitter, and other social networking platforms has changed expectations surrounding internet privacy. People who use these platforms volunteer personal information and agree to share it with either limited audiences or with everyone. However, even people who do not want to share their personal information (for example, those without Facebook or Twitter accounts) can feel pressure to do so for career or marketing purposes. Employers often perform a Google search on candidate employees. While no results are better than bad results, today's job candidates generally use the internet to market themselves, either by creating a LinkedIn account, or showcasing accomplishments through a personal website, blog, or article. The same is true for small businesses: most either have an online presence, or lose business because they do not have one.

Another major technology trend in the past decade has been the emergence of the on-demand economy (briefly called the sharing economy), in which providers and users of goods or services connect through web or phone applications or sites to transact. This has the effect of cutting out established middle players (a process called disintermediation). Just as ride-sharing services like Uber and Lyft have rendered traditional taxi services and city taxi medallion systems nearly obsolete, Wikipedia has replaced large privately edited encyclopedias like Microsoft Encarta. Travelers today check not just hotel prices in other cities, but also Airbnb prices to rent short-term rooms or homes directly from other people. As Airbnb and other companies emblematic of the on-demand economy have emerged, they have addressed customer security needs by requiring hosts and guests to provide personal information. Additionally, after an Airbnb stay, the host and guest are invited to review each other, and these reviews often contain personal information and are freely available to anybody browsing the Airbnb website.

Though companies such as eBay have used identity verification and user reviews to fight fraud and encourage quality in online marketplaces for decades, the new generation of sharing economy apps consider equate personal information with credibility: the more the better. Since participants in on-demand services interact more closely with one another than buyers and sellers on eBay, this makes sense. Getting in a stranger's car, sleeping in a stranger's house, and allowing a stranger to walk your dog require a high degree of trust in the application, site, or platform. Platforms that collect more information engender more trust. For example, while Airbnb guests can build trust through a history of positive host reviews, guests with no prior history may upload government ID, or even link to their Facebook account, to signal credibility. So, while the sharing economy's disintermediation allows people to trust each other, it also often expects them to disclose public information to the platform or even into the public domain.

The personal data individuals provide to social media networks and on-demand economy services can provide a base for organizations or people looking to profile individuals based on attributes such as location, age, gender, consumer preferences, social preferences, and other similar attributes. Personal information empowers its possessor, so individuals should carefully consider the level of personal privacy they are comfortable with in different situations.

Part 2: Organizations



Protecting Organizational Strategy and Proprietary Information

Organizations need to protect sensitive information, such as corporate strategy insights, or proprietary information (such as intellectual property), which could be

used by competitors or nefarious actors to undermine the organizations. This is not just the case for organizations that manufacture cutting-edge technology in their industries (such as those in the defense, aerospace, or automobile industries), but for all kinds of organizations. In 2016, hackers targeted the Democratic National Committee and released its internal e-mail communications, undermining the credibility of several Democratic Party candidates. Also in 2016, hackers posing as Bangladesh central bank officials sent instructions to the New York Federal Reserve in an effort to steal $951 million from the Bangladesh central bank's account at the New York Federal Reserve. They succeeded in siphoning $101 million, most of which international authorities have still not recovered. These headline-grabbing hacks are emblematic of the challenges organizations face in protecting their organizational strategy and proprietary information from competitors and bad actors alike.

Collecting Customer Information for Marketing and Research Purposes

Organizations collect customer information for marketing purposes. Grocery stores sift through location information collected from people's phones to determine how much time they spend in certain aisles. Frequent flyer and other loyalty programs provide perks to people in exchange for their personal information, which can then be used for enhanced promotion of products and services. Both for-profit and not-for-profit organizations build customer or donor profiles that help them make sales and raise funds.

Customer information can also be used to help understand consumer preferences and provide better products and services in the future. Additionally, an organization's collection of customer information often makes it more convenient for a customer to transact with that organization in the future.

In collecting such information, organizations must comply with applicable federal and state law. In the United States, health care companies, financial services companies, and other companies are limited in different ways in the types of customer information they are permitted to collect. Sophisticated organizations are familiar with the legal frameworks governing their industries. As data collection and analysis is increasingly performed by non-human actors, legal and regulatory compliance is growing significantly more difficult.

Protecting Customer Information

For all consumer-facing companies, and perhaps especially for technology companies such as Google, Apple, and Amazon, collecting personal information from consumers helps to provide more personalized service to each consumer. It also creates a responsibility for the companies to safeguard that information. For example, syncing data across a person's Mac, iPhone, and iPad allows for convenient access to information, but also creates an expectation that Apple will take steps to protect this information from outsiders.

Protecting Client Information

For organizations that service other organizations (such as accounting or legal services organizations), protecting client information is similarly crucial to maintain client relationships. Hackers have previously targeted professional service companies in order to get their clients' data, in attempts to circumvent the clients' sophisticated data protection measures. Understanding this risk, major professional services firms have undertaken significant efforts to protect client information.

Current Organizational Measures to Protect Sensitive Information

Organizations have adopted many measures to protect sensitive information: for example, hiring internal and external information security professionals, educating employees on how to protect information, and vetting employees to protect against insider threats. Some organizations that have been targeted or are likely to be targeted have also started using honeypots (fake, company-monitored data rooms purporting to hold sensitive company information, which bait and deceive hackers and help companies understand hackers' motives). These measures are important and necessary, and need to evolve to meet new challenges.

Part 3: Big Data

Organizations collect data that encompasses all kinds of information, such as about a company's products and services, internal processes, market conditions and competitors, supply chains, trends in consumer preferences, individual consumer preferences, and specific interactions between consumers and products, services,

and online portals. The amount of data collected by organizations has been expanding significantly.

Concerns about the expanding quantity of stored data have existed at least for the past century. In April 2014, research organization IDC released a report entitled 'The Digital Universe of Opportunities: Rich Data and the Increasing Value of the Internet of Things', which predicted that "from 2013 to 2020, the digital universe will grow by a factor of 10 — from 4.4 trillion gigabytes to 44 trillion". The present-day expansion of data is powered by increases in computing and data storage capabilities, an increase in sensors, and an increase in connectivity.

Increases in Computing Power and Data Storage Capacity

Over time, we find it easier to store more information because both computing power and storage capacity have increased dramatically in the past decades. Intel co-founder Gordon Moore observed in 1975 that the number of transistors on a chip doubled every two years. This observation, known as Moore's law, accurately described exponential gains in computing power well into the twenty-first century. Similarly, and concurrently, the last few decades have seen exponential growth in data storage capacity, and especially in our ability to store vast quantities of data on ever smaller drives.

Thanks to these increases, it has become possible, cheap, and even convenient to store larger amounts of data. Consequently, organizations have tended to err on the side of storing more data, because the risks of losing data that subsequently turns out to be useful outweigh the benefits of minor cuts in storage costs by saving less data.

The Rise of Cloud Computing

Cloud computing simply means the on-demand use of remote (rather than local) computing power, data storage, applications, or networking. Thanks to cloud computing, organizations can simply rent computing power or storage from cloud providers, and no longer need to store large amounts of data on their own servers, maintain vast computing power, or maintain traditional databases with vendors (though, traditional databases can still be useful for large organizations). Since cloud providers must provide reliable on-demand, scalable solutions, large corporations like Amazon, Microsoft, and Google are the dominant cloud providers.

Cloud computing services for business come in three flavors: Software as a Service (SaaS), in which the cloud provider allows an organization to use its software online (for example, accessing TurboTax online), Platform as a Service (PaaS), in which an organization develops applications for its members to access using the cloud provider's resources (for example, Microsoft Azure), and Infrastructure as a Service (IaaS), in which the cloud provider provides basic infrastructure services for the customer to offer a service on (for example, Netflix using Amazon Web Service infrastructure to allow video streaming). (Individual users may be more familiar with

cloud applications such as iDrive, Google Docs, or Dropbox.) Cloud computing is enabled not only by the advances in computing power and data storage capacity discussed earlier, but also by significant increases in internet access, speed, and reliability. Though cloud computing was adopted partly in response to the difficulties of storing ever-growing amounts of data, its widespread adoption has contributed to the expansion in the amount of data stored.

Increased Sensor Use, Sensor Sophistication, and Connectivity

While traditionally, the internet has consisted of human users interacting with each other and with databases, the internet is increasingly used to connect physical devices to one another. This qualitative and quantitative growth in Machine to Machine (M2M) interactions is expected to result in an omnipresent Internet of Things: a network of smart devices that integrate with one another and perform increasingly complex functions with minimal human intervention.

The Internet of Things does not require radically new infrastructure. Instead, it comes about by embedding existing devices and infrastructure with sensors. For example, when a family air conditioning system uses sensors to determine when people are home, and uses this information to decide temperature to keep each room, it becomes 'smart'. Similarly, when urban energy and water infrastructure is embedded with sensors, smart systems can emerge to monitor use, predict future use, and allocate resources more efficiently. Advanced sensors can improve almost any technology, from a smartphone, to a heart monitor, to a massive farm or factory.

Smart devices require different kinds of sensors depending on their uses. Computers have had cameras and microphones for decades. Now, devices can also be equipped with sensors that measure temperature, motion, distance of other objects, pressure, chemicals, and various other things. Sensors are improving in quality every year, and are also becoming available at lower prices.

While sensors alone can improve a device greatly, communication among devices is necessary for many smart systems. For example, though it would be useful to have your car drive itself with the use of various sensors embedded in the car, it would be even more useful to have all the cars on the road communicating with each other. This would ease traffic flow, and ideally make car travel safer. Similarly, when the Internet of Things is adapted for large scale production or warehousing, it will require excellent communication between devices. Advances in communication technology of all kinds, but especially wireless communication technology, have unlocked potential for Internet of Things technologies.

Smart Devices often collect Personal Data

Before smart devices, you would create little to no data by going on a morning run. Today, if you install a health app on your smartphone and go on the same run, data on the duration of the run, the route you took, the number of steps you took, and your heart rate at various points throughout the run can all be collected and stored

in your phone. Similarly, thirty years ago, an air conditioner installed in your window would not have created much data. Today, a smart home temperature system collects significant amounts of data daily, on temperature and humidity. Once collected, this data could be used not only to keep a home at a desired temperature and save energy, but also to deduce when you are usually at home, or when you are most likely to adjust your temperature settings. The examples of your morning run and your home air conditioning system show that smart devices create more data. They also show that personal data collected for one purpose can be used for many other purposes.

The digital universe is expanding at an exponential rate: in an April 2013 post, Ralph Jacobson published an article on IBM's Consumer Products Industry blog estimating that the world created 2.5 billion gigabytes of data every day. Just as advances in computing power and storage capacity have contributed to an increase in the amount of data collected by organizations, so have the emergence of improved sensor and communications technologies. Sensors measure things, and these measurements are communicated to other devices or servers, collected, and stored as data points.

Artificial Intelligence

Artificial Intelligence emerges from data, as I discussed in a **prior post**.

Most Artificial Intelligence research is funded by Google, Amazon, and Baidu, because data is the food of Artificial Intelligence, and these firms generate massive amounts of data every day. Microsoft acquired LinkedIn not for its platform, but for its data.

Thus far, companies have used Artificial Intelligence to revolutionize finance and manufacturing. Protecting our financial information can sometimes seem like a lost cause, since the government, landlords, banks, credit card companies, and credit rating agencies all collect it (and as the Equifax hack showed, store it poorly).

People often consider their healthcare information to be even more sensitive than their financial information. Artificial Intelligence has been used on healthcare data, but since this data is often dispersed and fragmented due to to privacy concerns, the impact of Artificial Intelligence in healthcare has been somewhat limited. Eventually, however, companies will compile increasingly comprehensive databases with our private health information.

If technology has caused this erosion in privacy, perhaps technology can help solve it.

Part 4: Blockchains

Blockchains with special protocols allowing varying degrees of anonymity, confidentiality, and privacy can enable the protection of healthcare, financial, and other personal data while still allowing this data to be used in Artificial Intelligence applications. For example, a user could have a blockchain with personal health information and only release particular elements of this information (such as vision prescriptions) briefly to product or service providers (such as contact lens manufacturers) for particular purposes.

Though a blockchain is a public ledger, stored in multiple locations, it can enable anonymity and trust, as demonstrated by multiple blockchain-based applications and high-privacy cryptocurrencies already in existence.

Currently, the personal data that third-parties collect is usually stored on centralized databases with a single point of failure. Leaks of this data often go unnoticed and unreported. Once our data is in the hands of an untrusted party, we have no control over how it is used.

The Blockchain Solution

As Bitcoin has shown, cryptography and well-thought-through economic incentives can create a secure way of storing and managing information, including personal information.

Private data on the blockchain is protected by cryptography. I have **discussed elsewhere** how hashing is at the heart of blockchain technology. Below are some ways in which blockchain technology can be used to protect personal data, even while making parts of that data available for processing by algorithms.

Homomorphic Encryption

A new kind of encryption called 'Homomorphic Encryption' allows for computations to be done on encrypted data without first having to decrypt the data. This means the privacy and security of the data can be preserved while computations are performed on it. Only users with the appropriate decryption keys can access the private details of the data or transaction.

Cryptographic techniques such as Zero Knowledge Proofs (ZKPs) and zk-SNARKs already use homomorphic encryption. A popular crypto-protocol called Zcash uses zk-SNARKs to encrypt its data and only gives decryption keys to authorized parties for them to see that data.

State Channels

The blockchain could provide models for non-blockchain solutions, or be part of a hybrid solution to protect privacy.

State channels are blockchain interactions which could occur on the blockchain, but are instead conducted off the blockchain. State channels work through three processes.

Locking: the transaction is locked using a smart contract on the chain.

Interaction: interactions happen off the chain or on a sidechain.

Publishing: after the interactions are complete and the state channel is closed, the smart contract is unlocked and a reference to the transaction is published on the blockchain.

State channels could allow service providers to keep user data private and secure. Transactions could take place off the blockchain with a reference hash of the transaction (revealing no confidential details about the transaction) being saved on the blockchain.

Conclusion

Our private information is currently centralized on the internet and in company databases, hence controlled by a few players. Exponential rates of growth in the creation and collection of data can be expected to continue to erode our privacy. Blockchain-based or blockchain-inspired solutions could help reduce this erosion of privacy, while allowing us to benefit from faster transactions, better service, and more capable Artificial Intelligence algorithms.

Why America Can't Regulate Bitcoin

By Beautyon

Posted March 15th 2018

Dr. Silberman from "Terminator 2", a dead ringer for Mr. Sherman. Both sceptical and WRONG.

Hearings on Bitcoin and its derivatives are being held in the USA on a regular basis, and invariably the expert witnesses fail to properly describe the actual processes going on. If they used the correct language and excluded all analogies, the only possible conclusion would be that **America cannot regulate Bitcoin under its current legal system**. The Constitution guarantees the inalienable rights of American citizens, and therefore Bitcoin is a protected form of publishing. The only way Bitcoin can be made regulable is if the Constitution is changed; and that does not mean adding a new Amendment, it means **removing the First Amendment entirely**. Inevitably the anti-Bitcoin protagonists will face a robust and ultimately successful legal challenge that will remove the possibility of any sort of "BitLicense" or interference from the CTFC, FinCEN or any other agency. It will also remove any possibility of interference at the State level. The consequence of adhering to the basic law of the United States will cause America to become the centre of all Bitcoin business for the entire world.

Let me explain why this is the case.

Some say that Bitcoin is money. Others say that it is not money. It doesn't matter. What does matter are three things; that Bitcoin is, that the Bitcoin network does

what it is meant to do completely reliably, and what the true nature of the Bitcoin network and the messages in it are.

Bitcoin is a distributed ledger system, maintained by a network of peers that monitors and regulates which entries are allocated to what Bitcoin addresses. This is done entirely by transmitting messages that are *text*, between the computers in the network (*known as "nodes"*), where cryptographic procedures are executed on these *messages in text* to verify their authenticity and the identity of the sender and recipient of the message and their position in the public ledger. The messages sent between nodes in the Bitcoin network are human readable, and printable. There is no point in any Bitcoin transaction that Bitcoin ceases to be *text.* It is *all text*, all the time.

Bitcoin can be printed out onto sheets of paper. This output can take different forms, like machine readable QR Codes, or it can be printed out in the letters A to Z, a to z and 0 to 9. This means they can be read by a human being, just like "Huckleberry Finn".

At the time of the creation of the United States of America, the Founding Fathers of that new country in their deep wisdom and distaste for tyranny, haunted by the memory of the absence of a free press in the countries from which they escaped, wrote into the basic law of that then young federation of free states, an explicit and unambiguous freedom, the "Freedom of the Press". This amendment was first because of its central importance to a free society. The First Amendment guarantees that all Americans have the power to exercise their right to publish and distribute anything they like, without restriction or prior restraint.

Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances.

This single line, forever precludes any law that restricts Bitcoin **in any way.**

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 .**

The original print out of the PGP source code.

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. As a binary, the US government ridiculously tries to assert that immaterial software is *a device*, and not *text (software or "binaries" is text that can be run **on** devices).* Clearly the idea that software is a device is patently absurd, but rather than waste money arguing this point in court, printing out PGP removed all doubt that a First Amendment act was taking place.

The printed source code was shipped to another country, perfectly legally and beyond challenge, and then transferred to a machine by OCR (*Optical Character Recognition , a software tool that can turn a printed page into a text file, removing the need for a person to manually type out a printed page*), resulting in a PGP executable that was legally exported from the United States.

The direct analogy to Bitcoin should be vividly clear to you now. PGP and Bitcoin are both:

1. Pieces of software that can be rendered as printed text on paper
2. Software that generates unique blocks of human readable text
3. Designed to generate text that is 100% covered by the First Amendment

The purpose of PGP is to absolutely verify the identity of the sender of a message and ensure that the message was not read or changed in transit. The purpose of Bitcoin is to absolutely verify the ability of the owner a cryptographic key (*which is a block of text*) that can unlock a ledger entry in the global Bitcoin network. Both of these pieces of software are *messaging systems and services* that absolutely fall under the First Amendment in every aspect, from the source code used to generate the software clients that do the message signing to the text the compiled clients generate, send, receive and process.

Bitcoin is **text.** Bitcoin is **speech.** It cannot be regulated in a free country like the USA with guaranteed inalienable rights and a First Amendment that explicitly excludes the act of publishing from government oversight.

Bitcoin and PGP generate messages that are initiated by their users. Each of the messages that are generated by these two pieces of software are unique. The only bodies of law that could possibly be invoked regarding their output and source code are Copyright and Patent law respectively. The Bitcoin source is not copyrighted and the core idea of it is not Patented, and in any case, none of this has anything to do with the nature of Bitcoin messages, or your right to publish.

Typewriters can include Patented methods in their construction, and those Patents have no bearing on your First Amendment right to publish what you create with Patented tools.

Copyright gives the generator of these texts privileges under the law imposing fines on someone copying your message without your permission, but Copyright law has nothing to do with exporting, regulating or imposing a tax *on the messages themselves*, and of course, forbidding the copying of your Bitcoin payment message rather negates the purpose of using Bitcoin.

Taking all of this into account, if any legislator, regulator, three or six letter US agency or other bureaucrat dares to try and regulate Bitcoin, they will be on a hiding to nothing. A legal challenge **will be mounted**, and will **have to be mounted**, because if the State can legislate against a single piece of software that generates messages, a legal precedent will be created allowing the US government to regulate ***all software no matter what it does*** .

Bitcoin's operation is fundamentally no different to what all email, text messaging and internet connected software does; **relay messages.** The only difference is in the software that tracks how the messages of the sender and recipient relate to each other. Email is no different to Bitcoin, save for the fact that a record of the sender and recipient and content of your email is not stored in a public ledger one against the other. We know it's stored in a *private* database, but that's another story. *Wink wink* .

Here is another example of case law proving that this reasoning is correct.

While a graduate student at the University of California at Berkeley, Bernstein completed the development of an encryption equation (an "algorithm") he calls "Snuffle." Bernstein wishes to publish a) the algorithm (b) a mathematical paper describing and explaining the algorithm and (c) the "source code" for a computer program that incorporates the algorithm. Bernstein also wishes to discuss these items at mathematical conferences, college classrooms and other open public meetings. The Arms Export Control Act and the International Traffic in Arms Regulations (the ITAR regulatory scheme) required Bernstein to submit his ideas about cryptography to the government for review, to register as an arms dealer, and to apply for and obtain from the government a license to publish his ideas. Failure to do so would result in severe civil and criminal penalties. Bernstein believes this is a violation of his First Amendment rights and has sued the government. → AND WON

In *Bernstein v. US Department of Justice* it was established that code is speech and is protected by the First Amendment. This absolutely and unambiguously applies to Bitcoin, with eerie parallels to KYC/AML in Bitcoin. The unconstitutional ITAR requirements are exactly the same as asking Bitcoin traders to register as "Money

Transmitters" and seek licenses before they can be paid to transmit text to the Bitcoin network for publication on the public ledger. The Ninth Circuit Court of Appeals found in Bernstein's favour, and ruled that **software *was speech* protected by the First Amendment** and that the government's regulations preventing its publication were unconstitutional. It is clear to see that Bitcoin falls squarely into the category of protected speech, there is no way around any of this, and the US courts must come to the same conclusion for Bitcoin. **Bitcoin is protected speech**, **and the case law says so explicitly**.

The position that Bitcoin is money is fundamentally wrong, and systems like it have existed for many years without gaining the attention of any three letter agencies. Take for example *FarmVille,* the massively popular farm simulation game on Facebook.

> *FarmVille* is available as an Adobe Flash application via the social-networking website Facebook and Microsoft's MSN Games,[9] and was available as an application ("app") for the iPhone, iPod Touch and iPad for a brief period in 2010. The game is free to play; however, to progress quickly within the game, players are encouraged to spend Farm Cash (in FarmVille) or Farm Bucks (in FarmVille 2), which are purchasable with real-world currency, or to "get help from their friends".
>
> After its launch on Facebook in 2009, FarmVille became the most popular game on the site, and held that position for over two years. At its peak in March, 2010, FarmVille had 83.76 million monthly active users. Daily active

From Wikipedia's entry on FarmVille

This hugely popular game is no different to Bitcoin in nature. *FarmBucks* exist in a closed system, just as Bitcoin does. The only difference is the size of the space where the messages are being sent, and in the case of *FarmBucks*, the number of users and transactions (messages sent) was large. FarmVille had 83,760,000 monthly active users and **not a single one** was subjected to KYC/AML to exchange fiat for FarmBucks or FarmCash. Why not? What happened to that money? Why weren't FinCEN or SEC all over that game as they are on ICOs? No one can explain this adequately. This example is very useful as a tool to pull back the curtain on the people who assert that Bitcoin is a money and is **fundamentally** different to a money kept in a game. All the rationales they use (mostly in the form of run on sentences) to explain the difference are inaccurate, and never address the fundamental processes; if they did, they would have no choice but to conclude that Bitcoin is no more subject to regulation than FarmBucks or PGP are.

Clearly, allowing legislation to touch Bitcoin means that any software *of any kind* will suddenly be liable to arbitrary and unconstitutional restriction. It will set a precedent that will be devastating to all software development in the USA, and software is the means by which everything is run, communicated, exchanged and ordered in modern society. In fact, it is impossible to run a modern society without software.

Twitter for example, could find itself being regulated; it transmits messages that are no different in nature to the messages that Bitcoin transmits; the only difference being the publicly maintained ledger and application of the messages. In fact, twitter could turn itself into a Bitcoin company quite easily by adding a few fields to its message JSON schema to include a Bitcoin address for each of its users, adding a page to its client and running its own Bitcoin server pool. Would that extra text suddenly transform Twitter into a bank? Would that suddenly change the nature of each Tweet that is sent on their network, and cause them to be "Money Transmitters"? How is having a Bitcoin address integrated into your Twitter account different to making a promise by hand on Twitter to your followers or in a direct message?

Essentially, Bitcoin allows you to make written contracts with people without knowing them or signing paper; the network and software takes care of identifying and fulfilling the promise, all with cryptographically signed pieces of text. What the people calling for "BitLicenses" are asserting is that because Bitcoin right now has a particular use, it should be exempted from the basic law of the United States of America. That is **completely insane**, and will have unintended consequences that would be **absolutely disastrous** for the American economy since almost everything today is mediated by or touches software.

On the other hand, if Bitcoin is left to flourish and the market allowed to define the services, means of setting the value and resolving disputes, Bitcoin as an ecosystem will be extremely robust and widespread, just like the Internet is today, after having grown for twenty years without any regulation or oversight from the State.

Furthermore, as I have said previously, the country that does not enact Bitcoin legislation will become the starting and endpoints of all Bitcoin transactions globally by first mover advantage. All other jurisdictions will see Bitcoin passing through them untaxed, and there will be nothing they can do about it, as Bitcoin is an unassailable peer to peer network.

We have seen a similar phenomenon with the legal position of encryption in France. SSL was regulated in France until Dominique Strauss-Khan removed the restrictions. They knew that "French e-commerce" would take place inside *"le pays Roosbeef"* if it were not possible to secure French websites with SSL on demand without friction. American Bitcoin businesses (since the endpoints will be in their jurisdiction) will be taxed on their profits, and this will be a percentage of the **trillions** of global transactions made on the network for every conceivable and inconceivable purpose.

The same is true for any other country. The United States looks set to cripple itself by enacting "BitLicenses" and declaring by fiat that Bitcoin is a currency, or a commodity or legal tender. As I describe above, Bitcoin is none of those things by nature, and the myriad number of applications it can be put to is only just being discovered. Our project Azteco is but one of them, with the potential to reach the billions of unbanked people in the world, and provide them with an easy way to access internet e-commerce, world-wide, with a system that makes payment fraud impossible. The potential benefit to the unbanked and the websites that sell goods on-line and the jurisdictions where those websites operate is without precedent. Only a *fool* would do something that could harm the advent of this transformation, or shun this new technology and the business building on it.

No legislature will be able to keep up with the advances in software that are taking place; there are too many developers and efficient tools in the wild all over the world, all with equal access to the market. The best the State can possibly hope for is to tax new businesses that use the new tools as they emerge, and encourage entrepreneurs to incorporate in their jurisdictions. If America wants to drive away Bitcoin developers, exchanges and new businesses, by all means, do so and take the consequences. There are many other places in the world where fast internet pipes have been laid and where the government is not so backward. Skype was founded in Estonia, not Silicon Valley, and this is for a reason. All the big Bitcoin exchanges are outside of the USA. There is a reason for that. No one wanting to start a Bitcoin business is planning to move to New York from anywhere, because they know that their business models will immediately come under attack.

For those of you who are frightened of a free market in Bitcoin, rest assured, all the laws that currently exist to do with fraud, theft, misrepresentation and everything else, continue apply to all people and corporations who use Bitcoin. Bitcoin does not make laws or your personal or corporate obligations moot. When you deal with a company, you retain access to the law and recourse to it. When someone makes a promise to sell you goods with Bitcoin, that promise is not nullified because you are paying with Bitcoin. Good Bitcoin businesses will build dispute resolution systems the way that eBay and Amazon have, so that you never have to go to court to obtain justice if there is a problem. Online, reputation is everything, and bad reputations can destroy your credibility and customer base over night. This is a far more powerful incentive to behave correctly and fulfil promises, which most people do by default in any case, rather than some arbitrary and absurd "BitLicense".

All the "BitLicenses" in the world could not stop MTGox from having a software problem, and no law can bring back the money lost either directly or through the disruption the event caused by the software error. Once again, entrepreneurs powered by the Internet make life easier and better, not laws and regulations. Regulation does not make software correct; developers do.

I have one recommendation for anyone advocating that there should be a "BitLicense". Don't waste everyone's time, money and resources proposing this anti-American idea. The EFF has better things to do with their time than teach the PGP

"Munitions Case" lesson all over again. If it goes to court, your side will lose, and as a consequence, America will lose its head start as all Bitcoin entrepreneurs flee the USA for environments that will allow them to innovate, grow and prosper.

And what can the business people who want a "BitLicense" forced on the software industry say? That they don't trust themselves? That's patently absurd. That they do not trust their competitors? If it's the case that their competitors are not good actors, then the good actors have a market advantage, and remember; a license cannot protect the public from fraud or provide any guarantee of any kind, it can only distort the market.

What these "BitLicense" advocates actually want is *a guaranteed market advantage*. They are **Crony Capitalists**. They want to prevent the emergence of a "Golden BB" entrepreneur that might destroy their business, they want to slow down and stifle innovation, so that they can become the entrenched and unassailable gatekeepers. They want to bar new entrants to the market. It simply will not work. **And it's un-American.** The American legislature must let the American dream flourish and extend its power to Bitcoin, or it will be compelled to obey the law, and this has started to happen. Two judges in the USA have now found that Bitcoin is not money, and have thrown out "Money Laundering" charges against two men:

U.S. Magistrate Judge Hugh B. Scott ruled in a money laundering case in Buffalo, N.Y. that bitcoin is more like a commodity and is not a form of currency, according to a local news report. He recommended the money laundering charge be dropped against the defendant since bitcoin isn't money. In another money laundering case last year, Miami-Dade Circuit Judge Teresa Mary Pooler stated it is very clear, even to someone with limited knowledge in the area, that bitcoin has a long way to go before it is the equivalent of money.

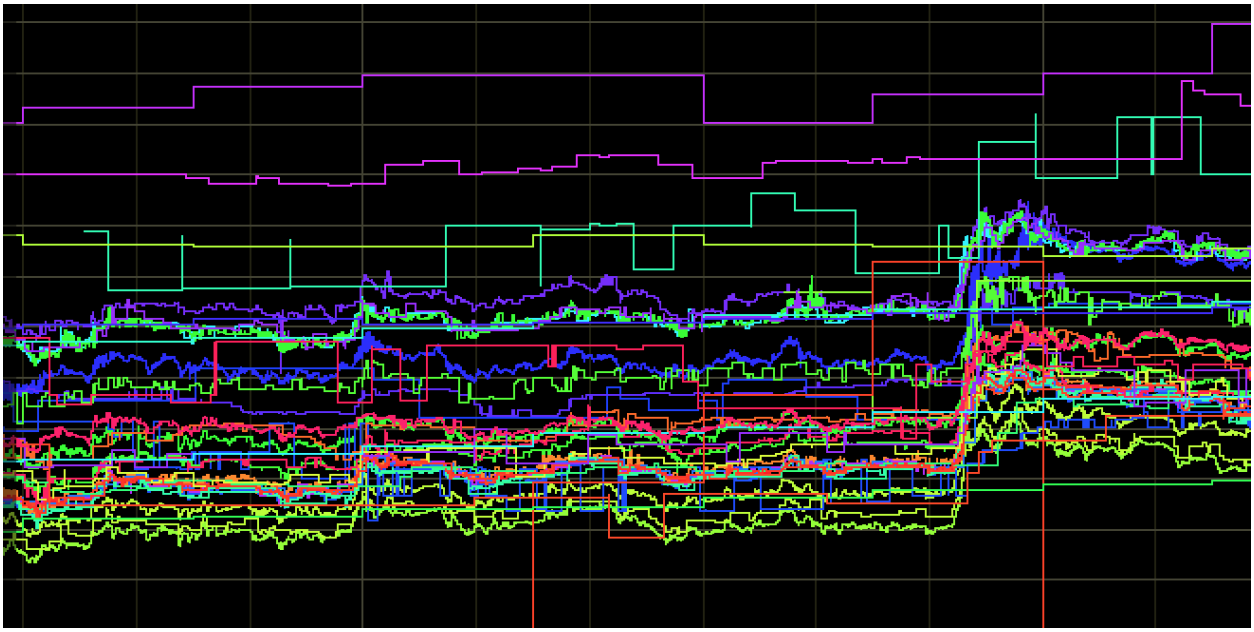
Bitcoin is not money. KYC/AML should not apply to it at all. The Hugh B. Scott ruling is highly significant, because it directly contradicts the idea of BitLicence. And lest there be any doubt, all of this, including legal remedies for breach of promise, applies to "ICOs", which are also nothing more than **text** stored in a database. The fact that they are called, "Initial Coin Offerings" is irrelevant to the underlying processes, and it is not illegal to parrot the language and terms of finance, which are not trademarked or copyrighted. The Hollywood Stock Exchange wasn't deceptive because it called itself a "Stock Exchange". Opponents of Bitcoin and ICOs have no good arguments, and the threadbare pretexts for regulation they're able to synthesize are as flimsy as fiat. If you like the content and feel so obliged to send some love via BTC donations you can do so at the address below:.↴

Are Bitcoin Bubbles Predictable?

By Tobias Huber

Posted March 16th 2018

A Fundamental Valuation of Bitcoin and a Diagnostic for Bitcoin Bubbles



Visualization of the bitcoin price _Spencer Wheatley, Didier Sornette, Tobias A. Huber, Max Reppen, Robert N. Gantner—based on our recently published paper.

Since its release in 2008 by Satoshi Nakamoto, Bitcoin has grown tremendously, and cryptocurrencies have become an emerging asset class. At the end of 2017, the price of bitcoin peaked at almost 20'000 USD, but now sits at around 8'500 USD. The explosive growth and volatility of bitcoin has intensified debates about the cryptocurrency's intrinsic or fundamental value. While many have claimed that bitcoin is a scam and its value will eventually fall to zero, others believe that further enormous growth and adoption await, often comparing it to the market capitalization of stores of value, such as gold. By comparing bitcoin to gold—an analogy that is based on the digital scarcity that is built into the Bitcoin protocol—some market analysts predicted bitcoin prices as a high as 10 million USD per bitcoin. Given bitcoin's wild trajectory, many are wondering where it will go next.

While there is an emerging academic literature on cryptocurrency valuations, which, for example, attributes some technical feature of the Bitcoin protocol, such as the "proof-of-work" system, as bitcoin's source of value, an alternative valuation can be based on its network of users—the more users/nodes it has, the more valuable the

network becomes. In the 1980s, Metcalfe proposed that the value of a network is proportional to the square of the number of nodes. Now, if Metcalfe's law holds here, fundamental valuation of bitcoin may in fact be easier than valuation of equities—which relies on various multiples, such as price-to-earnings, price-to-book, or price-to-cash-flow ratios—and might, therefore, be indicative of bubbles.

Here, we develop a diagnostic for bubbles and crashes in bitcoin that combines Metcalfe's law—which will provide a fundamental value for bitcoin—and the Log-Periodic Power Law Singularity (LPPLS) model, which has been developed to detect bubbles. When both measures coincide, this provides a convincing indication of a bubble and impending correction. For more details, see our paper.

A Fundamental Valuation of Bitcoin

Metcalfe's law states that the value, in this case market capitalization (cap), of a network is proportional to the number of users squared—i.e., relating to the number of connections when all users are connected to each other. To visualize this, Figure 1 shows the bitcoin market cap versus the number of users in logarithmic scales, where a linear relationship with slope 2 would qualify Metcalfe's Law. Fitting by linear regression provides an estimate of 1.7—being significantly smaller than Metcalfe's value of 2. This would mean that, for instance, for 1 million users, a typical user would be connected to "only" 10'000 other users, rather than 1 million.

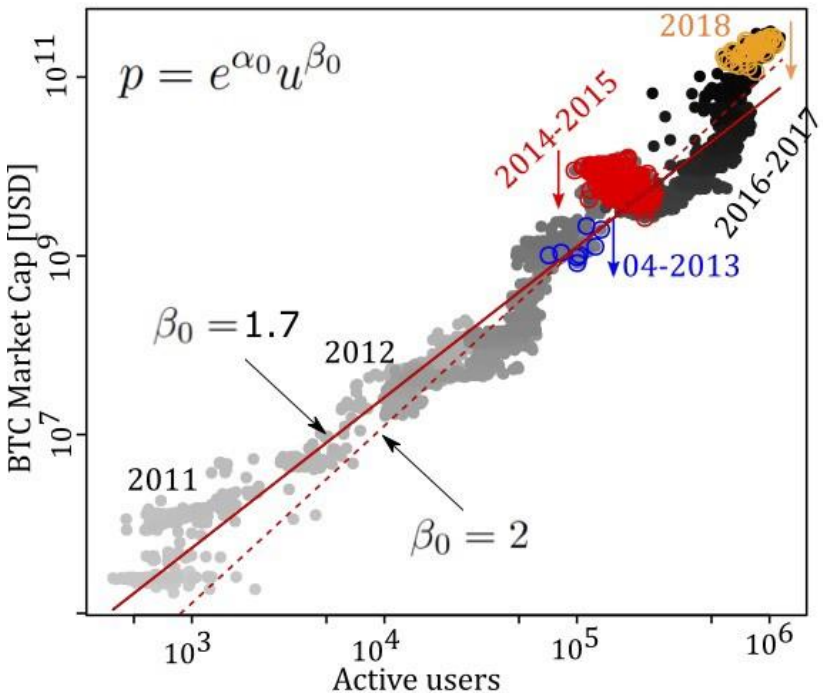


Figure 1: Scatterplot of the bitcoin market cap versus the number of active users, with logarithmic scales

It is however more interesting to directly compare the market cap predicted by Metcalfe's Law with the true market cap, as visualized in Figure 2. In particular, we interpret the blue and orange dashed lines as fundamental support levels, whereas the rough red and green lines, with parameters given by the regression in Figure 1, fall between the fundamental level and bubble levels.

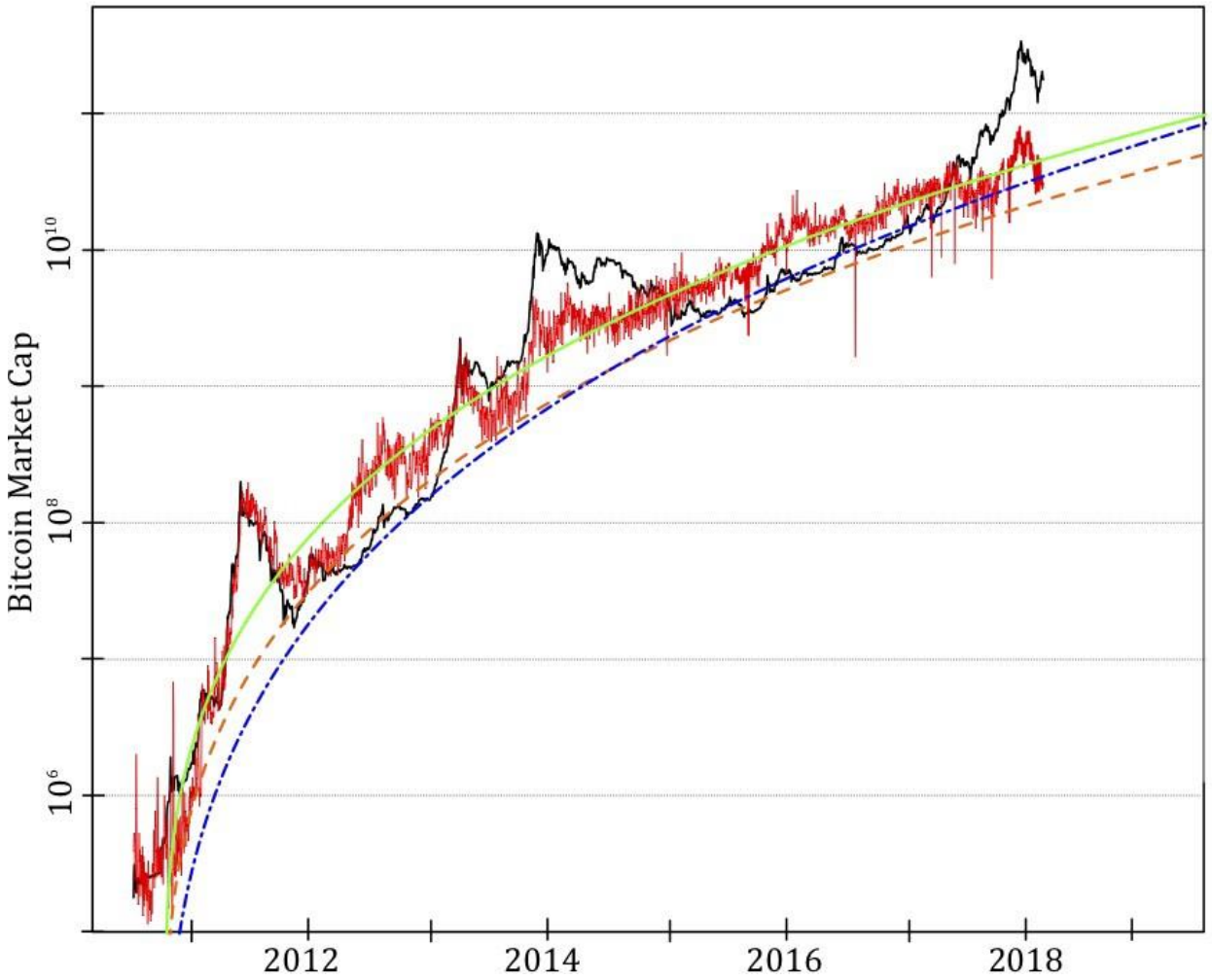


Figure 2: Comparing bitcoin market cap (black line) with predicted market cap based on various generalized Metcalfe regressions of active users.

In any case, the predicted values for the market cap indicate a current (as of the first week of March, 2018) over-valuation of at least four times. Further, assuming continued user growth (whose growth rate is in fact decreasing), the Metcalfe-based predictions for the market cap at the end of 2018 are 77, 39, and 64 billion USD respectively, still well below the current level. On this basis alone, the current market looks similar to that of early 2014, which was followed by a year of sideways and downward movement. In other words, some separate fundamental development would need to exist to justify such high valuation, which we are unaware of.

Bitcoin Bubbles: Universal Unsustainable Growth?

As is well known, bitcoin's history has been punctuated by spectacular bubbles and crashes. We were able to identify four main bubbles, corresponding to massive upward deviations of the market cap from its estimated fundamental value. These four bubbles are highlighted in Figures 3 and 4—in some cases exhibiting a 20 fold increase in less than 6 months! In all cases, the burst of the bubble is attributed to fundamental events: In 2011, for example, the bitcoin exchange Mt. Gox was hacked, which resulted in a 88% decrease in the cryptocurrency's price. In 2013, China banned financial institutions from using bitcoin, which caused bitcoin's market cap to drop by 50%, and two weeks later Mt. Gox shut down. Similarly, in the end of 2017, South Korean regulators threatened to close local cryptocurrency exchanges, which triggered a steep decline in prices. However, the fourth and most recent bubble was much longer, and it is plausible that the triggering factor, which resulted in the bubble's bursting, was bitcoin's all-time high price of 20'000 USD. In other words, bitcoin collapsed under its own weight.

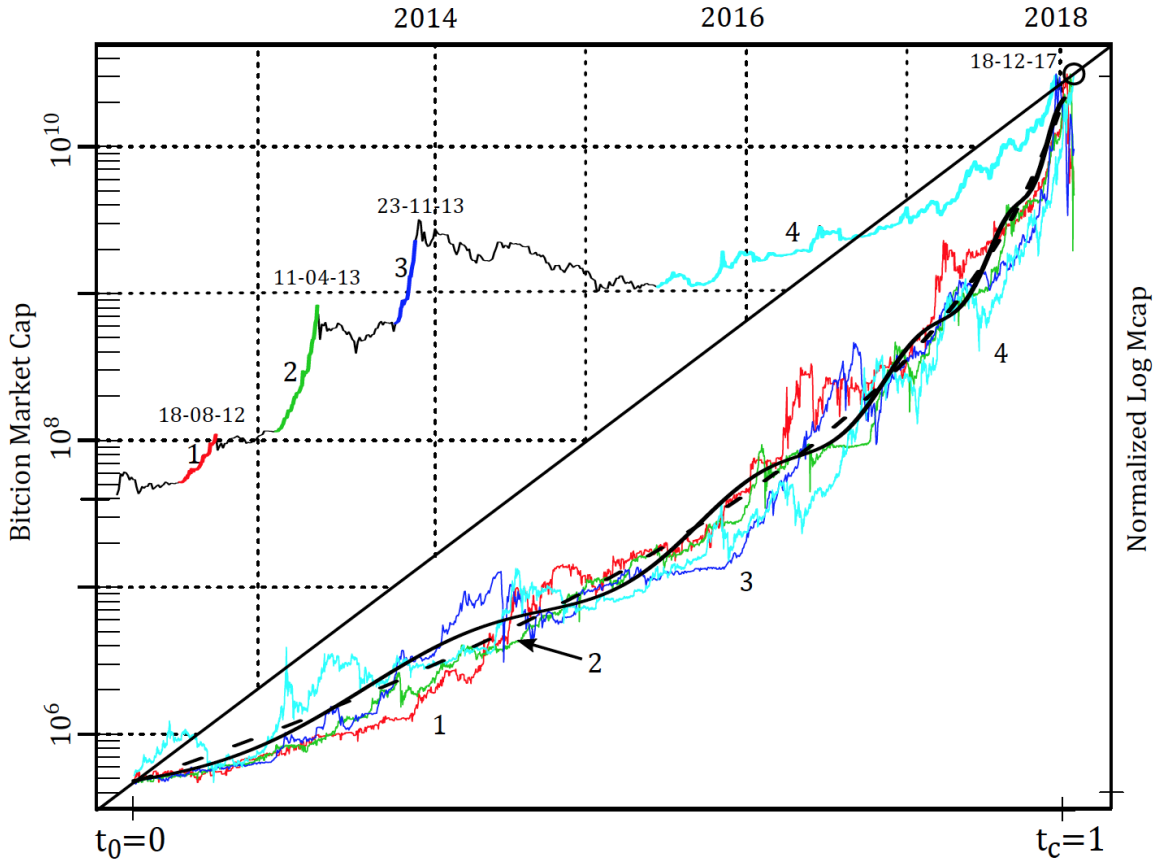


Figure 3: The upper triangle represents the market cap of bitcoin with four major bubbles indicated by bold colored lines, numbered, and with bursting dates given. The lower triangle shows the four bubbles scaled to have same log-height and length with the same color coding, and with pure hyperbolic power law and LPPLS models fitted to the average of the four bubbles, given in dashed and solid black, respectively.

What is interesting is that, although the height and length of these bubbles vary considerably, when scaled to the same log-height, a near-universal super-exponential growth is evident. And in this sense, like a sandpile, once the scaled bubble becomes steep enough (the so-called angle of repose), it will avalanche. In other words, what causes the collapse is the instability of the system itself; the instantaneous cause of collapse is secondary. This key insight is built into the Log-Periodic Power Law Singularity (LPPLS) model, which has been developed by Didier Sornette and collaborators.

In sharp contrast to the deeply entrenched view in finance and economics that financial bubbles can be characterized as unpredictable phenomena, as asset prices are assumed to follow random walks, the LPPLS model captures the radically different insight that financial markets have predictable components. Based on Sornette's hypothesis that the underlying causes of crashes should be identified in the preceding period, the LPPLS model captures the unsustainable super-exponential price acceleration, which means that the growth rate of the price grows itself. As the speculative frenzy intensifies and the bubble matures, the market approaches a critical point, being driven by positive feedbacks in herding and imitation behavior, at which time any small disturbance can trigger a crash.

Formally, the model looks like this:

$$y_i := \ln(p_i) = a + (t_c - t_i)^m \Big(b + c \cos\big(w \ln(t_c - t_i)\big) + d \sin\big(w \ln(t_c - t_i)\big) \Big) + \epsilon_i$$

where *p_i* is the price of the asset, *t_c* corresponds to the bubble, and *ε(t)* is noise. When applied to bitcoin, the LPPLS allows one to detect the signatures of bubbles, which are represented in Figure 3.

Now, given the proposed fundamental value of bitcoin based on the generalized Metcalfe regression presented above, we define the Market-to-Metcalfe value (MMV) ratio as the actual market cap divided by the market cap predicted by the Metcalfe support. As shown in Figure 4, bubbles are persistent deviations of the MMV above support level 1. In our paper, we show that these bubbles are not only well modeled by the LPPLS model, but that the model offered useful advance warning information for the 2017 correction, producing a confidence interval bracketing the true crash time, when back-tested.

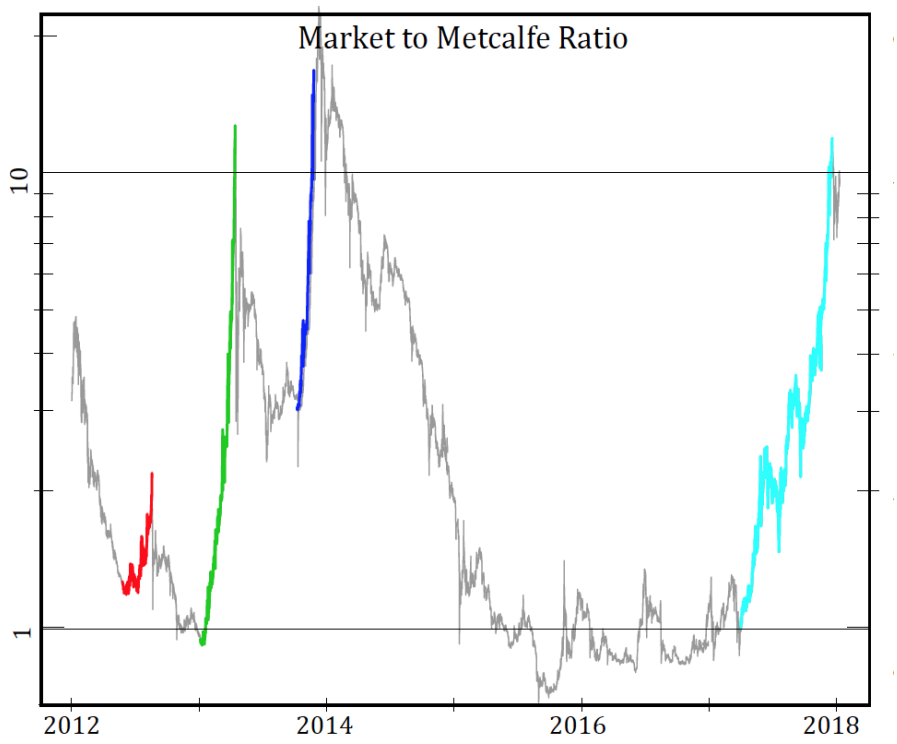


Figure 4: Market-to-Metcalfe value ratio (MMV) over time. The apparent bubbles, which radically depart from the fundamental level 1, are colored.

To sum up, by combining a generalized Metcalfe's law, which provides a fundamental value based on network characteristics, with the Log-Periodic Power law Singularity (LPPLS) model, we were able to develop a rich diagnostic of bubbles and their crashes that have punctuated the cryptocurrency's history. In doing so, we were able to diagnose four distinct bubbles, being periods of high overvaluation and LPPLS-like trajectories, which were followed by crashes or strong corrections. This is in radical contrast to the view that crypto-markets follow a random walk and are essentially unpredictable. Further, in addition to being able to identify bubbles in hindsight, given the consistent LPPLS bubble characteristics and demonstrated advance warning potential, the LPPLS can be used to provide ex-ante predictions. Our Metcalfe-based analysis indicates current support levels for the bitcoin market in the range of 22–44 billion USD, at least three times less than the current level. Given the high correlation of cryptocurrencies, the short-term movements of other cryptocurrencies are likely to be affected by corrections in bitcoin (and vice-versa), regardless of their own relative valuations.

The many traditions of non-governmental money

By Nick Szabo

Posted March 23, 2018

The central bank of the United States, the Federal Reserve, has put out "educational material" on Bitcoin for teachers and students (including a quiz!). The Bitcoin parts are odd enough, but this and a subsequent blog post will focus on the following statement: "traditionally, currency is produced by a nation's government." Is that a fair representation of monetary traditions? At the very least it is quite incomplete. This two-part series will proceed back in time, showing some of the many examples non-governmental money, in order to fill in some of the gaps.

Privately issued IOUs and privately minted coins are covered here in part (i) of the series. These IOUs can more specifically be described as bearer promissory notes, and even more specifically, when issued by banks, bank notes.

The Bitcoin public blockchain implements a global settlement layer ("layer 1" in bitcoin parlance). The closest historical analog to the Bitcoin settlement layer is not to the bank notes, nor even to the coins (despite its name), it is to the monetary metal that for most of monetary history from ancient civilization to the 20th century ultimately underlay the IOUs. This "metal layer" of historical money systems will be covered in part (ii) of this series, as will some even more ancient forms of non-governmental money.

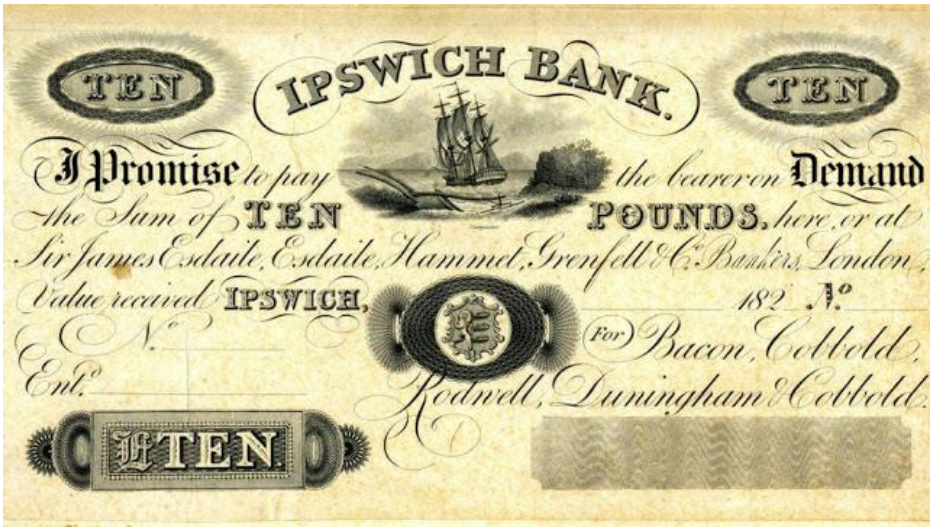
Bank notes

Higher layers of the bitcoin ecosystem, which can include exchanges (centralized or decentralized) as well as more trust-minimized systems such as Lightning, correspond most closely in our rough historical analogies to checking accounts (which, although often counted by economists as part of the money supply, and not created or managed by governments, will be so familiar to most readers that they will not be covered in this series) and to private bank notes. In these higher layer monetary systems, a more computationally (or for bank notes physically) efficient medium is substituted for a less efficient medium (for bank notes, often the underlying metal), usually (as is the case with checking accounts, bank notes, and centralized bitcoin exchanges alike) at the cost of increasing trust and thus vulnerability and risk in the system.

Bank note (bearer promissory instrument) issued by the North of Scotland Bank, 1945. Many banks besides central banks have issued bank notes that circulated as currency. George Selgin and Lawrence White among others have done extensive work in this area. Knowledge of the long history of non-governmental money was one of the inspirations of the original invention of trust-minimized cryptocurrency. This practice continues to this day in Hong Kong and Scotland.

Stockholms Enskilda Bank note, Sweden, 1876. Critics have said that decentralized note issue, following the same principles of fractional reserve and maturity mismatch as central banks, were just as or more prone to runs on the bank. Defenders have argued that competition between note-issuing banks formed a peer-to-peer system where banks could redeem competitors' notes, making it more reliable and robust form of fractional reserve banking than a central bank run or managed fractional reserve.

Hong Kong & Shanghai Banking Corporation (HSBC) bank note, 2009.



Ipswich Bank, a “country” (non-London) bank in England, 1820s (this instance unissued). Traditionally country banks, like the Bank of England, redeemed for specie, i.e. the official coin, which contained a standard weight of monetary metal (usually in this era silver). After 1833, Bank of England notes became legal tender which holders of country bank notes had to accept in lieu of specie.

Bank of Prince Edward Island note, Canada, 1871

Mechanic's Bank note of 1856, Augusta, Georgia. Before our Civil War, most paper money in the United States was privately issued.

Boone County Bank note, Lebanon, Indiana 1858. "During this era the U.S. had no central bank and paper money was issued by a variety of private banks. Some was even issued by manufacturing and retail companies. This money was backed by gold, silver, real estate, stocks, bonds, and a wide variety of other assets. You can no longer cash them in, but they are now worth often substantial sums as

collectibles…the note designs were more varied and creative than modern money, and were remarkably free of politicians' faces."Source

Bank of De Soto note, De Soto, Nebraska, 1863. Critics have called this era of U.S. private bank note issue the "wildcat banking" era. Collectors sometimes call surviving private bank notes "broken bank notes", because notes from banks that were quickly or never redeemed are much more likely to have survived in reasonable to excellent condition.

Hagerstown Bank note, Hagerstown, Missouri, 1850s (this instance unissued). Some other scholars within the Federal Reserve remembered the private note-issuing era in the United States; their central bankers' view of it can be found here.

Jiaozi, a bearer promissory note from the Song Dynasty. The earliest jiaozi were issued in Sichuan province by merchants to relieve their fellow merchants of the high costs of transporting the heavy government-issued iron coins.

Gordon Tullock wrote of bearer promissory notes in an earlier time and different part of China,

By A.D. 700-800 there were shops in China which would accept valuables, and, for a fee, keep them safe. They would honour drafts drawn on the items in deposit, and, as with the goldsmith's shops in Europe, their deposit receipts gradually began to circulate as money. It is not known how rapidly this process developed, but by A.D. 1000 there were apparently a number of firms in China which issued regular printed notes and which had discovered that they could circulate more notes than the amount of valuables they had on deposit. Source

Coins

A brass half-penny issued by grocer Edward Nightingale, probably dating from the early 1670s. [Source] While in most times and places, coinage was a royal or

otherwise political monopoly, there were a number of important exceptions where coins were minted privately and successfully circulated as currency. Per monetary historian Glyn Davies, during the English Commonwealth, Protectorate, and early Restoration occurred "a vast issue by merchants, manufacturers, and municipalities, between 1644 and 1672, of copper tokens, mostly of farthings and halfpence." [Davies p243]

Anglesey & Mines druid half-penny, England, 1788. "From 1787 to 1797, private merchants and industrialists issued 600 tons of custom-made 'commercial' copper coin, which was more copper coin than the Royal Mint had supplied during the previous half century." [Source].

Ironbridge coin, minted by Coalbrookdale Works, Shropshire, England, 1782. In the industrial revolution, factories had to attract workers with frequent pay that could be spent at bargain shops. The Royal Mint was not producing low-denomination coins, so factories minted their own or used the coins minted by another firm. A good review by Jeffrey Hummel of George Selgin's excellent analysis of this era here.

Privately minted coins from Sichuan province, China, 1912. While the minting of private coins, especially imitations of official coins, was often banned in order to secure a royal or other political monopoly, the industrial revolution was not the only time or place where private entities minted. Private coinage was by no means even limited to the Anglosphere. Nevertheless, the vast majority of coins in the numismatic record were minted by or under the license of kings, emperors, elected officials, and other kinds of political leaders, and these are also the kinds of coins prized by political historians as the most durable records of a leaders' reign.

In part (ii) of this series we will explain and give a few examples of the monetary metals themselves, usually mined and processed by private entities. For most of monetary history, from ancient civilization until recent times, the monetary metals were the ultimate "O" in the IOUs – the substances that bearer promissory notes were most often redeemed for – and constituted the most common contents of the coins themselves. The various forms into which monetary metals could be shaped, including coins, were sampled and assayed for their metal content when used outside of the locale where they were issued or covered by legal tender laws.

Part (ii) will also explain why these metals, not any of their particular forms, are the closest analog we have to Bitcoin in monetary history. Finally, we will cover some the many other forms besides coins that these metals could take, the monetary and quasi-monetary functions of these forms, and get some glimpses of even more ancient forms that were the common ancestors of modern money and modern jewelry. Part 2 can only scratch the surface of this vast topic and will refer the reader to more in-depth works including those of this author.

Homo Sapiens, Evolution, Money & Bitcoin

By Alex Svetski

Posted March 28, 2018

How a strange species of ape went from Barter to Bitcoin. An Essay.

Preface

I started writing this damn article about 6mths ago…or maybe longer — I can't even remember now. It's been sitting there with my other 50 unfinished / partly written articles which I keep saying "I'll find the time to finish soon"..

The information here has formed the basis of alot of my arguments in the space, and also the basis of a few talks I've given, including one really rough presentation I held in Australia a few months ago that was recorded (linked at the end).

My aim is to use history, anthropology, communication, evolution and more to explore what money is, what Bitcoin is, how they've evolved, what's different this time & why this innovation is so important.

Although I've picked up information from the thousands of books, videos, essays, articles and blogs I've read over the years, a HUGE thankyou goes to Yuval Noah Harari, Andreas M. Antonopoulos and Naval Ravikant for being big inspirations. I recommend you find out who each of them are..asap.

So now…well…I'm going to actually try & finish it. Or at least make it good enough to release…

In the beginning…there was Bitcoin

Bitcoin & "Blockchain" development commenced roughly 70,000yrs ago—when homo sapiens as a species transcended their biological limits. It's a story that has its roots in the evolution of humanity. Humans have been on the planet for over 2m years.

Homo-Sapiens, as a species of human have only been around for about 150,000.

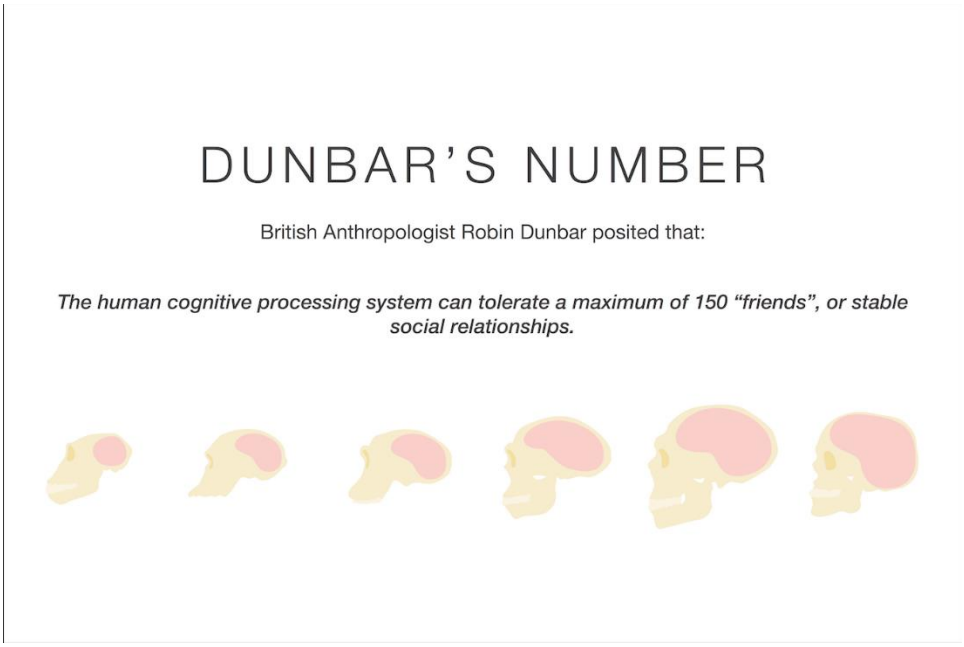
70,000yrs ago, something happened—it's linked to the activation of our prefrontal cortex, the shrinking of our digestive system and a few other things, and although nobody really knows "how" it happened, it resulted in us moving from the middle of the food chain, to the top of the food chain—*very quickly.* And this is where the age of "history" begins, which for humans and the world, changed everything.

But…before we explore what changed, let's get some context.

Dunbar's Number

Robin Dunbar was a British Anthropologist who spent years studying the average social group size and brain function of humans & primates throughout history.

His findings led him to posit that: *The human cognitive processing system can tolerate a maximum of 150 "friends", or stable social relationships.*



This 150 has come to be known as "Dunbar's Number" and has held roughly true over the millennia, across all species of human & primate.

It's considered an evolutionary biological limit that we homo-sapiens still have to this day.

BUT…

It was the ability to cooperate in groups beyond this number that changed everything 70,000yrs ago (the dawn of History)..

How?

Communication

Communication changes everything. But it's not just any form of communication.

Animals, mammals, insects, etc all communicate in their own ways—and as a result build tribes, colonies, packs, etc.

In fact, most are way better at organising & building complex cooperative colonies than humans are (eg; ants)—but—these groupings & their communication is purely *biological.* Homo Sapiens evolved beyond ALL other species (including humans) because we were somehow able to communicate on a higher level, transcending our biological constraints.

There are 2 parts to this; one the foundation, the second; the derivative & key to it all.

Part 1: Complex Language

"Language may have arisen as a "cheap" means of social grooming, allowing early humans to maintain social cohesion efficiently. Without language, Dunbar speculates, humans would have to expend nearly half their time on social grooming, which would have made productive, cooperative effort nearly impossible. Language may have allowed societies to remain cohesive, while reducing the need for physical and social intimacy." Source: Wikipedia: Dunbar's Number Complex language was something unique to the way our brain evolved, (ie; neocortex & prefrontal cortex).

It gave us the time (physically) and space, **cognitively,** to build the second layer:

Part 2: "Shared Fictions"

We are the ONLY species that is able to communicate about, share & relate to things that don't actually exist.

Monkey who just stole a banana…and is on the run…yep…Monkeys can Lie.

They can say there is an eagle in the sky to trick their fellow monkey into running, so he gets all the bananas to himself.

Monkeys can also warn of danger, ie; "there is a Lion at the River".

Only Homo-Sapiens, on the other hand can say: "The Lion is the Spirit ancestor of our people".

Only Homo-Sapiens—who are from different parts of the world, don't know each other, have never met, and have no biological reason to trust each other—can strike up a conversation, build rapport and build trust simply because they are Italian, or Chinese, or some other "fictitious" Nationality.

Only Homo Sapiens can use that same reason to band together & build the Pyramids, or blow each other up "in the name of our country" like we did in WW1, WW2 or any other war for that matter..

Shared fictions are languages in and of themselves, and over the millennia there have been many:

- Caste's
- Races
- Kings
- Gods
- Religions
- Nations
- Laws
- Corporations
- Money

All of these are designed to facilitate cooperation, coordination on a broader level, helping to abstract exchange and allowing for a more complex society to grow and evolve.

One of the earliest "shared fictions" was money, and **it still exists today** because of how fundamentally important it is for society to function.

Money & Communication

Money, at it's very basic level, is a form of communication.

Money is a shared fiction. It's an abstraction that we've all agreed represents value.

The "form" of money has evolved over the years. From spices, to shells, to coins, to gold, to paper, to plastic, and now native digital currencies.

Money is one of the only forms of communication (shared fiction) that has stood the test of time & managed to transcend the borders & barriers all other shared fictions have been restricted by.

Not even religion can come close to the power of money.

Why?

Because of what it represents:

Value & Exchange

At the very foundation of Society and its ability to grow & function is one key ingredient: **VALUE** Furthermore, the ability to *exchange* value is what makes society run.

When we cooperate, we are doing "work", which has some form of "value" and in all our contributions and interactions, we have exchanges of this value. When you extrapolate that out in layers of complexity, you create societies that are able to exceed Dunbar's number by orders of magnitude.

It's also important to note that as a society increases in complexity, value will continue to abstract in order to lower the friction of exchange.

THIS is why money is so important.

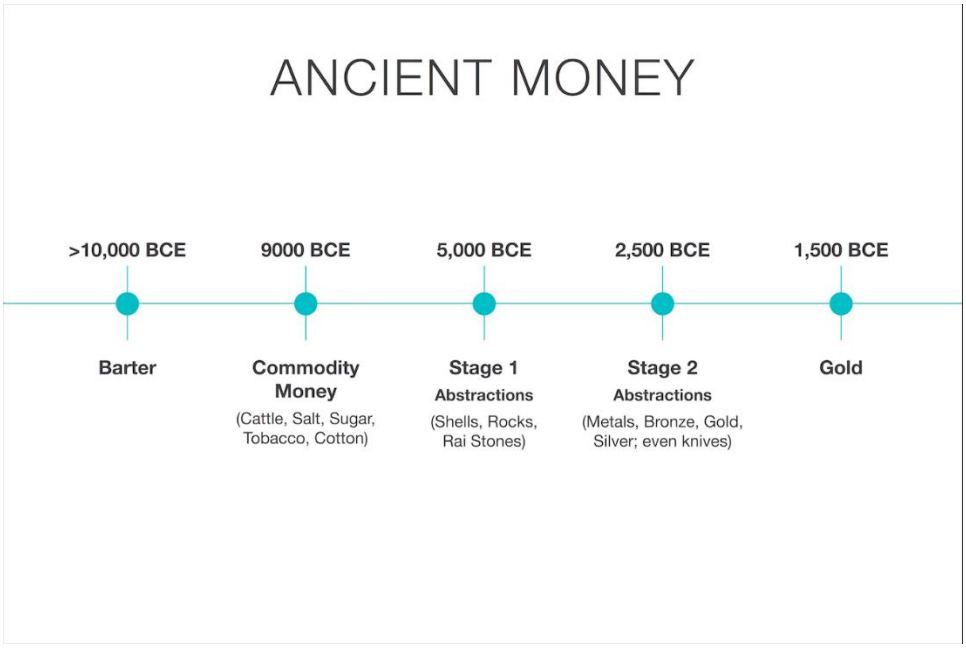
Value is subjective and can come in many forms, but money is an objective tool that gives us an opportunity to represent / quantify it.

Money's Evolution

(Grossly simplified for this essay) Over the centuries, money has come in many, many forms.

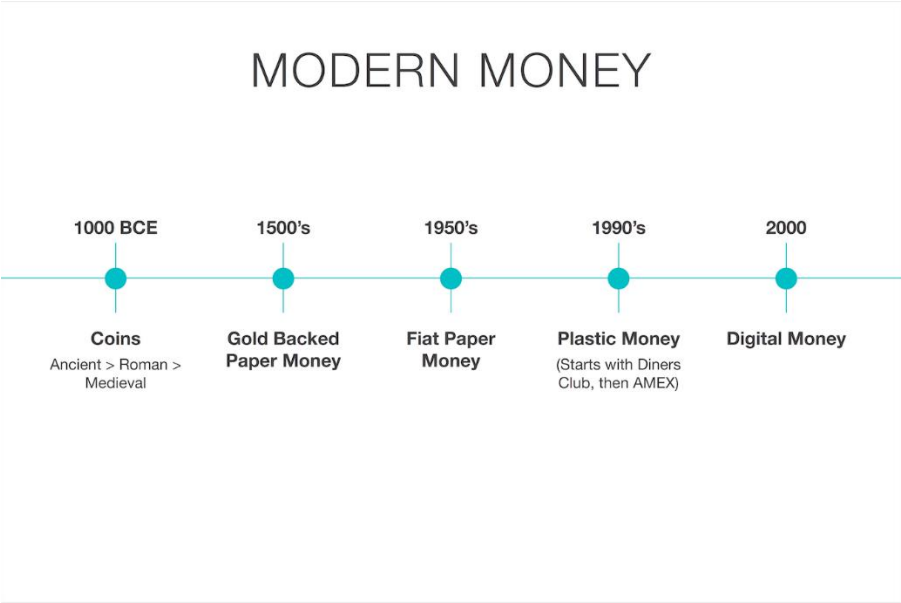
We went from barter, to commodity money like cows & spices, to initial abstractions like shells to better abstractions like metals such as bronze, then silver then gold.

About 3000–5000yrs ago, we entered the period of layer 2 abstractions where "trust" was introduced to help facilitate better transactions & exchange, ie; coins were created with the stamp of approval by an emperor/authority.



This model persisted (in many variants) over the millenia, in & amongst multiple barter, gold, hyper inflationary coinage era's, etc (thankyou, Nero, for one of the first big ones) until the next major abstraction; ie; Paper or Promissory notes.

It was popularised by the Florentine banking families during the renaissance, because it was easier to carry a note that promised the redemption of an amount of gold, than having to carry the gold around.



This was the defining model (in and amongst periods of gold standards, etc) for 500yrs, until the promissory notes transformed into our current era of "fiat currency", ie; a currency that is backed by nothing other than "trust in the state", or "trust in the issuer".

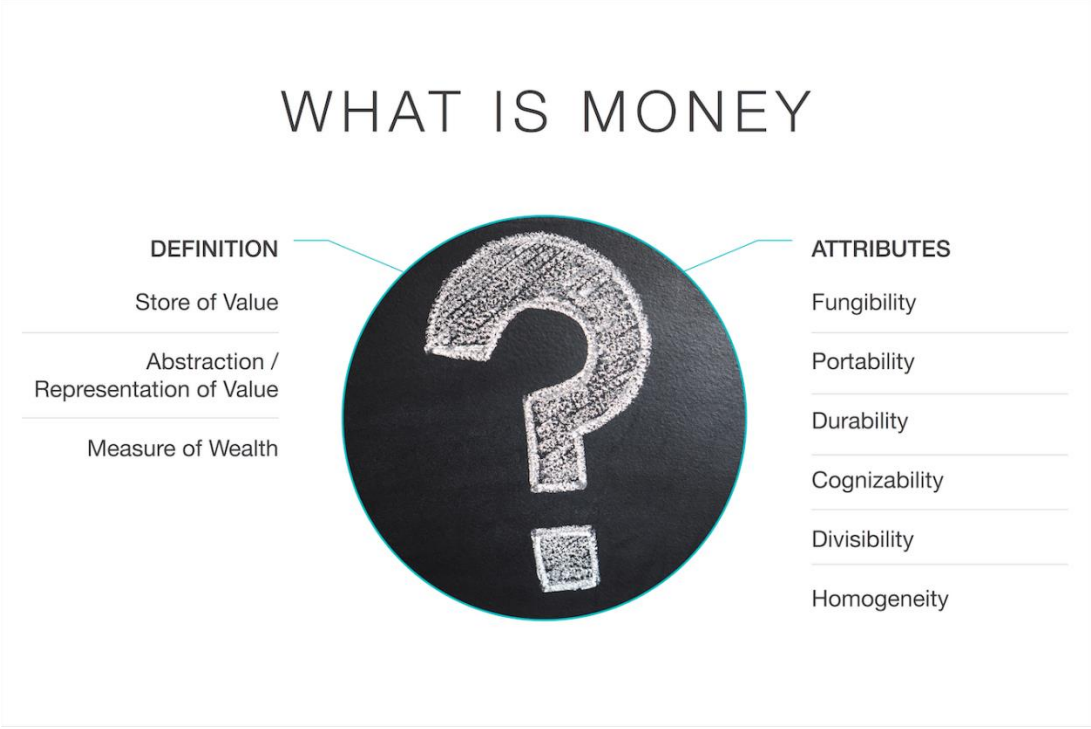
This fiat currency model has had 3 iterations so far:

- Paper
- Plastic
- The Digital Veneer (now)

And it has reigned supreme..until January of 2009—when Satoshi Nakamoto launched Bitcoin. *And the timing…could not have been better.*

Attributes of Money

Before we define the "money we need", lets review the attributes of money.



With each abstraction, we were able to add better attributes to money.

But with each layer of of abstraction, we increased the dependence on trust.

The more attributes we added, the more the pillar of trust was shrouded in power, secrecy & the few. And this is why we need a new for of money.

The Money We NEED?

What's the ideal type of money / value storage for a world that:

- Is becoming increasingly interconnected?
- Is becoming increasingly complex?
- Requires better forms of exchange, that are faster & more transparent?
- Needs a more robust, anti-fragile, trustless form of value abstraction?
- Is moving quickly to one where borders mean less than they used to, and where the language barriers are being broken down to their most fundamental layers?

We need a form of value storage and exchange that is open & decentralised, censorship resistant, can be viewed by the public, on a ledger accessible to all, with a token that is digital, divisible, fungible, fixed & finite in supply.

And that already exists—it's been staring at us since 2009.

Growing up in a Digital World

Each generation has been conditioned to believe "x" is real money.

Gold and Paper backed by "governments" or central banks have been the major incumbents for the last few centuries.

When we first started moving to plastic there was an uproar that this was not "real money".

The same thing happened with building the digital veneer over money, that we use today. But people adapt.

And whilst these continual abstractions have come with advantages & disadvantages, they've pathed the way for truly native digital, global currencies / stores of value / means of exchange to emerge.

For some of us, it still seems like internet funny money, but for the next generation—paper, cash & plastic will seems like useless relics of the past. *Native Digital* currencies are the future, and most importantly those that are decentralised, borderless, global & censorship resistant—because technology is democratising everything else, and we need a form of money to go with it.

A Digital Store of Value

There is a lot of contention around the idea of digital, non government backed currencies—and a big part of that is due to their volatility.

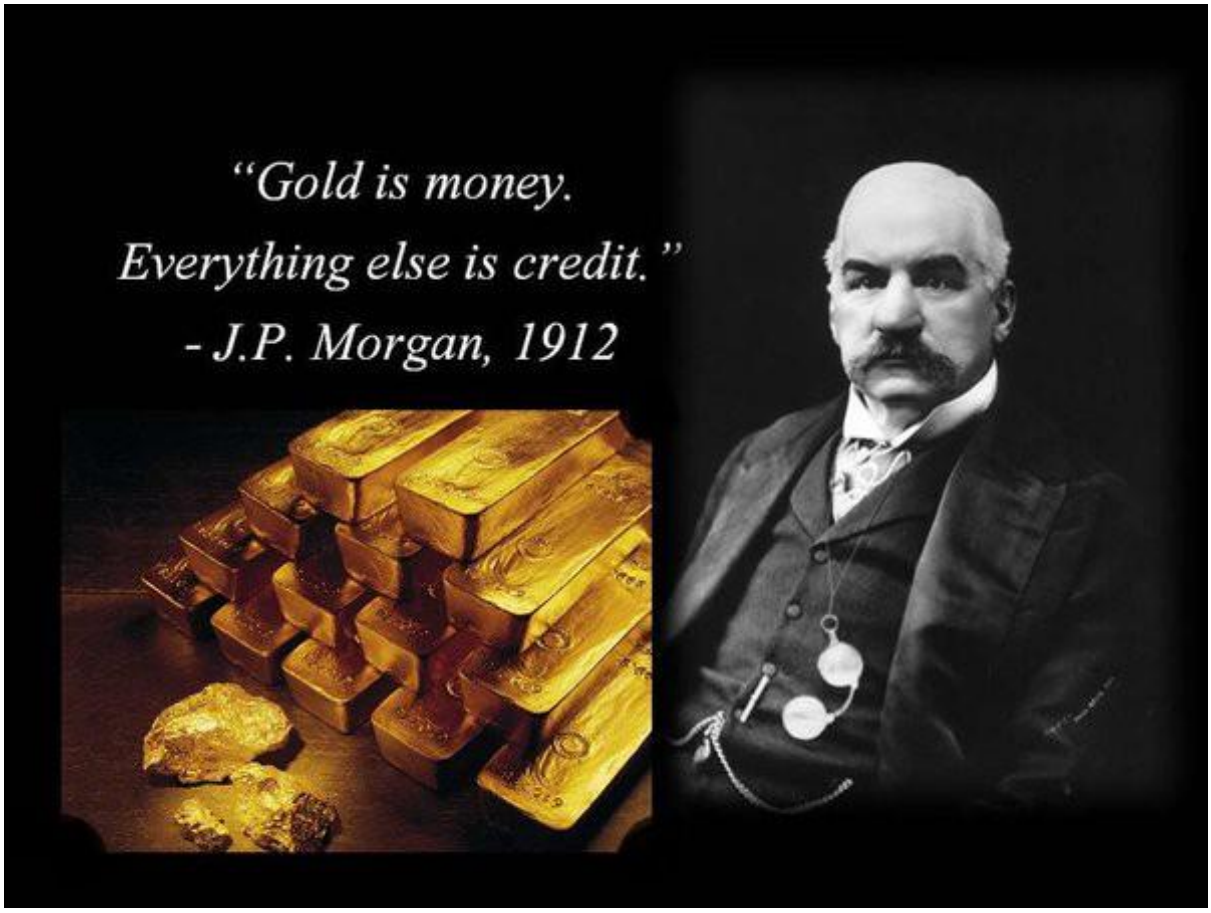
People say that "these can never be currencies" because they're unstable.

And whilst that may be true now, they miss something fundamental: ***Before something can become an exchange of value, it must become a store of value.*** And becoming a store of value takes time—ESPECIALLY when it's something so disruptive to so many stakeholders in so many parts of the world.

We're conditioned to think that because we're living in a technology driven world, and we can innovate at a rapid pace—that this new form of money should somehow too innovate / change / move just as quick. And that's incorrect—because money is more like the internet than an internet company. It's a network that takes time to build (more on this later).

The other argument is that it's not "backed by anything".

Well, the last (and only) real, 'trustless' store of value was Gold. Which is also back by nothing, except that it's real & tangible, which there means it's safe & secure. It also happens to be relativaly fungible, finite (scarce), recognizable, durable and mostly stable, and thus we all agree it has some sort of value.



From the OG Banker himself…Jamie should take a leaf from him.. In fact, it's because it DOESN'T change, that it's valuable.

By the way; it also has a market capitalization (network value) of more than $7T—and more importantly, it took 5000yrs to get there! *Bitcoin has thus far become the default digital store of value, because it is censorship-resistant money, with sovereign-grade protection ; designed to withstand an attack by a large nation-state.* Bitcoin's first and most important use-case will be to become a reserve asset. **Security and censorship resistance are the fundamentals.** Digital currencies already have the rest of the attributes. Over time, as long as the fundamentals hold true, their

adoption will grows, and so too will their network value, thus giving them a real shot at being real mediums of exchange.

It's not an "if"—it's a "when"

Because time *and* history is always on the side of "Networks".

Which brings me to the next point:

Networks

NOBODY has ever successfully predicted the growth of any network that's had a significant impact on society (that may be an exaggeration, but you get my point). The most important & entrenched networks, such as:

- Electricity
- The Telephone
- The Internet
- Facebook
- Money & Value Exchange

Nobody saw any of those coming, nor predicted their growth.

My favourite part of looking back on the growth of each of these networks is reading these quotes:

"The truth is; no online database will replace your daily newspaper, no CD-ROM can take the place of a competent teacher and no computer network will change the way government works." American astronomer and author Clifford Stoll, 1995 *"The Americans have need of the telephone, but we do not. We have plenty of messenger boys."* Sir William Preece, Chief Engineer, British Post Office, 1878.

"This 'telephone' has too many shortcomings to be seriously considered as a means of communication. The device is inherently of no value to us." A memo at Western Union, 1878 (or 1876). *"When the Paris Exhibition [of 1878] closes, electric light will close with it and no more will be heard of it."* Oxford professor; Erasmus Wilson

and one of my favourites:

"The growth of the Internet will slow drastically, as the flaw in 'Metcalfe's law' becomes apparent: most people have nothing to say to each other! By 2005 or so, it will become clear that the Internet's impact on the economy has been no greater than the fax machine's." **Paul Krugman,**winner of the Nobel Prize in Economics, wrote in 1998. The same has been true for Bitcoin, since the early days (see Bitcoin Obituaries for some laughs), or this one I picked up from Wired Magazine: *"Wired, Tired, Expired for 2012: EXPIRED—Bitcoin"* **Complete Air Swings—All Around.** But in their defence, there is a reason why this happens. There's a reason why very very smart people get these predictions very very wrong:

Linear VS Quadratic / Exponential Growth.

The human mind has developed over hundreds of thousands of years to think & perceive linearly.

Out in the Savannah, when you're running from a lion, you need to be aware of how quickly you can outrun it—or you're dead! *Linear thought is a survival mechanism:* 30 steps = 30m.

Another 30 steps = 60m all up. Linear.

Exponential Growth is on the other end of the spectrum. It's a doubling at each step.

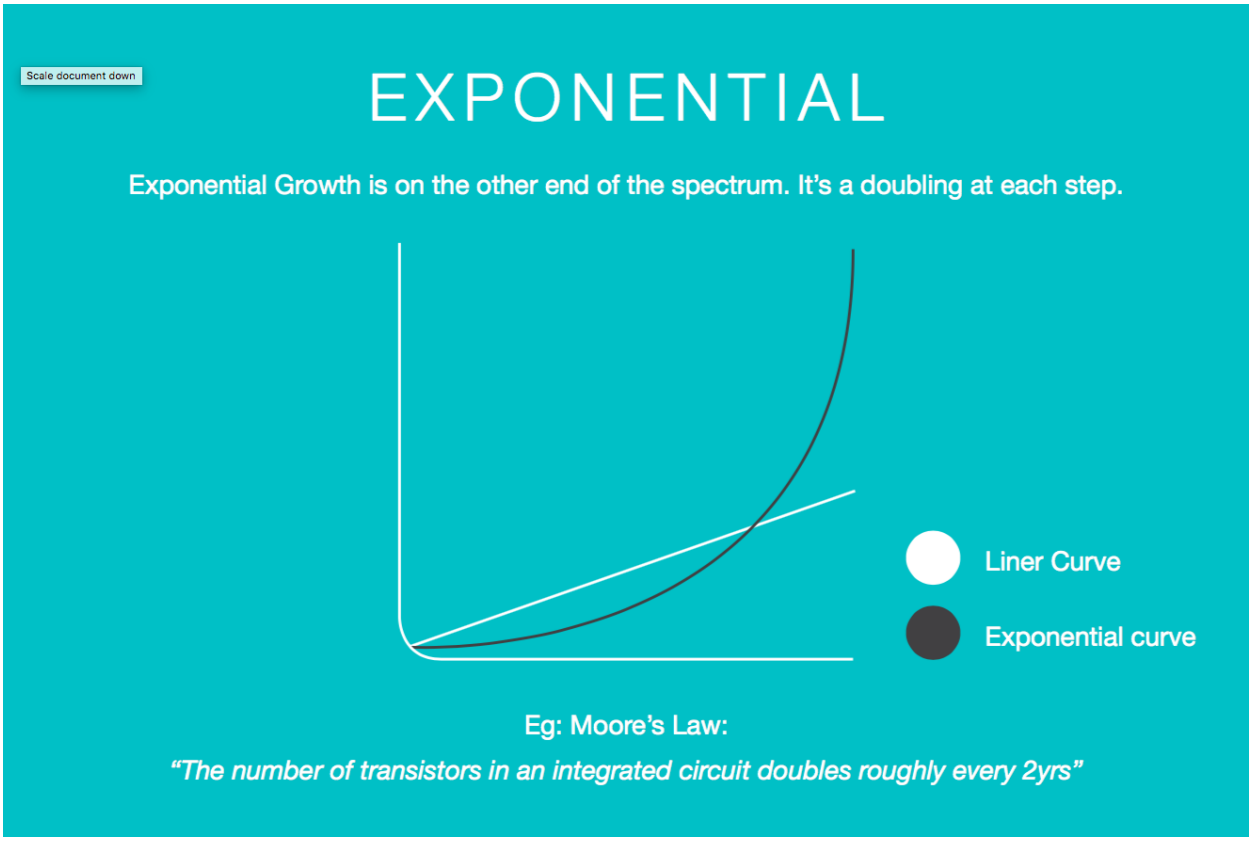
An example we've all heard of is Moore's Law, which states that the number of transistors in an integrated circuit doubles roughly every 2yrs.

Tech has followed this trajectory very closely over the past 70yrs and is a big reason why we've been wrong (as a society) on just about every prediction we've made.

It's non-intuitive growth:

30 linear steps = 30m.

30 exponential steps = 1bn metres!



It's deceptive. We initially over-estimate, and subsequently underestimate. Quadratic growth is not the same, but somewhere in between. It's best described by Metcalfe's law, which states that:

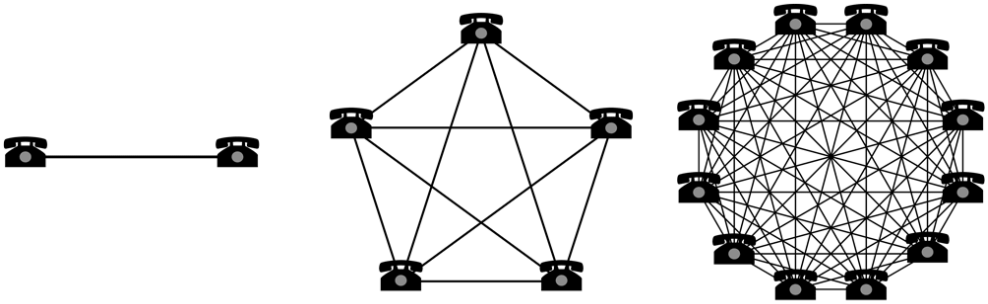
"the number of potential connections in a network is proportional to the square of the number of participants, ie; n2"So if there is 1 person in the network, there is one connection.

10 = 100 connections

100 = 10,000 connections

1000 = 1m connections

1m = 1,000,000,000,000 connections



Simple Representation of Metcalfe's Law.

Neither economists, nor bankers, nor astronomers, nor any of us can really fundamentally grasp this. It's not in our DNA to do so, and to add to that, most of the training in traditional disciplines is built around linear, local concepts—so it further conditions us away from how technology & networks grow.

Now here's an interesting thought:

Bitcoin & real public blockchain networks are a combination of BOTH Quadratic Network Growth & Exponential Technological Expansion.

That only happens once in a while…

In fact, the last time something so big happened was arguably the Internet (although you could probably argue AWS and Facebook are good examples too, I would say the internet is more akin to Bitcoin because they're both more like utilities than companies), and despite hoe much it's changed the world so far, we're just scratching the surface of what's to come.

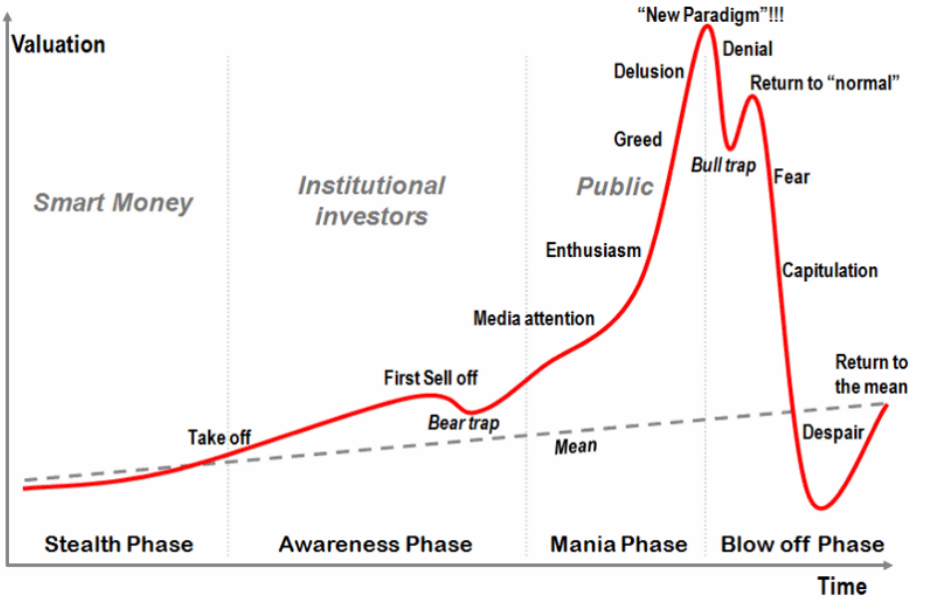
Networks VS Companies

With that basic overview of how Network growth works, let's explore why we're getting valuations completely wrong. *Networks are fundamentally different to companies traditional capital infrastructure models.* The mental models we've developed over the last 100yrs to measure & analyse capital, markets, corporations,

cooperatives & more don't fit with the laws that govern Networks. *Networks are not companies.* They don't have to worry about profit, loss, shareholders, a board, customers or ANY of that.

Think back to the dot com bubble for a moment. Do you remember what happened?

Web companies boomed & busted, but the internet continued to grow. In fact, it accelerated!



Red = Web Companies. Dotted Line = Internet. Same will be true for Crypto & Bitcoin.

The companies built on the internet were affected, but the underlying network (the internet) was not.

We've been trained & conditioned to value things based on profits, earnings, revenues, customers, margins, returns on investment, capital allocation, etc.

Networks are just not subject to the same valuation models & hence we can't predict what their future value will look like.

Networks have *time* on their side. Time is usually against you in the corporate world because you're fighting for market share, fighting for mindshare, fighting the competition, fighting the new startups.

With something like Bitcoin, apart from a catastrophic failure, the fact that new technologies come & go doesn't really mean much.

Bitcoin (as a protocol) is stable. Bitcoin has infrastructure. Bitcoin has security. Bitcoin is the most decentralized thing we have. Bitcoin has no "head of the snake" and is thus the most censorship resistant. Bitcoin is a freak accident with massive Network effects in play and as a global, digital, neutral, censorship resistant store of value is orders of magnitude ahead of anything else.

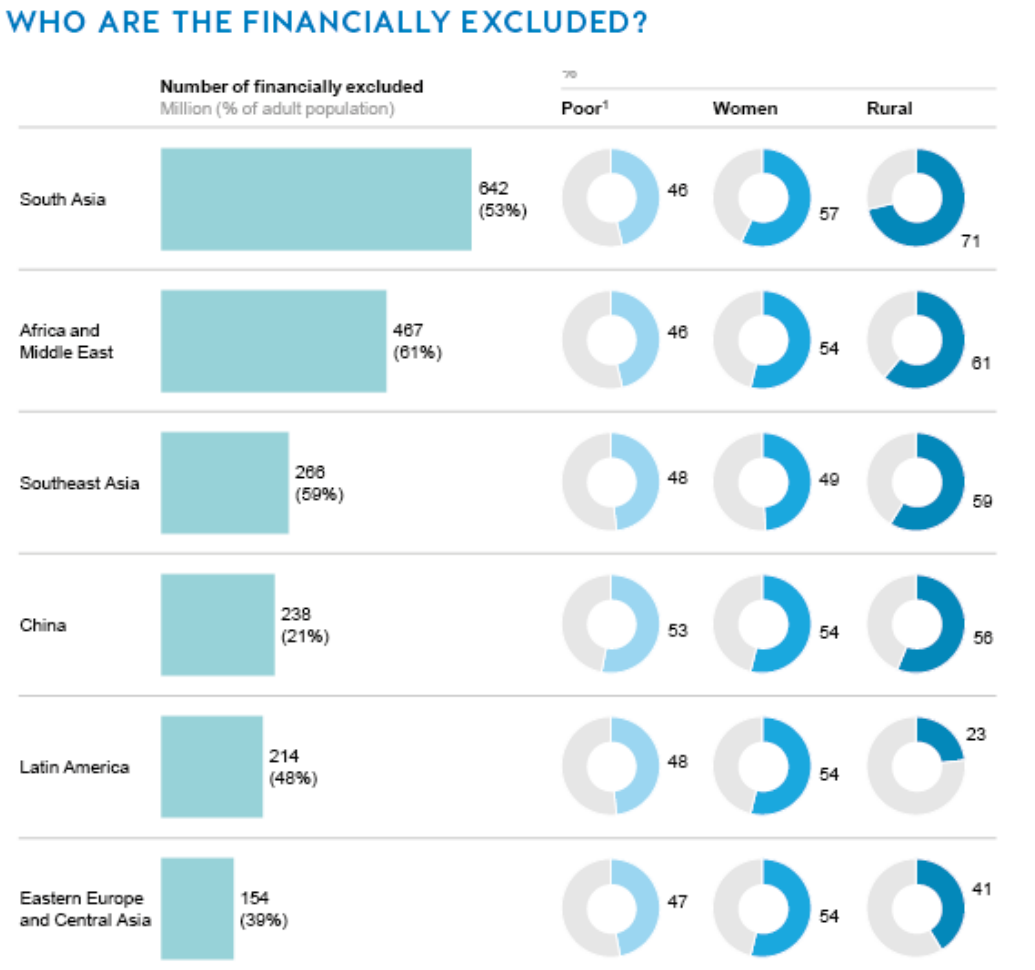
So the question you should be asking when trying to evaluate this space is not; "How good or valuable is the technology today", but;

"How will it evolve over time? Does it have a foundation? and How valuable is a decentralized, digital means of exchange that is scarce, secure, censorship resistant, open, public, transparent & divisible, that allows people all over the world to transact value instantly, freely (cheaply) with anyone at any time"?

It's a very different question, that requires a new framework and a whole new set of mental models in order to measure and evaluate. Chris Burniske is doing some fantastic work in this space, as is Brian Koralewski.

4bn Unbanked or Underbanked

Before I bring this home, I'll outline an example I used at one of my talks. Nope, this is not my version of the creepy "babies are dying" that Roger Ver keeps referring to..



Source: Digital finance for all: Powering inclusive growth in emerging economies, McKinsey, 2016

Combining banked & underbanked, we get to roughly 4bn (or more).

One of Bitcoin's major use cases is banking the unbanked, which if successful will probably result in de-banking the banked. Let's explore: **You may have heard of "The Rising Billion"** That's 1bn people crossing the traditional "poverty" line and entering the global economy.

Exponential Technology is already bringing them the tools they need to participate. Smart Phones, Wireless Internet, etc.

But what about banking & financial services? *Well; the banks cannot & will not service them because banks are companies* They need to make money & there is NO money to be made out there…yet.

Open, public, decentralised protocols (networks) do NOT have that issue.

Bitcoin doesn't care who you are, where you are, how much you have or why you want to use it.

With a phone & internet access the unbanked will have the basic financial services that we in the "developed" world currently take for granted—and in fact, probably better because they won't have to sell their privacy and souls to get access.

By the time banks catch up & try to service these 4bn people, it will already be too late.

Why the hell would anyone subject themselves to the rigor, discrimination & constraints of traditional banking when they've got something so much better?

How do you think the rest of us are going to feel when we're leapfrogged?

How do you think this will impact the world?

What does 1bn people do to the value of a Quadratic Network?

I'll let you do the Math.

Looking Ahead. What comes after Money?

Progressive societies, once they've worked out money, go on to build new governance structures and further layers of communication and exchange.

They begin to ask the question of "how we can run society better"?

And this is where things get interesting.

Where in a world now where a communication & information infrastructure has brought the first wave of massive change, and we're at the dawn of the value transfer & exchange layer atop it.

What happens after that will be transformations in the key pillars of:

Equity, Morals, Liberty, Opportunity, Innovation, Identity, Sovereignty, etc.

We have 2000 digital currencies today, with probably only 5 that will survive long term—because the other 1995, apart from a large proportion being just naive & stupid (or scammy), just don't need their own infrastructure and the ideas they represent are just way too far away. They are simply not required any time soon because money / value needs to be sorted out first, followed by the key pillars listed above.

After all of that's done (which will take many years) we will see layers abstraction on top of those, where millions of applications will be developed that function better in a world operating on a more modern, decentralized form of value exchange, governance, identity, etc.

Note that there will also be a million applications that run better in their current centralized format—not everything with Blockchain at the end of it is better. In fact, much of it is worse!

What the actual fuck….

But, the foundational elements of society, ie; Value Exchange, Governance, Identity are where all of the real innovation will happen in the space.

Our job is to get the base layer right first—all else comes after.

Adoption → Value → Stability

In order for this experiment to succeed, I believe we need to do the following:

1. Increase Adoption, and as a result;
2. Increase the Network Value (Store of Value / Reserve Asset), and as a result;
3. We will see this asset class stabilize, and then, because of it's utility, it will have a chance at being a global, open, public, instant, decentralized form of value exchange (ie; Money).

What's most important now though, is we need to place our effort in (1).

2 and 3 will happen as a result of increasing adoption.

So how do we do that? Simple (but not necessarily easy):

a) Better on-ramps & off-ramps.

We simply need to create better exchanges & better ways for people to get into the space. There is NO better way for someone to learn about this new technology than to actually buy some.

b) Better infrastructure.

This includes wallets, nodes, lightning nodes, tools such as Metamask, etc. Once people are "in" the space, they need to have a better experience. Wallets, for example, have come a long way—but they have a long way yet to go.

c) Education.

All nascent industries that "boom" bring with them the cowboys & snake oil salesman, in droves. You see crap like Bitconnect, USI Tech, Mayweather, Steven Seagal, Ai Blockchains that will solve world hunger & clean your house, dentist coins, and god knows what other horse shit come out of the woodwork and you wonder how any of this is even legal..

Well—most of it isn't—and most of it is short term noise which will all disappear in the next "crypto winter" (overdue, but much needed).

But it's up to us as the people who understand "something" about this space to educate and explain things to the rest of the populace in ways that make sense—which I know is not easy. To this day, after years of studying, there is still no simple 1 liner that explains WTF Bitcoin or Blockchains are without opening up a pandora's box of further questions..But, we're getting there.

In that vein, here is a quick list of people you should follow / subscribe to if you want to learn more:

- Andreas M. Antonopoulos
- Naval Ravikant
- Jimmy Song
- Trace Mayer
- Kyle Samani
- Chris Burniske
- Yannick Roux
- TwoBitIdiot
- Giacomo Zucco
- Saifedean Ammous
- Tuur Demeester
- Nassim Nicholas Taleb

There's more, but this is a quick list off the top of my head.

Closing Thoughts

My hope is that this slightly prolonged article gives the reader a good foundational understanding of why Bitcoin exists, why it's important, why it's probably not going away, and why "history" is now on a different trajectory than it was before.

And maybe that understanding will make you realise what all the hype is about. Because despite the scammy ICO's and stupid money flying around, there actually is some real stuff here worth being excited about.

Last one..I promise…I don't even know if this is real…but FML…

NOTE:

Some might construe me as a "bitcoin maximalist" after reading this article, and…..well that's partially true:

When it comes to money, what I am interested in is the most decentralized, ***censorship resistant*** *store of value and subsequent opportunity for medium of exchange that will form the basis for value measure and transfer in the future.* And currently, based on the research I've done over the years—not just on blockchains, but on societal evolution, the history of money, the history of humanity, etc—Bitcoin stands head and shoulders above the rest as the one with the most viable chance of success.

Bitcoin's value proposition is not digital currency (yet)—90% of existing money already exists as digital currency; Bitcoin's value proposition is its methodology in guaranteeing the trustworthiness of digital currency. I think there is scope for a different set of protocols to be optimised for a different set of use-cases—which in my mind is a good idea, ie; use the best tool for the job. And that will likely happen. Bitcoin should

do SoV + money + reserve asset layer / secure global network and do that best. (It's the most contentious anyway so it's big enough problem to solve as it is).

Lastly, I want to be clear that my aim with the article was to present the conclusions I've come to thus far, based on what I've managed to procure & distill. I'm sure there is more out there and as things progress, so too will my opinion.

Note that this could've gone a hell of alot longer, but seeing as though I have a company to build, I need to go do some work, so: Whether you buy some Bitcoin through the application I'm involved in at www.getamber.io or any other exchange, it doesn't matter.

What matters is that we ADOPT this new technology, and spread the word.

Buy some Bitcoin. Be a user, be a "node" — and the network will grow faster than any of us could've ever imagined.

Thankyou.

Proof-of-Stake & the Wrong Engineering Mindset

By Hugo Nguyen

Posted March 18, 2018

Proof-of-Stake (PoS) is all the rage these days. Ethereum Casper, Cardano Ouroboros, etc. you name it. The rising interest in PoS protocols is probably due to the desire to scale blockchains indefinitely, combined with the mistaken notion that Proof-of-Work (PoW) is somehow "wasteful." (Go here for a detailed discussion on PoW).

A topic not emphasized enough with PoS protocols is their lack of resilience in dealing with worst-case scenarios [1]. For examples: extraordinary events that could knock offline or partition a significant portion of the network, or even the entire network. Or the risk of stolen/purchased private keys.

One might think that these kinds of scenarios are rare or unlikely, but a) they might not necessarily be as rare as you think and b) even something with a 0.1% chance of happening means that it *will* happen in the long run — these are what Nassim Taleb termed Black Swan events.

Simply put, these events are highly unlikely to happen, but when they do happen, the results are often catastrophic. We humans regularly underestimate high-impact, long-tail events. E.g. the illusion that tomorrow is safe simply because it has been safe for the last 10 or 100 years.

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, that millions of people & businesses will rely on.

We must handle Bitcoin software with the same respect we handle nuclear reactor software. In engineering literature, this class of software is known as critical systems. There're three types of critical systems: *safety-critical*, *mission-critical* and *business-critical*. Bitcoin fits the bill for all three (loss of money *can* cause loss of life). There's absolutely no margin for error.

Experienced engineers wouldn't sleep well at night even with the current level of Bitcoin security, which is far from perfect. They know that we're always one step away from a disaster, no matter how sound things are on paper & how smoothly things seem to have gone so far.

There have been many high-profile engineering failures in the past that clearly demonstrate this type of hidden danger. Some examples:

1) Concorde crash (2003)

Concorde (1976–2003) was one of the only two supersonic passenger planes ever existed. The Concorde crash happened as a result of a blown tire hitting the fuel

tank during takeoff, causing a chain reaction. Concorde was once considered one of "the safest planes in the world".

2) Challenger disaster (1986)

NASA initially estimated that the odds of failure was 1 in 100,000. Richard Feynman led the investigation which discovered the cause to be the failure of the O-rings to expand in 32-degree weather. The true odds was closer to 1 in 100. A thousand fold miscalculation!

3) Fukushima meltdown (2011)

Japan is one of the best countries in terms of earthquake technology & earthquake safety.

The Fukushima meltdown happened as a result of what you can call the perfect storm of disasters: a magnitude-9 earthquake, the most powerful ever recorded in Japan, followed by a 15-meter (~50 feet), once-in-a-thousand-year tsunami.

Thinking about worst case scenarios is an absolute must when dealing with critical systems, and even more important when these systems are on the global scale.

Let's examine how PoW & PoS deal with network partition & unexpected outage [2].

Just to drive home the point that this type of scenario is not as far-fetched as one might think: during the Arab Spring movement, the Turkish government successfully performed BGP hijacking to block Twitter traffic from Turkish citizens. China has even more sophisticated tools to block Internet traffic, as part of their Great Firewall.

You can also imagine situations like wars — where countries might try to take out the enemy's communication infrastructure, which would be typically the first target since whoever has better communication gains the upper hand.

So how resilient is a PoW or PoS system under these scenarios? Let's go through some examples.

Scenario 1: The entire network is forced offline for some period. Then reboot.

Since all regions might not reboot and regain contact with each other simultaneously, what you'll likely end up with is several regions starting their own independent chain, from the last common block just before the network went dark, in effect creating multiple chain splits.

When cross-region communication gets re-established, nodes on these independent chains will come into contact with one another.

In PoW, the nodes will automatically self-organize & eventually gravitate towards one single chain: the chain with the most accumulated PoW (and the most secure).

It will be painful, since some chains will get wiped out in the process. But it will work, and the behavior is deterministic.

In PoS, the nodes would have no idea which chain is the more "correct" chain. Unlike PoW, PoS has no objective yardstick to compare the "realness" between 2 chains. Behavior is indeterministic & impossible to automate away without introducing some arbitrary rules that increase the attack surface. The split might become permanent, as some PoS protocols make it impossible to go back too far into the past.

PoS protocol designers often go to great lengths to "punish" misbehaving actors. What they don't consider is the possibility that all nodes act honestly, but there's a chain split nonetheless!

Scenario 2: Some portions of the network get partitioned from the main network.

It turns out that this scenario results in a similar outcome to what we saw in scenario 1. Partitions will continue to run as if everything is operational- except that the number of "active" staking nodes in each isolated partition is smaller. When the partitions regain contact with the main network, confusion will ensue. Nodes have no idea which chain is the canonical chain.

One crucial difference between scenario 1 and scenario 2 is that the likelihood of scenario 2 happening is even higher. Redirecting traffic is easier than shutting down traffic wholesale- we already saw it being done. Partitions can be as small as a small town's network. We can imagine something like that happening once every few years or even more frequently.

Scenario 3: PoS also fares worse in other worst case scenarios such as stolen private keys.

Wealth distributions often follow power laws, and there's no reason to think cryptocurrencies are any exception. The "1% of crypto", which could be just a handful of people, might very well control a significant portion or the majority of the total coin supply.

These richest PoS stake holders' private keys might get stolen as a result of sophisticated social engineering attacks (kidnapping, torture, extortion, etc.). By stealing keys instead of renting or buying coins on the open market, the attacker avoids raising the currency value during the attack. Strangely, when considering this attack vector, PoS protocol designers often assume that buying coins on the open market is the only way to get majority control, and thereby incorrectly conclude that the cost of attacking a PoS currency is merely determined by its market value. Stealing private keys sidesteps that "defense" altogether & significantly reduce the cost of attack.

(A variant of this attack is to purchase old keys from past large stake holders who no longer have an interest in the currency).

In PoW, this is equivalent to gaining control over the majority hash rate.

What can someone with majority hash rate do in PoW? He can try to double-spend or rewrite history. But to double-spend, he has to spend a lot of money. Gaining majority control is only the first step. As bad as it sounds, even under this scenario, the protocol still functions as expected & only one chain can be considered valid (although SPV nodes might get confused- hence the reason running full nodes is often encouraged). To rewrite history costs an even more insane amount of money, so the risk of losing user balance is low. Users could choose to wait out the storm or take action to change the PoW algorithm.

All in all, it's a pretty ugly situation. But we can see that gaining majority hash rate in PoW doesn't grant the attacker unlimited power. You have to gain majority control AND spend money to carry out an attack. We can think of this as a *two-layer defense*. When there's an attack, the behavior is deterministic & there's no confusion about which chain is valid. This resilience in hostile situations is under-appreciated.

In contrast, gaining majority stake in PoS grants you unlimited power. You can double-spend without spending any extra money unlike in PoW. You can also either a) rewrite history, if the protocol doesn't have checkpoints or b) cause irreconcilable chain splits, if the protocol has checkpoints (e.g. Casper). Changing PoS algorithm doesn't help as there's virtually no switching cost, unlike investment in hardware.

To sum it up, what PoW gives you are two benefits, when it comes to security guarantees:

1. *PoW protects the future*: When there's a chain split, it gives us an objective mechanism, automatable way of resolving conflicts, without requiring manual human intervention or trusted third parties.
2. *PoW protects the past*: Getting control of majority hash rate still costs an attacker an enormous amount of time & money to rewrite history, so the balances are somewhat safe.

PoS offers neither of these things. PoS proponents might claim that checkpoints alleviate problem #2, but in reality checkpoints just shift the problem from one area to another. Checkpoints is a centralized solution that opens up another can of worms [3].

*(*For a more in-depth discussion of "private keys attacks", check out Part 2 .)*

In conclusion, it's very important to have the right mindset when it comes to Bitcoin & blockchain protocol development. They are critical systems that deserve the highest level of engineering.

PoS protocols are built on faulty & naive assumptions that rapidly break down under worst-case scenarios. PoS is a step in the wrong direction: lowering the bar of quality, instead of raising it.

Part 2 : Proof-of-Stake, Private Keys Attacks and Unforgeable Costliness the Unsung Hero .

[1]: Some prior analysis of PoS: Andrew Poelstra, 'On Stake & Consensus' https://download.wpsoftware.net/bitcoin/pos.pdf

[2]: Network partition is an important area of research. Check out Ethan Heilman's work in this area: https://eprint.iacr.org/2015/263.pdf

[3]: Checkpoints could be implemented in a decentralized manner, but they will cause problems that will require centralized solutions down the line. So in effect, checkpointing is centralizing.

Maduro's Mint of King Cnut

By Beautyon

Posted March 19, 2018

O GREAT MADURO, BY THE POWER OF YOUR TREASURY, YOU CAN BEAT BITCOIN! News is just in that the Venezuelan government's own "Blockchain not Bitcoin" attempt to ride the Bitcoin wave has just been sanctioned by the White house of President Donald John Trump. This is extraordinary in several ways, and allows a general principle to be explored.

First off, the Venezuelan government doesn't understand how Bitcoin (or economics) works. That is clear. They've made the common error of believing what computer illiterates in well regarded newspapers mistakenly repeat verbatim about Bitcoin; that you can have "Blockchain without Bitcoin". And this is only the first of their many errors in this project.

Even if their technical and economic assumptions were correct, there is no way that their private money system can beat the market. And now President Donald John Trump has forbade by executive order, its use in America, making it even less fungible as everyone will be terrified of touching it.

Executive Order on Taking Additional Steps to Address the Situation in Venezuela

> Section 1. (a) All transactions related to, provision of financing for, and other dealings in, by a United States person or within the United States, any digital currency, digital coin, or digital token, that was issued by, for, or on behalf of the Government of Venezuela on or after January 9, 2018, are prohibited as of the effective date of this order.

Trump Prohibits U.S. Purchases of Venezuelan Cryptocurrency _President Donald Trump banned U.S. purchases of a cryptocurrency the Venezuelan government is rolling out, as part of a…_www.bloomberg.com

Venezuela should at a minimum, settle on Bitcoin as the civilized global standard. These people have made the fundamental error of thinking that they can beat the market. It is the same error the Americans made thinking that everyone would use CDMA instead of GSM.

What if cross chain atomic swaps happen with Venezuela's Petro as one half? Will alts and Bitcoin traded for it be tainted?

> Sec. 2. (a) Any transaction that evades or avoids, has the purpose of evading or avoiding, causes a violation of, or attempts to violate any of the prohibitions set forth in this order is prohibited.

Any transaction must include (presumably) cross chain atomic swaps. The real answer to stopping Maduro is to let the market exanguinate Venezuela; that means getting Bitcoin into the hands of the people on a mass scale.

This new money will never be international. No one will trust a system that requires advance permission from and which is controlled by a Socialist government to use it, that can exclude any actor based on arbitrary rules of a hostile government when Bitcoin is available. There is no logical reason to trust anyone when Bitcoin exists; any system that is tainted by the requirement of trust, or the backing of a government **is inherently inferior to Bitcoin**, and will make rational actors choose Bitcoin over those other, broken systems every time.

There are other problems with this new project, some of which will be of grave concern. With a software simulation of money, backing in this case a commodity (oil), **the company providing the service is the mint**, with absolute control over that money and its operation, **not the government mint or bureaucracy**. In order to *be* the mint, you must directly control the levers of the machinery, you cannot outsource that control to others, and *certainly never to others from a **foreign country or foreign authored software***; these foreigners de facto control everything if no one in the mint can understand how anything works. They seem to have forgotten what the word "Sovereign" means.

If you're going to outsource the creation of a new e-money to back a national commodity, and cede control over its development to foreigners, why not go all the way and give it to the global experts: **Bitcoin Core?** You get all the benefits of the hundreds of developers working on Bitcoin, and access to the global Bitcoin network, its first mover advantage, huge ecosystem and its network effects. You are already willing to give up control, so you may as well give it up for *something* and not for *nothing*.

Computer Illiteracy

This is another example of the global Computer Literacy Crisis, where the apparatchiks don't understand how anything works, and are rendered helpless, delegating all responsibility to software developers who are now one of the top global powers on Earth as a class. We saw this with government departments around the globe accepting Microsoft Windows as "the standard" for decades, with the late realization that this gives control (and back-door NSA espionage access) to a foreign company. Much better to use Linux and Open Office that belongs to no one, is transparent and infinitely more secure and controllable. Just like Bitcoin.

For 7 years I've been talking about the book "Good Money" by George Selgin.

Good Money: Birmingham Button Makers, the Royal Mint, and the Beginnings of Modern Coinage, 1775… _Edit description_www.amazon.com

If you are interested in Bitcoin and why "Private Blockchain" (like Maduro's "Petro" coin) are junk, you should read this book. What is fascinating about this news of a sovereign mint creating a system like this is that the private money vs State money is turned on its head in the Bitcoin era.

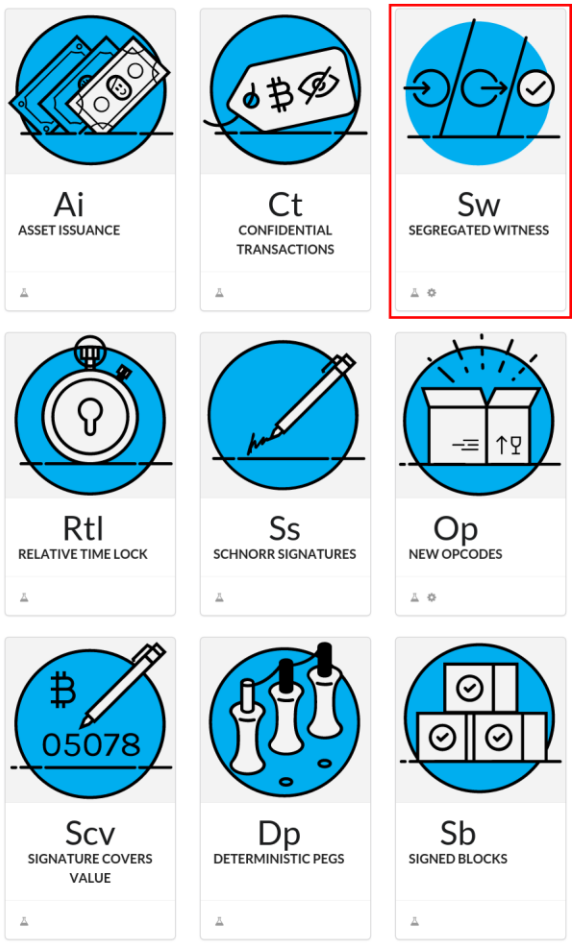
In the 1700s button makers switched to minting coins for private use, because the Royal Mint couldn't supply the demand for small change. Now, government mints are turning to bespoke "Blockchain not Bitcoin Tokens" while Bitcoin becomes the sovereign money of the world. The picture is entirely reversed; the state is minting private money to fill an (imaginary) need while Bitcoin is the money everyone uses but has trouble getting a hold of. Azteco is a service that aims to solve *that* problem.

Unlike many projects with no hope of traction because they are fundamentally flawed, this new platform has failed to put its software up on GitHub, which means no one can inspect the software to see if it is sound. The number of developers with the skill to hack cryptocurrencies in C is extremely small, and all of them are working on Bitcoin. There is no way you are going to persuade these ethical men to stop working on Bitcoin and to devote that time to a bogus "permissioned ledger" State OilCoin project run by a madman.

Our submission to the British Government's "Digital currencies: Call for Information" _We made the following submission to the British Government's "Digital currencies: Call for Information". There is at…_medium.com

Bitcoin devs simply aren't going to split their limited time between projects like Corda, the Petro or any anti-Bitcoin project. And of course, Corda has conceded defeat and given up on "making blockchains programmable " an other fanciful hand-waving nonsense.

Every year States like Venezuela waste time on vanity projects they can't even understand, Bitcoin grows, spreads and strengthens. The number of new, fundamental features coming to Bitcoin is not matched by any other project, and how these will synergise is anyone's guess. Schnorr signatures are one example of space savings and efficiency that will impact all users.



From The Elements Project, new features coming to Bitcoin https://elementsproject.org/elements/ SegWit will activate, on Litecoin first and then Bitcoin. Then everything will change.

Every software project has a use case. The developers are eager to make their case so they can gain users. When they won't make the case clearly, something is very wrong. There is no use case for a sovereign nation to launch its own alt coin that is inferior to Bitcoin. It's like launching a new mobile phone network standard; no manufacturer is going to incorporate another set of protocols, chips, transceiver and antennae into its phone to accommodate you, and yet, this is exactly what these people believe they can do

with Bitcoin. All rational nation State actors are now running to embrace and profit from the inevitable domination by Bitcoin and not betting against it.

We can be sure of this. No "permissioned", "Blockchain", alt-coin reality denying project launched by a Nation State that has outsourced development of its software to a private company in a foreign land can **ever hope** to outperform Bitcoin on any level. Incredibly, the lessons of the doomed and fundamentally flawed Canadian "Mint Chip " have not been learned yet. This is a good thing, believe it or not. The longer Bitcoin's enemies think they can reinvent the wheel and beat Bitcoin, the better it is for Bitcoin. By the time they figure all of this out, it will be too late. In fact, it already is too late.

Disclaimer:

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 the operator of the journal, that means any business I am associated with. Bitcoin, shitcoins, and related technologies can be volatile. Don't buy what you can't afford to lose and please do your own research.

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.

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.

Share this journal early and often. Engage the authors and tell them what you think. We sharpen our position through discourse and debate.

DYOR | BTFD | HODL

Thanks for your attention and support. I appreciate your feedback and hope you enjoy this publication.

- @_joerodgers