CRYPTO WORDS

CY19 June

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

Updates to this Journal

9-20-2019 The following items were added to the journal:

- Statechains: Non-custodial Off-chain Bitcoin Transfer
- The Political Theology of Crypto
- The Sovereign, the Subject, and Crypto-power

Satoshi's Rebuttal of Modern Monetary Theory

By Jack Purdy

Posted June 3, 2019

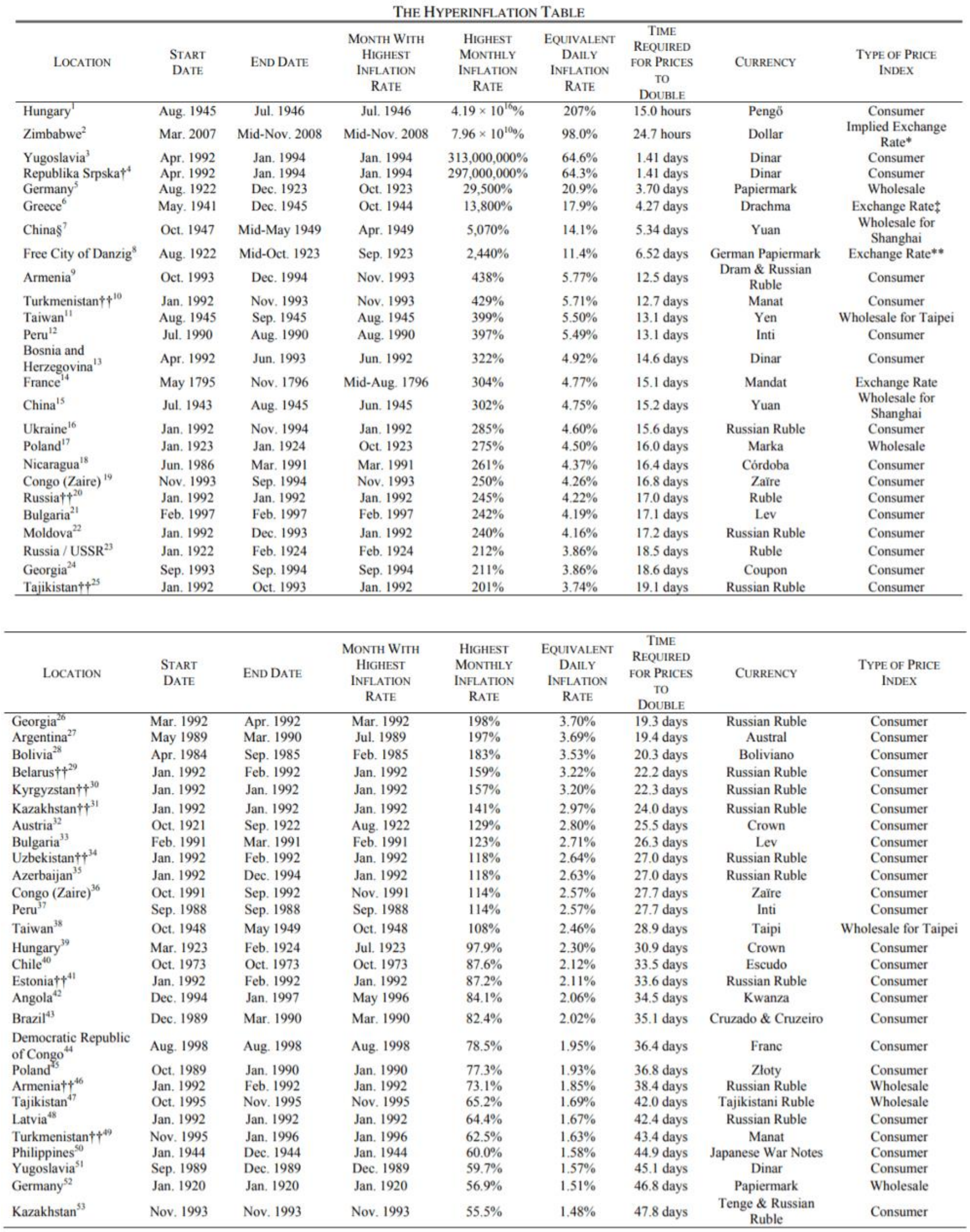
What is money?

For something so pervasive in our day-to-day lives, it is unfortunate that people don't ask themselves this question more often. Most people simply equate money with those pieces of paper stamped with faces of dead people, for that is what fulfills their preconceived notion of money—they buy groceries (means of exchange) at different relative prices (unit of account) with money saved in their checking account (store of value). It's really no surprise then that the nature of money isn't frequently questioned, as these pieces of paper have been all most people have known to be money for their entire life.

This hasn't always been the case. Today's sovereign money is—in the grand scheme of monetary history—an experiment. The U.S. dollar in its current form has been around for less than a century. Dollar bills used to be freely redeemable paper representations of gold until FDR suspended their convertibility and outlawed private gold ownership. Nixon later solidified the lack of any hard backing to the dollar when he ended the Bretton Woods System that fixed the dollar to gold in international markets. While most people wouldn't notice any difference—after that day they went from transacting using a millennia old commodity to the "full faith and credit" of the United States.

Modern Day Monopoly Money

This notion of using "fiat"—money that exists by government decree—is still a relatively new concept. And not only has it not endured the tests of time, but it has demonstrated a propensity for mismanagement. After Germany went off the gold standard post World War 1, for instance, it took less than a decade for hyperinflation to set in and their economy to collapse. From Zimbabwe to Argentina, there have been countless examples of fiat money failing spectacularly.



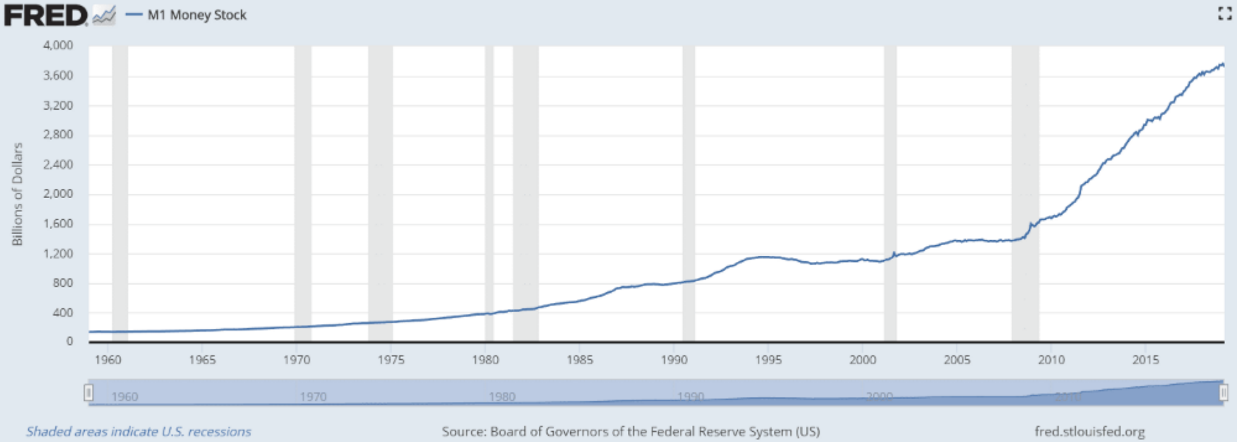
THE HYPERINFLATION TABLE

LOCATION	START DATE	END DATE	MONTH WITH HIGHEST INFLATION RATE	HIGHEST MONTHLY INFLATION RATE	EQUIVALENT DAILY INFLATION RATE	TIME REQUIRED FOR PRICES TO DOUBLE	CURRENCY	TYPE OF PRICE INDEX
Hungary[1]	Aug. 1945	Jul. 1946	Jul. 1946	4.19×10^{16}%	207%	15.0 hours	Pengő	Consumer
Zimbabwe[2]	Mar. 2007	Mid-Nov. 2008	Mid-Nov. 2008	7.96×10^{10}%	98.0%	24.7 hours	Dollar	Implied Exchange Rate*
Yugoslavia[3]	Apr. 1992	Jan. 1994	Jan. 1994	313,000,000%	64.6%	1.41 days	Dinar	Consumer
Republika Srpska†[4]	Apr. 1992	Jan. 1994	Jan. 1994	297,000,000%	64.3%	1.41 days	Dinar	Consumer
Germany[5]	Aug. 1922	Dec. 1923	Oct. 1923	29,500%	20.9%	3.70 days	Papiermark	Wholesale
Greece[6]	May. 1941	Dec. 1945	Oct. 1944	13,800%	17.9%	4.27 days	Drachma	Exchange Rate‡
China§[7]	Oct. 1947	Mid-May 1949	Apr. 1949	5,070%	14.1%	5.34 days	Yuan	Wholesale for Shanghai
Free City of Danzig[8]	Aug. 1922	Mid-Oct. 1923	Sep. 1923	2,440%	11.4%	6.52 days	German Papiermark	Exchange Rate**
Armenia[9]	Oct. 1993	Dec. 1994	Nov. 1993	438%	5.77%	12.5 days	Dram & Russian Ruble	Consumer
Turkmenistan††[10]	Jan. 1992	Nov. 1993	Nov. 1993	429%	5.71%	12.7 days	Manat	Consumer
Taiwan[11]	Aug. 1945	Sep. 1945	Aug. 1945	399%	5.50%	13.1 days	Yen	Wholesale for Taipei
Peru[12]	Jul. 1990	Aug. 1990	Aug. 1990	397%	5.49%	13.1 days	Inti	Consumer
Bosnia and Herzegovina[13]	Apr. 1992	Jun. 1993	Jun. 1992	322%	4.92%	14.6 days	Dinar	Consumer
France[14]	May 1795	Nov. 1796	Mid-Aug. 1796	304%	4.77%	15.1 days	Mandat	Exchange Rate
China[15]	Jul. 1943	Aug. 1945	Jun. 1945	302%	4.75%	15.2 days	Yuan	Wholesale for Shanghai
Ukraine[16]	Jan. 1992	Nov. 1994	Jan. 1992	285%	4.60%	15.6 days	Russian Ruble	Consumer
Poland[17]	Jan. 1923	Jan. 1924	Oct. 1923	275%	4.50%	16.0 days	Marka	Wholesale
Nicaragua[18]	Jun. 1986	Mar. 1991	Mar. 1991	261%	4.37%	16.4 days	Córdoba	Consumer
Congo (Zaire) [19]	Nov. 1993	Sep. 1994	Nov. 1993	250%	4.26%	16.8 days	Zaïre	Consumer
Russia††[20]	Jan. 1992	Jan. 1992	Jan. 1992	245%	4.22%	17.0 days	Ruble	Consumer
Bulgaria[21]	Feb. 1997	Feb. 1997	Feb. 1997	242%	4.19%	17.1 days	Lev	Consumer
Moldova[22]	Jan. 1992	Dec. 1993	Jan. 1992	240%	4.16%	17.2 days	Russian Ruble	Consumer
Russia / USSR[23]	Jan. 1922	Feb. 1924	Feb. 1924	212%	3.86%	18.5 days	Ruble	Consumer
Georgia[24]	Sep. 1993	Sep. 1994	Sep. 1994	211%	3.86%	18.6 days	Coupon	Consumer
Tajikistan††[25]	Jan. 1992	Oct. 1993	Jan. 1992	201%	3.74%	19.1 days	Russian Ruble	Consumer
Georgia[26]	Mar. 1992	Apr. 1992	Mar. 1992	198%	3.70%	19.3 days	Russian Ruble	Consumer
Argentina[27]	May 1989	Mar. 1990	Jul. 1989	197%	3.69%	19.4 days	Austral	Consumer
Bolivia[28]	Apr. 1984	Sep. 1985	Feb. 1985	183%	3.53%	20.3 days	Boliviano	Consumer
Belarus††[29]	Jan. 1992	Feb. 1992	Jan. 1992	159%	3.22%	22.2 days	Russian Ruble	Consumer
Kyrgyzstan††[30]	Jan. 1992	Jan. 1992	Jan. 1992	157%	3.20%	22.3 days	Russian Ruble	Consumer
Kazakhstan††[31]	Jan. 1992	Jan. 1992	Jan. 1992	141%	2.97%	24.0 days	Russian Ruble	Consumer
Austria[32]	Oct. 1921	Sep. 1922	Aug. 1922	129%	2.80%	25.5 days	Crown	Consumer
Bulgaria[33]	Feb. 1991	Mar. 1991	Feb. 1991	123%	2.71%	26.3 days	Lev	Consumer
Uzbekistan††[34]	Jan. 1992	Feb. 1992	Jan. 1992	118%	2.64%	27.0 days	Russian Ruble	Consumer
Azerbaijan[35]	Jan. 1992	Dec. 1994	Jan. 1992	118%	2.63%	27.0 days	Russian Ruble	Consumer
Congo (Zaire)[36]	Oct. 1991	Sep. 1992	Nov. 1991	114%	2.57%	27.7 days	Zaïre	Consumer
Peru[37]	Sep. 1988	Sep. 1988	Sep. 1988	114%	2.57%	27.7 days	Inti	Consumer
Taiwan[38]	Oct. 1948	May 1949	Oct. 1948	108%	2.46%	28.9 days	Taipi	Wholesale for Taipei
Hungary[39]	Mar. 1923	Feb. 1924	Jul. 1923	97.9%	2.30%	30.9 days	Crown	Consumer
Chile[40]	Oct. 1973	Oct. 1973	Oct. 1973	87.6%	2.12%	33.5 days	Escudo	Consumer
Estonia††[41]	Jan. 1992	Feb. 1992	Jan. 1992	87.2%	2.11%	33.6 days	Russian Ruble	Consumer
Angola[42]	Dec. 1994	Jan. 1997	May 1996	84.1%	2.06%	34.5 days	Kwanza	Consumer
Brazil[43]	Dec. 1989	Mar. 1990	Mar. 1990	82.4%	2.02%	35.1 days	Cruzado & Cruzeiro	Consumer
Democratic Republic of Congo[44]	Aug. 1998	Aug. 1998	Aug. 1998	78.5%	1.95%	36.4 days	Franc	Consumer
Poland[45]	Oct. 1989	Jan. 1990	Jan. 1990	77.3%	1.93%	36.8 days	Złoty	Consumer
Armenia††[46]	Jan. 1992	Feb. 1992	Jan. 1992	73.1%	1.85%	38.4 days	Russian Ruble	Wholesale
Tajikistan[47]	Oct. 1995	Nov. 1995	Nov. 1995	65.2%	1.69%	42.0 days	Tajikistani Ruble	Wholesale
Latvia[48]	Jan. 1992	Jan. 1992	Jan. 1992	64.4%	1.67%	42.4 days	Russian Ruble	Consumer
Turkmenistan††[49]	Nov. 1995	Jan. 1996	Jan. 1996	62.5%	1.63%	43.4 days	Manat	Consumer
Philippines[50]	Jan. 1944	Dec. 1944	Jan. 1944	60.0%	1.58%	44.9 days	Japanese War Notes	Consumer
Yugoslavia[51]	Sep. 1989	Dec. 1989	Dec. 1989	59.7%	1.57%	45.1 days	Dinar	Consumer
Germany[52]	Jan. 1920	Jan. 1920	Jan. 1920	56.9%	1.51%	46.8 days	Papiermark	Wholesale
Kazakhstan[53]	Nov. 1993	Nov. 1993	Nov. 1993	55.5%	1.48%	47.8 days	Tenge & Russian Ruble	Consumer

Hanke & Krus, World Hyperinflation Table

Often these are cases in which the absolute worst case occurred: the complete collapse of money led to economic ruin.

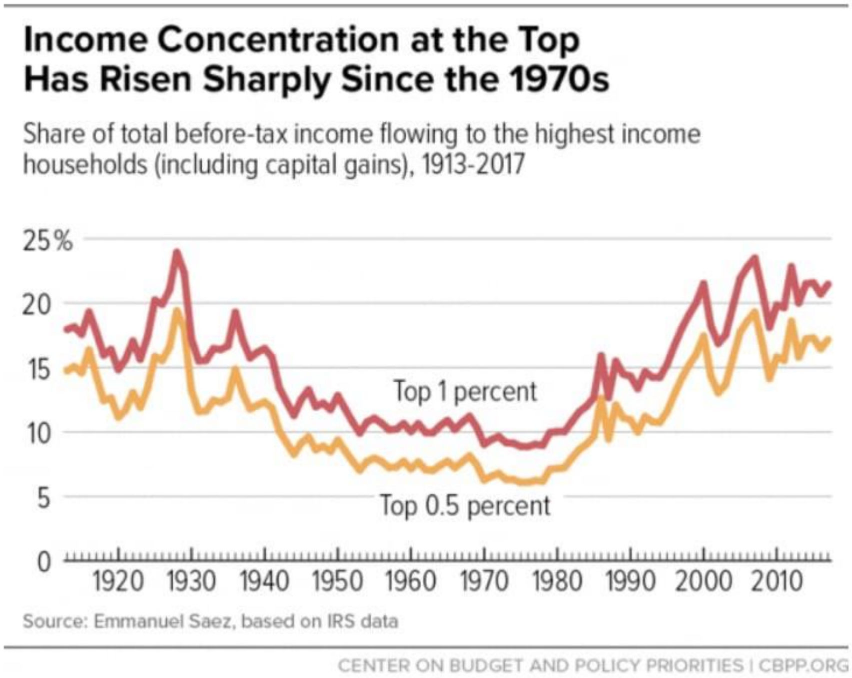
The threat of hyperinflation is always present in fiat systems, but many developed nations have been able to manage their monetary systems to avoid this type of collapse. The USD is just one example. Since its departure from the gold standard, the U.S. has maintained its status as a world power despite massive increases in the national debt and M1 money supply.

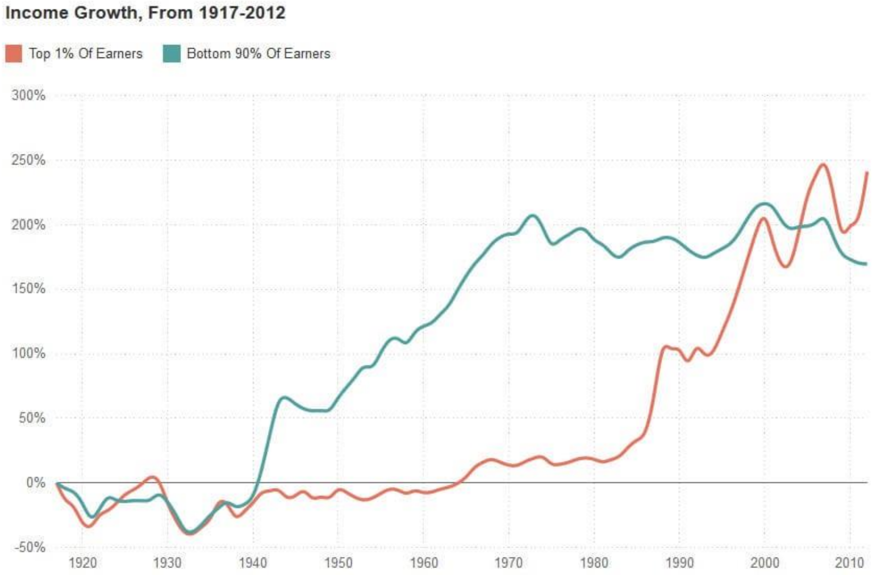


Many argue that the dollar is our leading export, and it is evident the U.S. Government has not been shy when it comes to its power of money creation. This has resounding implications for everyone using the USD.

Holding fiat means that you are continuously losing value, and in order to "beat" inflation you have to create a diversified investment portfolio. The wealthy can plow their money into equities, real-estate and commodities which bubble up from all the easy money, while those without access to these investments see their purchasing power decline. This is a classic case of the rich getting richer and is attributable to inflationary monetary policies.

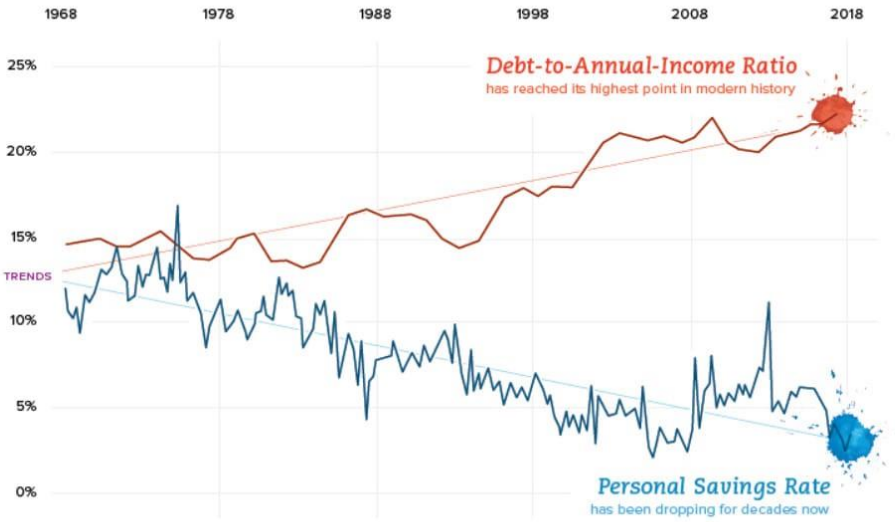
Notice the chart below and what happens right around 1971… when fiat money was born in the U.S. (Source: Center on Budget Policy, NPR)





Since you know your dollar will be worth less tomorrow than it is today, you are incentivized to have a "high time preference" and to spend more now.

If you don't have the money to spend, but lots of money is generally available, you might take out debt because you know those goods you want/need will only cost more tomorrow. Inflationary regimes lead to more spending, less saving and larger indebtedness as we see today in a society drowning in debt.



Source: Visual Capitalist

This begs the question, what other forms of money have *succeeded* for longer periods of time?

The obvious answer is gold, and most people are familiar with its use as money but haven't given much thought to why. In addition to gold, humans have also used other commodities such as shells or Rai stones to transact **because they held certain desirable characteristics**. To varying degrees they were:

- Secure from loss/theft
- Scarce, difficult to counterfeit
- Easily measurable/divisible

Over time goods that held these desirable characteristics outlived others. (Insert obligatory Nick Szabo article on the origins of money)

The Not So Modern, Modern Monetary Theory

While the idea of valuable commodity money makes sense to some, most of the conversation today is gravitating towards a school of thought with a diametric viewpoint, known as Modern Monetary Theory (MMT).

The foundations of this viewpoint, known as Modern Monetary Theory (MMT), date back to the early 20th century with George Knapp's *The State Theory of Money.* **This theory directly contradicts the prior notion that money holds value due to its desirable characteristics**. Knapp argues that "money is a creation of law" and derives its value from the State, and its requirement that taxes be paid in their native currency.

The degree of "moneyness" is a result of acceptability, with the ultimate form of acceptance as payment to the government. This theory (also known as Chartalism) was further refined in *The Credit Theory of Money* by A. Mitchell Innes, which postulates **money is a liability imposed by the State to measure obligations**. When you buy groceries you are taking on debt and measuring it with that fiat. Currency acts as an IOU so the grocer then has a debt owed to them with which they can again redeem for something valuable using the currency. This seems to suggest that money has no intrinsic value, directly rejecting the prior idea of sound commodity money. The market is no longer a place where goods are exchanged but simply a clearing house for settling debits and credits.

While the sound money view says humans began with barter and transitioned to using goods with desirable characteristics to transact in order to solve the double coincidence of wants, the Chartalist view says we progressed from shells to gold coins to fiat as a result of finding more efficient means to track debt. This explains the desire to transition away from the gold standard since redemptions of paper notes for gold coins are merely the exchange of one form of obligation for another that's identical in practice. The notion of an asset backed currency is one in which the government's flexibility to control the money supply is restricted.

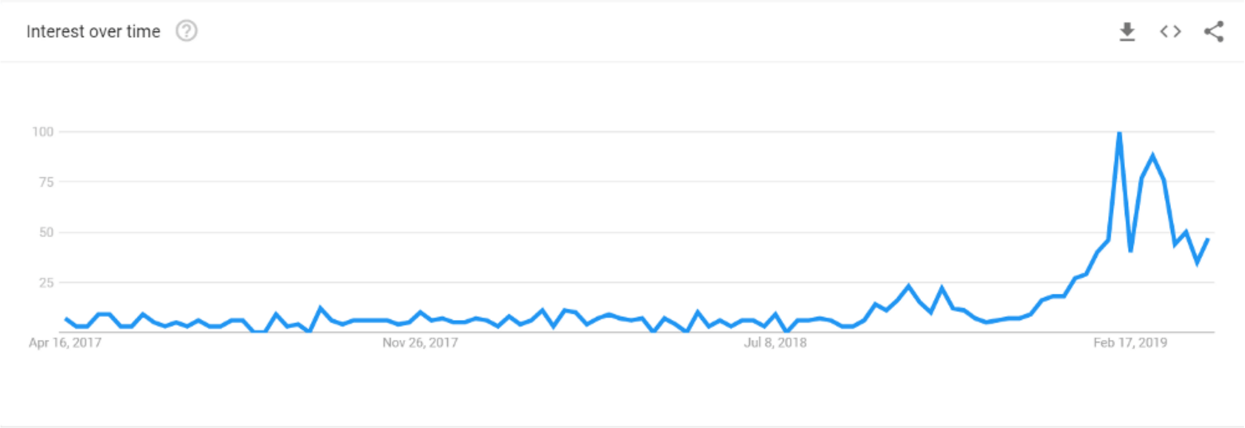
Subscribing to this Chartalist view of money leads one to arrive at some interesting policy conclusions.

In today's world, only sovereign governments claim this ability to impose liabilities on others because they can create demand by requiring taxes to be paid in that same government liability. **Therefore a government has no need to balance its budget and spending can greatly outpace tax revenue since the difference can be covered by the creation of more money—i.e. debt**.

MMT economists believe that governments can create as much debt as they want so long as there is adequate demand for their currency from state imposed obligations. In theory, governments can finance themselves strictly through issuing currency until inflation rises to a point where taxes need to be levied to increase the demand side of money to keep pace with supply.

If that's too much of a mouthful, former Fed Chairman Alan Greenspan sums it up:

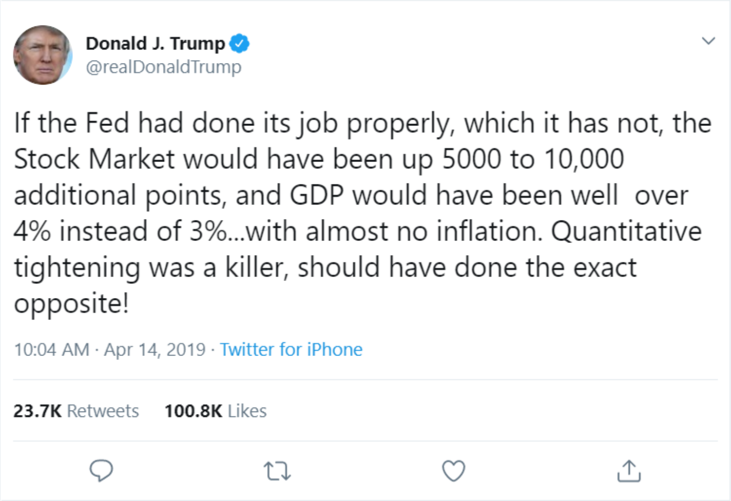
"The United States can pay any debt it has because we can always print money to do that. So there is zero probability of default."



Google search trends for "Modern Monetary Theory

MMT in the 21st Century

While the underpinnings of MMT are not new, there has been a strong resurgence of these ideas in recent years from both sides of the political spectrum. The modern belief is that the government can run perpetual deficits to fund wars or pay for universal healthcare. If these policies don't work as intended and lead to financial distress, they can simply print more money!



Donald J. Trump @realDonaldTrump

If the Fed had done its job properly, which it has not, the Stock Market would have been up 5000 to 10,000 additional points, and GDP would have been well over 4% instead of 3%...with almost no inflation. Quantitative tightening was a killer, should have done the exact opposite!

10:04 AM · Apr 14, 2019 · Twitter for iPhone

23.7K Retweets **100.8K** Likes

On paper the Chartalist view of money might make sense. You look around the world and every form of money with mainstream adoption is required by the State to be paid in taxes. Therefore, one could conclude that what makes it valuable is this requirement. However, a truly competitive market has not been possible to challenge the hegemony of fiat money. Every attempt from liberty dollars to E-gold was shut down by the government. The State has and will go to great lengths to maintain financial control over its citizens.

Enter Bitcoin

This all changed a decade ago, when pseudonymous author Satoshi Nakamoto wrote the Bitcoin White Paper and released his monetary experiment to the world that fundamentally challenged the core beliefs of MMT. The decentralized nature of Bitcoin meant that even if the State wanted to shut it down, it would be an incredibly difficult project to kill at a certain scale. This new form of money was able to exist out in the wild, allowing for the first time the possibility of a true competitor to fiat money.

Recall that the Chartalist belief is that money has value because of its acceptability by the State. This thinking would lead one to believe that an asset looking to be used as currency should not be desired unless it can be used to pay taxes. Yet, despite not operating as legal tender, it has led to millions of people across the world **demand it for its desirable characteristics.** Bitcoin has built a robust social contract with its users and for that reason has a network value of ~ $160 billion, nearly a million active addresses, and $17 million being spent every day to secure the network (data from OnChainFX). This contract is described in the following:

- Only the owner of a coin can produce the signature to spend it (confiscation resistance)
- Anyone can transact and store value in bitcoin without permission (censorship resistance)
- There will only be 21 million bitcoins, issued on a predictable schedule (inflation resistance)
- All users should be able to verify the rules of bitcoin (counterfeit resistance)

These unique features are what have allowed the unlikely outcome of Bitcoin's relative success.

Not because it is accepted by the State. Not because it is an effective means of tracking debt.

So What?

If you rebut the core assumptions upon which an argument is made, then you have destroyed the argument. MMT argues that money isn't valuable because of its characteristics, yet bitcoin has accrued value and achieved usage solely because of them. Since people value money for its inherent nature, in the long-run money that is susceptible to be printed at the whims of the government won't be as successful as one that is not. We've seen this play out in extreme situations where nations abuse their money creating abilities and their currency becomes worthless as users adopt more sound money. In a world absent free-market competition besides fiat, this has traditionally been the U.S dollar.

However, now that Satoshi has introduced Bitcoin, those living in places where modern monetary policies are rampant can now opt for an alternative. The U.S. dollar has long been a safe haven asset, but if these policies continue unobstructed that could change. (Note: The next Bitcoin halving will lower inflation below the U.S. target rate) This will not likely be an expedient process, money is a social construct that takes decades if not centuries to become entrenched in everyday life. But if you recognize the second and third order effects of fiat money and its abuses, then you should be open to the sound money alternative that is Bitcoin.

Tweetstorm: Bitcoin rescues the human

By Conner Brown

Posted June 3, 2019

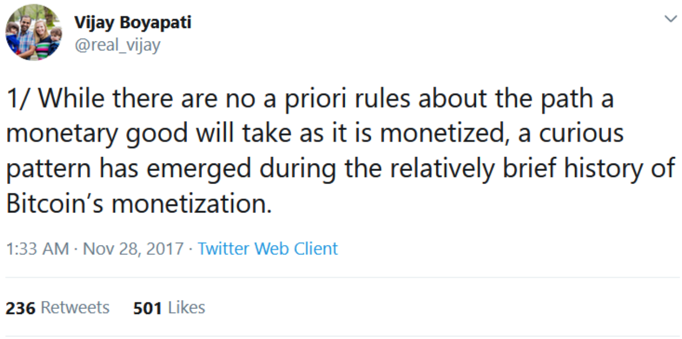
- Bitcoin rescues the human.
- The pursuit of rationality has attempted to achieve objectivity in all forms of knowledge by removing the subject.
- The common refrain is that academic thought is only useful if pesky human biases are removed.
- While incredibly useful in some domains, this has devastating consequences in the social sciences.
- Unbridled rationality has led academics to believe they can perfectly engineer society by reducing citizens to the right variables and controls.
- This exploded in dramatic fashion through the totalitarian regimes of Hitler, Stalin and Mao (to name a few). Killing millions in the pursuit of objective utopia.
- We can see similar trends today in China's social credit systems—reducing citizens to compliance algorithms.
- While less serious, this thinking is also a cornerstone in our present monetary systems.
- Central banks around the world actively try to engineer a financial system better than the billions of interrelated ideas, desires, and values in the marketplace.
- Institutions such as the FOMC attempt to reduce infinitely complex human networks to predictable curves.
- The world is not so simple—the financial meltdowns of the past 100 years are plenty proof.
- Such arrogance results in inequality, stagnation, and crisis.
- Bitcoin returns an essential subjectivity to our social order by providing a constant, predictable money that individuals can rely on to honestly communicate their subjective preferences.
- Our money supply will no longer be controlled by a small group of men huddled around a table, attempting to read the monetary tea leaves.
- Instead, rates and credit will be set by the sum total of interactions—with each actor pushing and pulling to reach a human balance.
- Long bitcoin, short the central bankers 🤠

Tweetstorm: Touchpoints

By Vijay Boyapati

Posted June 4, 2019

1. How many times did you have to hear about #Bitcoin before you were ready to acquire some or, at least, explore its significance? This number of "touchpoints" is an important factor in the process of Bitcoin's monetization. Let's explore the idea of touchpoints in a thread: 👇
2. We now know that the process of #Bitcoin's monetization is occurring in a series of hype cycles where the magnitude of each cycle is defined by the people "reachable" in that cycle. Which people defined the prior cycles? 👇



Vijay Boyapati
@real_vijay

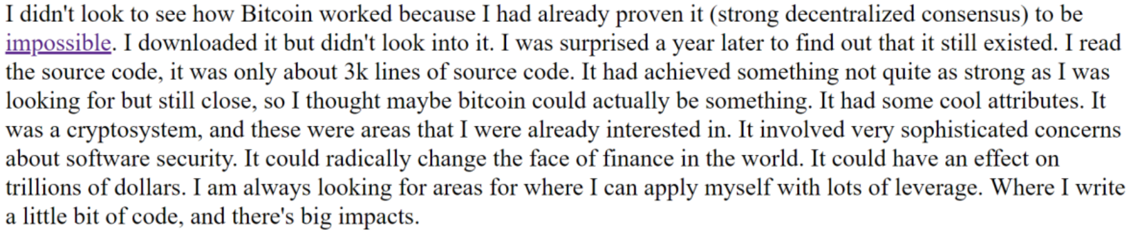
1/ While there are no a priori rules about the path a monetary good will take as it is monetized, a curious pattern has emerged during the relatively brief history of Bitcoin's monetization.

1:33 AM · Nov 28, 2017 · Twitter Web Client

236 Retweets 501 Likes

thread link

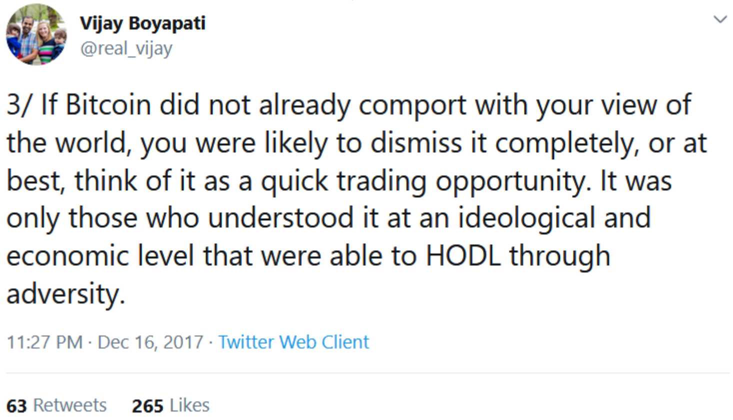
3. The first hype cycle in the #Bitcoin market was dominated by cryptographers and cypherpunks who were already primed to understand the importance of Satoshi Nakamoto's groundbreaking invention.
4. But even among the cohort of cryptographers and cypherpunks primed to understand #Bitcoin, some of the most brilliant required multiple touchpoints before being convinced that Satoshi was onto something. Consider the words of Core developer Gregory Maxwell:



I didn't look to see how Bitcoin worked because I had already proven it (strong decentralized consensus) to be impossible. I downloaded it but didn't look into it. I was surprised a year later to find out that it still existed. I read the source code, it was only about 3k lines of source code. It had achieved something not quite as strong as I was looking for but still close, so I thought maybe bitcoin could actually be something. It had some cool attributes. It was a cryptosystem, and these were areas that I were already interested in. It involved very sophisticated concerns about software security. It could radically change the face of finance in the world. It could have an effect on trillions of dollars. I am always looking for areas for where I can apply myself with lots of leverage. Where I write a little bit of code, and there's big impacts.

5. I was personally part of the second hype cycle which attracted those with an ideological affinity for #Bitcoin's freedom promoting potential (libertarians). But it took many touchpoints for me to recognize its importance (I'm a slow learner).
6. Luckily for me, I had a very high opinion of the two people who evangelized #Bitcoin to me (one of them had been my co-founder in a @YCombinator startup). And they were planting seeds in fertile ideological ground. But what if I had no ideological affinity?

7. One lesson to take away is that if a person is not reachable in a particular hype cycle, there is almost no point is trying to convince them of #Bitcoin's importance. As best they would view it as a quick trading opportunity



Vijay Boyapati
@real_vijay

3/ If Bitcoin did not already comport with your view of the world, you were likely to dismiss it completely, or at best, think of it as a quick trading opportunity. It was only those who understood it at an ideological and economic level that were able to HODL through adversity.

11:27 PM · Dec 16, 2017 · Twitter Web Client

63 Retweets 265 Likes

8. To be "reachable" to #Bitcoin's potential most people will typically have to have heard about it multiple times from multiple people that they trust. One sign that a new group will become reachable is that a respected person in the group becomes an evangelizer to the group.
9. Consider, for example, Superbowl winning left tackle @RussellOkung. A well respected pro-bowl player is now evangelizing #Bitcoin to his fellow players in the #NFL. Some will pay attention to Okung and begin evangelizing it in turn, priming more and more NFL players.
10. Another way a person can be primed is if they made a small allocation to #Bitcoin (or received it as a gift) and saw that grow in a prior cycle. They will already be awake to the financial potential of a larger allocation and more receptive to learning more.
11. However, for those who are ideologically *opposed* to #Bitcoin there is no number of touchpoints that will convince them of its importance. Think of people like @paulkrugman or @Nouriel. They will be walking around with wheelbarrows of worthless fiat before owning bitcoins.
12. So when explaining #Bitcoin to friends, family and colleagues get a sense of how "primed" they already are. Have they already heard of it? Are they curious or dismissive? Are they ready for a tiny allocation, or are they ready to take the leap?
13. In the coming hype cycle, the people most ready to increase their allocation to #Bitcoin are those who were already curious about it and perhaps had made a small allocation to it in the prior cycle. They are ready to be activated in the next bull run and will define its size

Tweetstorm: Money is the most important field

By Hasu

Posted June 6, 2019

Money (not finance) is the most important field in the world today and will be for at least 20 years.

Why? 99% of history is written in 1% of the time. We are in the early phases of another 1% where the medium-term future will be written (what Neil Howe calls "The 4th Turning".)

Money is ripe for a paradigm shift, but the direction of that shift is still undecided. There are currently forces pulling into several directions, with the extreme ends being hyper-control of money (MMT) and removal of all control of money (Bitcoin.)

While in most of history local governments have issued money, many private producers will be able to compete in the future. Networks like Bitcoin are constructed from the ground up to resist, while private firms like Facebook are effectively sovereign to nation-states.

These changes in money could move the world closer to utopia or dystopia, depending on what your values are. The only outcome that seems certain today is that money will fragment as more and more producers enter the market and increase the options for consumers manyfold.

Much has been written about money being a winner-take-all or -most market, but I don't really believe in that. As the costs of storing different monies as well as exchanging between them decreases, consumers automatically put more focus on other properties.

Consolidation into one money assumes a world where custody and exchange are the biggest sources of friction for money. In reality, the friction just changes its form. The walled gardens of supranational networks like Facebook will replace the walled gardens of national economies.

The biggest friction might come in the fragmentation of the internet itself. In the same way that the unipolar world order and US-protected free trade are ending, the internet itself will almost certainly break into several shards between China, Russia, and the West.

We may be using different money in every shard and yet another money that is entirely trustless (bitcoin?) between them. The design space for money today is magnitudes greater than it has ever been, so history isn't really a guide for us.

It's hard to wrap your head around how easy it is to participate in the Cambrian explosion of money, whether we end up with one large winner in the end or several medium-sized ones. Hell, Bitcoin was created by, at most, a small group of people that is still anonymous today.

This shift will produce winners and losers. One loser could be (supporters of) big government. The large governments we have today are only possible because a) seigniorage from inflation and b) control over the financial system encourages people to honestly report their income.

If private money allows people to dodge taxes at low risk, this behavior will eventually normalize. This may be the tipping point in the growth of government that causes a mean reversion. Thus, private money will further accelerate the rise of the individual over the collective.

The biggest winners when all has been written will be the people in Emerging Markets. Local money has long been a layer-3 institution. Stable money needs stable property rights needs a stable monopoly on violence. But no more.

Soon, individuals can import their money directly via the internet without relying on the government-provided bottom layers at all. Combine that with digital goods and p2p services making up more and more of the world GDP, and we could see a democratization of trade and capital.

In sum, these are the reasons I have committed myself to the private money space, which, I fully believe, will turn into one of the biggest and most powerful industries in the world. It is on us to shape what values that industry will be built on.

The Golden Ratio Multiplier

Unlocking the mathematically organic nature of Bitcoin adoption

By Philip Swift (@PositiveCrypto)

Posted June 17, 2019

Disclaimer: Nothing contained in this article should be considered as investment or trading advice.

As Bitcoin continues to progress on its adoption journey, we learn more about its growth trajectory.

Rather than Bitcoin price action behaving like a traditional stock market share price, we see it act more like a technology being adopted at an exponential rate.

This is because Bitcoin is a network being adopted by society, and because it is decentralised money with limited supply, its price is a direct representation of that adoption process.

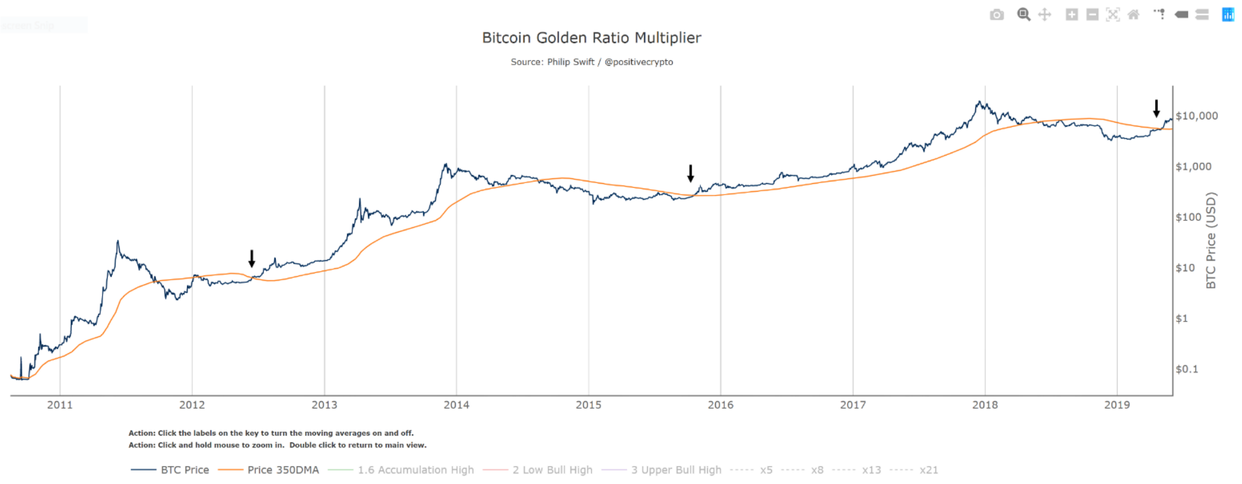
There are a number of regression analysis tools and stock to flow ratio studies that are helping us to understand the direction of Bitcoin's adoption curve.

The new tool outlined in this paper brings an alternative degree of precision to understanding Bitcoin's price action over time. It will demonstrate that Bitcoin's adoption is not only following a broad growth curve but appears to be following established mathematical structures.

In doing so, it also:

1. Accurately and consistently highlights intracycle highs and lows for Bitcoin's price.
2. Picks out every market cycle top in Bitcoin's history.
3. Forecasts when Bitcoin will top out in the coming market cycle.

To begin, we will use the 350 day moving average of Bitcoin's price. It has historically been an important moving average because once price moves above it, a new bull run begins.



Bitcoin Golden Ratio Multiplier

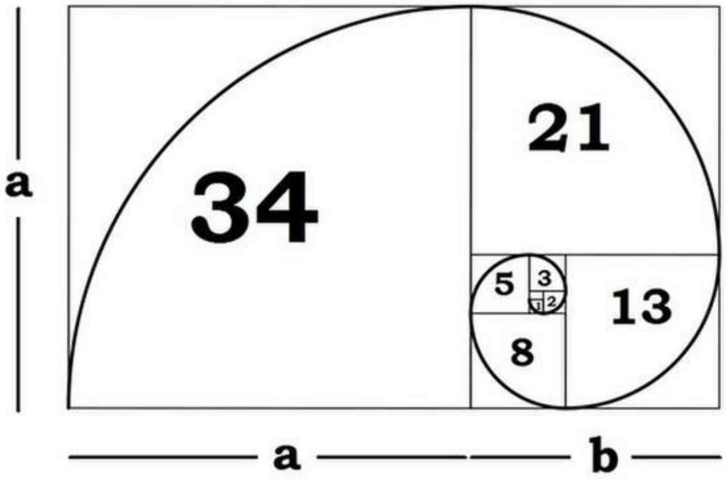
Source: Philip Swift / @positivecrypto

Action: Click the labels on the key to turn the moving averages on and off.
Action: Click and hold mouse to zoom in. Double click to return to main view.

The new insight comes when we multiply the 350 day moving average (which we will refer to as the 350DMA) by specific numbers. Those mathematically important numbers are:

The Golden Ratio = 1.61803398875

Fibonacci Sequence = 1, 1, 2, 3, 5, 8, 13, 21...



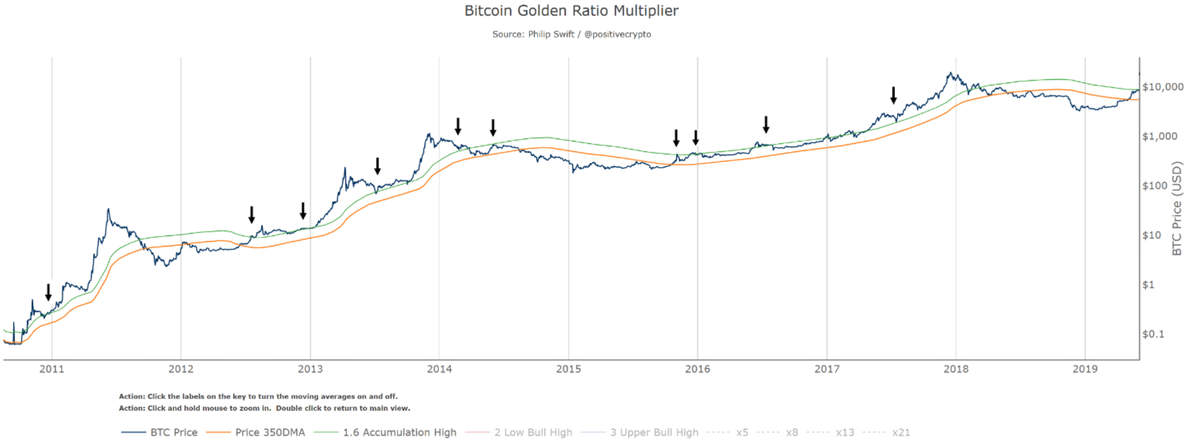
You can use these hyperlinks if you need a refresher on the importance of the golden ratio or Fibonacci sequence in nature and mathematics. But we see them consistently throughout life whether it is in the pattern of how plants grow, the structure of hurricanes, or even trader behaviour in financial markets.

Building the cyclical layers

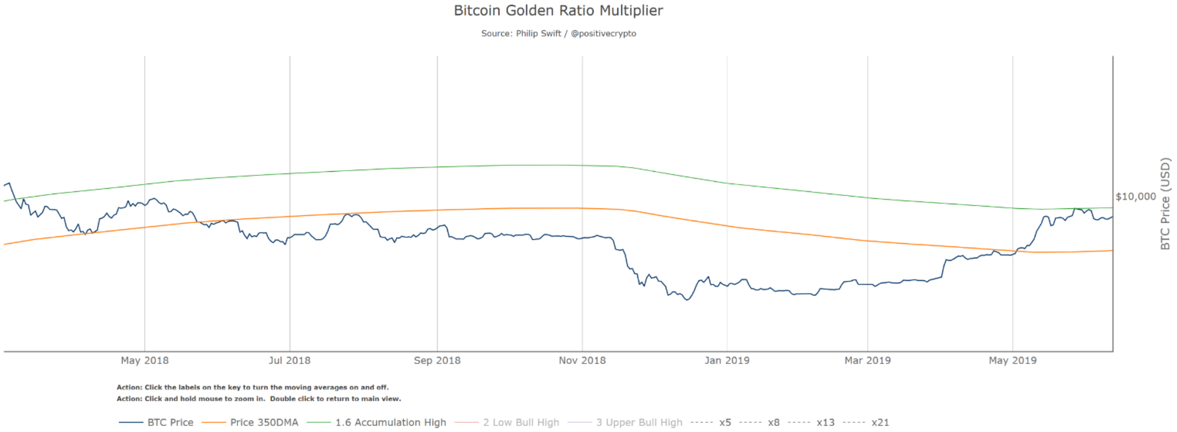
We will start with the Golden Ratio of 1.6 (rounded here to one decimal place).

If we take the 350DMA (orange line) and multiply its value by 1.6, we create a new line above it, the 350MA x 1.6 (green line).

We then discover in the chart below how this newly created green line has in fact acted as support and resistance throughout Bitcoin's history, examples of which are highlighted by the arrows on the chart:



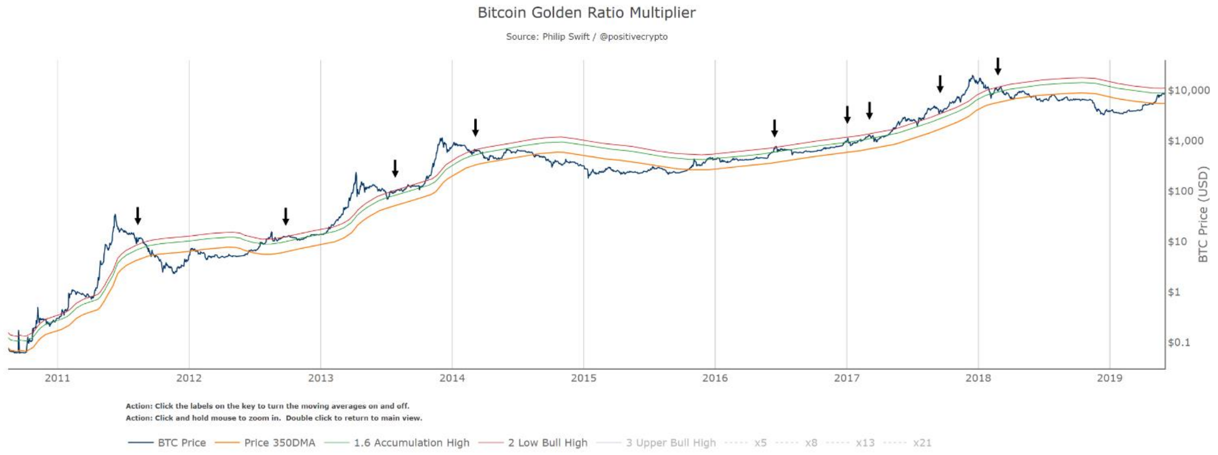
It is also worth noting that the 350DMA x 1.6 line acted as resistance in the parabolic price move from the Dec 2018 low. Rejecting price perfectly on the first touch and causing a $1,500 pullback before approaching it again and likely breaking through at the time of writing:



Things become more interesting when we then start to multiply the 350DMA by each number in the Fibonacci sequence: 1, 2, 3, 5, 8, 13, 21, etc.

Given that multiplying the 350DMA by 1 would not change its value, we start with the next number in the sequence, which is 2.

So we multiply the 350DMA by x2. Which is the red line in the chart below:

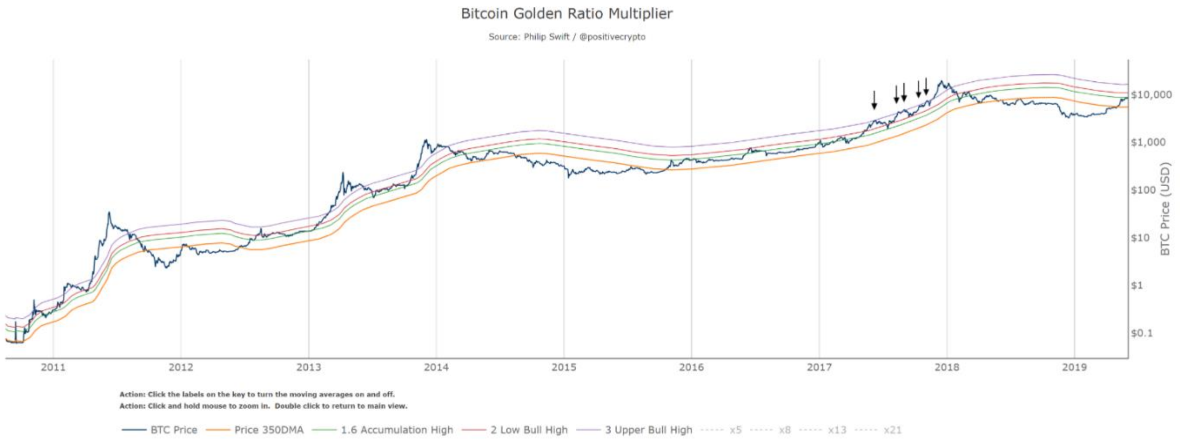


Again, the arrows highlight examples of where we see it act as a major level of support and resistance throughout Bitcoin's history. As a trader or investor this, as well as the other multipliers, makes a potentially very useful short term take profit signal when price first reaches it.

The next number in the Fibonacci sequence is 3. So now we multiply the 350 day moving average by 3.

350DMA x 3 is the purple line in the chart below.

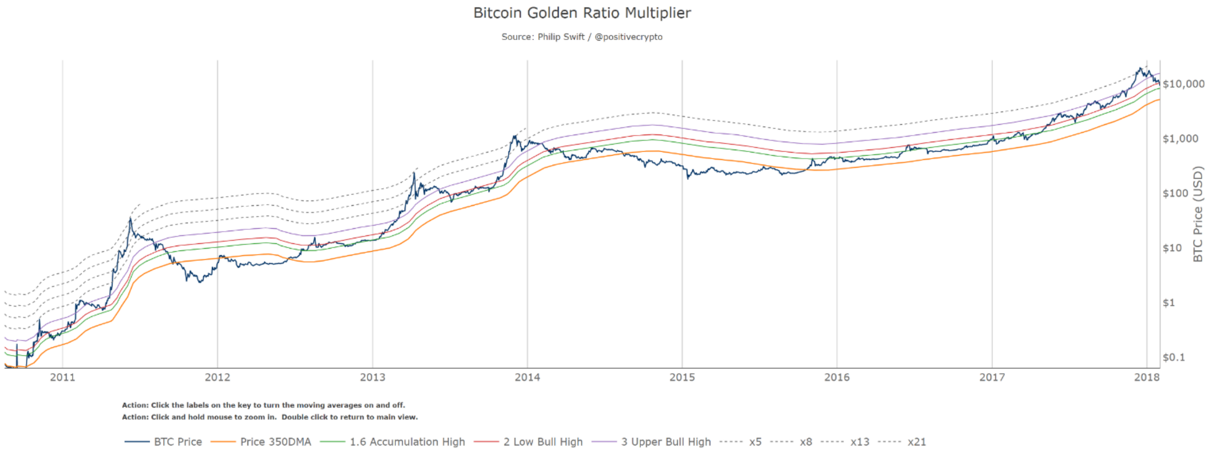
We see it acted as particularly strong resistance towards the upper stage of the 2017 bull market, with price unable to break above it on 5 separate occasions:



Using those three moving average lines (350DMA x 1.6, x2, x3) has allowed us to pick out almost every single intra-cycle price high in Bitcoin's history.

The next numbers in the Fibonacci sequence are 5, 8, 13, and 21.

Remarkably, when we use these multiples of the 350 day moving average, they pick out each of Bitcoin's market cycle tops going all the way back to the first price bubble in 2011. They are shown as dotted lines here:



Bitcoin Golden Ratio Multiplier

Source: Philip Swift / @positivecrypto

Action: Click the labels on the key to turn the moving averages on and off.
Action: Click and hold mouse to zoom in. Double click to return to main view.

Bitcoin price action obeying Fibonacci multiples of the 350 day moving average

350DMA x21 = 2011 top

350DMA x13 = 2013 top

350DMA x 8 = 2014 top

350DMA x5 = 2018 top

Practical application

As with any indicator, the Golden Ratio Multiplier should not be used in isolation, but it does offer a risk management opportunity. Using the previous cycle as an example, if one had bought the breakout at the 350DMA and then taken profit the first time price reached the x1.6, the x2, and the x3, buying back lower each time, that would have been a very successful investment strategy. One could then have sold the top of the market as price touched the 350DMA x5.

If Bitcoin's market cycle tops continue to follow this declining Fibonacci sequence, then the next market cycle top will be when price hits the 350DMA x3 (purple line).

Why does price obey these levels?

We know that Bitcoin goes through multi-year market cycles which are driven by over-optimism and over-pessimism. The 350DMA appears to be particularly relevant to those market cycles as to date it has been the axis that the cycles have rotated on.

Given that market psychology (of over-optimism and over-pessimism) is a major factor driving these market cycles, it is plausible that part of the reason why Fibonacci multiples of the 350DMA are so important is due to how herd mentality responds to price action:

In many cases, it is believed that humans subconsciously seek out the golden ratio. For example, traders aren't psychologically comfortable with excessively long trends. Chart analysis has a lot in common with nature, where things that are based on the golden section are beautiful and shapely and things that don't contain it look ugly and seem suspicious and unnatural. This helps to explain why, when the distance from the golden section becomes excessively long, the feeling of an improperly long trend arises.

Understanding Fibonacci Numbers. Dima Vonko, Investopedia, 2019

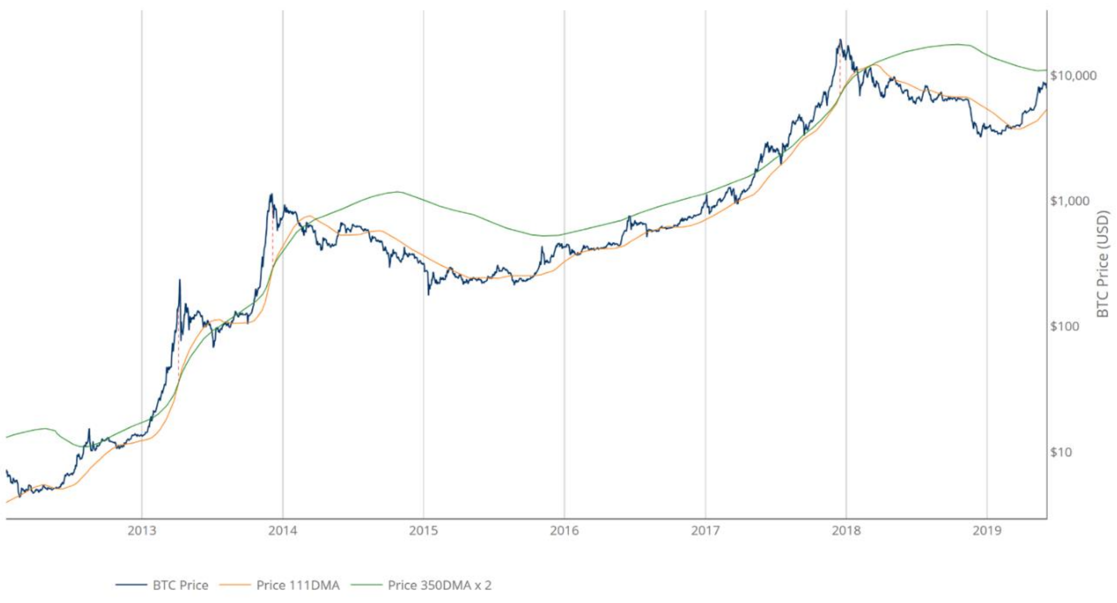
Whatever the reason, the tool highlights the cyclical nature of Bitcoin adoption and the flattening of its growth trajectory on a log scale.

Bonus: picking market cycle tops to within 3 days

Using the x2 multiple of the 350 day moving average along with the 111 day moving average provides us with a different market cycle indicator.

When the 350DMA x2 crosses below the 111DMA, Bitcoin price peaks in its market cycle. Over the past three market cycles, this has been accurate **to within three days** of Bitcoin price topping out:

Source: Philip Swift | @positivecrypto



This will be something worth monitoring in the latter stages of the coming bull run.

It is also of interest to note what 350 / 111 equals:

350 / 111 = 3.153

Which is very close to Pi.

Pi = 3.142

It is, in fact, the closest we can get to Pi when dividing 350 by another whole number.

Conclusion

The Golden Ratio Multiplier will be a useful investment tool in this coming market cycle for identifying areas of take-profit as price approaches the multiplier levels of 350DMA x1.6, x2, and x3.

Assuming the Fibonacci sequence countdown continues to play out, the 350DMA x3 will signal the top of this coming market cycle.

The tool can also signal market tops when used alongside the 111DMA.

But arguably more powerful than these investment and trading benefits is the ability to demonstrate how Bitcoins adoption, and therefore our herd behaviour as humans, is following mathematical structures.

Via its price action, Bitcoin is offering us the opportunity to view free market adoption in real time, revealing how humans adopt at scale. Which is a beautifully humbling phenomenon to observe.

Thanks to Willy Woo for his assistance with the Golden Ratio chart layout aesthetic.

To use the live chart of the Golden Ratio Multiplier follow me on Twitter where there is a link to it in my bio. It is free to use and doesn't require sharing any personal data. I'll be sharing more tools via Twitter in the coming months.

There Can Be Only One

By Tamas Blummer

Posted June 18, 2019

Network effect is a weak argument for Bitcoin's value. There is a stronger one: There can only be one definition of time with computation.

An argument against Bitcoin's value is that alternate crypto currencies, also known as "shitcoins", exhibit the same digital scarcity within their own network. Pundits add up market cap of Bitcoin with shitcoins to come up with a market cap of "crypto".

Some think the existence of shitcoins defies Bitcoin's scarcity and show that Bitcoin can be copied and multiplied and consequently Bitcoin and all crypto is worthless.

It is pointless to argue against this with the network effect of Bitcoin, as the question is not if Bitcoin could be replaced with a better version of itself, but if scarcity can be achieved at all by a design similar to Bitcoin.

Similar to Bitcoin?

A shitcoin could be considered similar to Bitcoin for many reasons. Some consider ZuckBuck similar, because … whatever.

The similarity that really matters is the mechanism that creates scarcity. In Bitcoin's case it is the Nakamoto consensus built on proof of work (POW).

Many shitcoins experiment with alternate consensus algorithms, such as BFT, POS, POET, governance or any combination of them. The ability to prove work is ultimately constrained by physics and available resources. Those alternatives to POW use strictly more assumptions hence the scarcity they achieve is of lower reliability, quality.

We will soon see if the quality of scarcity offered by Zuck is deemed sufficient by the masses and hence ZuckBuck manages a "flippening" against fiat in the daily uses of buying likes or in-app gadgets in facebook and related apps.

Our quest is however not for a good enough scarcity for some use case, but that of ultimate digital scarcity, which would give rise to highest value.

Proof of Work

Different qualities of scarcity are with us already. There are less guarantees for scarcity of fiat than that of gold. The marginal supply of fiat changes at the will of bureaucrats, that of Gold is limited by natural reserves and work invested.

A doubt of Gold Standard could be articulated as: Other precious metals exhibit very comparable physical properties, hence they are as good as gold, therefore supply of "hard money" is not constrained by gold supply.

The world however operated on Gold Standard and not on Precious Metal Standard. Those promoting an alternate Silver Standard experienced heavy losses in the process of consolidation.

It seems that although several precious metals are eligible through their physical properties and supply of all of them is constrained by work, only one became the standard to store value.

Scarcity through POW

There is a striking parallel between work in gold mines and in Bitcoin mines. The resulting product proves work performed. POW is not unique to Bitcoin. POW is used by countless shitcoins. Do shitcoins that also use POW undermine digital scarcity?

Digital scarcity based on POW does not require that Bitcoin, as we know it today, becomes the only one, but that only one POW coin is desired by all. Like there can only be one Highlander, one immortal swordsman.

POW Standard or Bitcoin Standard ?

To keep its emission schedule Bitcoin requires the proof that miner did (busy-)wait a time span (expected 10 minutes) before producing a new block. The proof is the result of a computation.

Alternate proofs of wait, such as POET suggested by e.g. Intel could deliver a lower quality of scarcity, but POW makes no compromises. POW is a method of measuring time with computation.

The difficulty adjustments based on timestamps are only there to periodically adjust for time measurement errors, the actual tool of time measurement is the computation itself.

Time measurement with computation is only reliable if the executed computation is irreducible and all resources capable of its computation are deployed to that task.

Fragmenting computing resources across competing time chains however will not achieve the reliability of one time chain that uses all resources. The Bitcoin Standard will arise as a consequence of aiming for the best quality of time chain.

I anticipate on the long run a convergence to a single time chain, that is likely a descendant of Bitcoin as we know.

There are many choices of irreducible computation, and double-SHA256 of Bitcoin is not one. See midstate or ASICBoost. A better time chain would have a simpler POW that is provably irreducible. One that can be evaluated on the least simple machine, a cellular automaton as in NKS to exclude any chance of shortcut. A time chain with such POW would give us the most precise measurement of time with computation.

Bitcoin bites the bullet

Some of its most puzzling tradeoffs explained

By Nic Carter

Posted June 19, 2019

In the matter of reforming things […] there is a paradox. There exists in such a case a certain institution or law; let us say, […] a fence or gate erected across a road. The more modern type of reformer goes gaily up to it and says, "I don't see the use of this; let us clear it away." To which the more intelligent type of reformer will do well to answer: "If you don't see the use of it, I certainly won't let you clear it away. Go away and think. Then, when you can come back and tell me that you do see the use of it, I may allow you to destroy it." – G.K. Chesterton, ***The Thing: Why I am a Catholic***

What's wrong with Bitcoin is that it's ugly. It is not elegant. **–**Gwern Branwen **,** ***Bitcoin is Worse Is Better***

It is sometimes said that there are no free lunches in cryptocurrency design, only tradeoffs. This is a frequent refrain from exasperated Bitcoiners seeking to explain why *hot new cryptocurrency* probably can't deliver 10,000 TPS with the same assurances as Bitcoin.

Today, as hundreds of alternative systems for permissionless wealth transfer have been proposed and implemented, it's worth contemplating *why* exactly Satoshi built Bitcoin as s/he did, and why its stewards oriented the project in such a deliberate way.

Here I'll argue that its features were not arbitrarily selected, but chosen with care, in order to create a sustainable and resilient system that would be robust to a variety of shocks. In many cases, this required choosing an option which appeared unpalatable on its face. This is what I mean by *biting the bullet.* It is evident to me that that, when faced with two alternatives, Bitcoin often selects the less convenient of the two.

This is confusing to many—hence "I just heard about Bitcoin and I'm here to fix it" syndrome—but when long-term consequences are taken into account, the design considerations often make sense.

As a consequence, Bitcoin is saddled with a variety of features which are cumbersome, onerous, restrictive, and impair its ability to innovate, all in service of a longer-term or more overarching goal. In this article I'll cover a few of the tradeoffs where Bitcoin opted for the unpopular or more challenging path, in pursuit of an ambitious long-term objective:

- Managed/unmanaged exchange rates
- Uncapped/capped supply
- Frequent/infrequent hard forks
- Discretionary/nondiscretionary monetary policy
- Unbounded/bounded block space

Managed/unmanaged exchange rates

One of the commonest critiques of Bitcoin, often emanating from central bankers or economists, is that it is not a currency because it lacks price stability. Typically, the mandate of central bankers is to optimize for relatively stable purchasing power (although currency depreciation at two percent a year is considered tolerable in the US) and other objectives like full employment. Lacking any mechanism to manage exchange rates, Bitcoin is considered *a priori* not a currency. Implicit in the conventional view of what constitutes a sovereign currency is some notion of management; just ask Christine Lagarde:

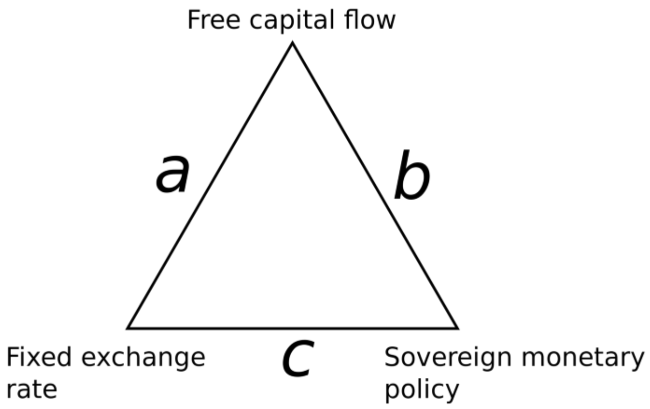
For now, virtual currencies such as Bitcoin pose little or no challenge to the existing order of *fiat* currencies and central banks. Why? Because they are too volatile, too risky, too energy intensive, and because the underlying technologies are not yet scalable.

Or Cecilia Skingsley, deputy director of the Swedish central bank:

I have no problem with people using [bitcoin] as an asset to invest in, but it's too volatile to be used as currency.

Of course, Bitcoin's volatility cannot be managed; against the backdrop of a scarce supply, price is almost exclusively a function of demand. Bitcoin is almost perfectly inelastic in its supply, and so waves of adoption manifest themselves in gut-wrenching price gyrations. This contrasts with sovereign currencies where the central bank pulls various levers to ensure relative exchange rate stability.

The tradeoffs inherent in monetary policy are often expressed as a trilemma, where monetary authorities can select two vertices but not all three. To put this another way, if you want to peg your currency to something stable (usually another currency like the US dollar), you have to control both the supply of your currency (sovereign monetary policy) and the demand (the flow of capital). China is a good example, taking side C: the Renminbi is soft-pegged to the dollar and the PBoC wields sovereign monetary policy; these necessarily require the existence of capital controls.



The 'impossible trinity' of monetary economics

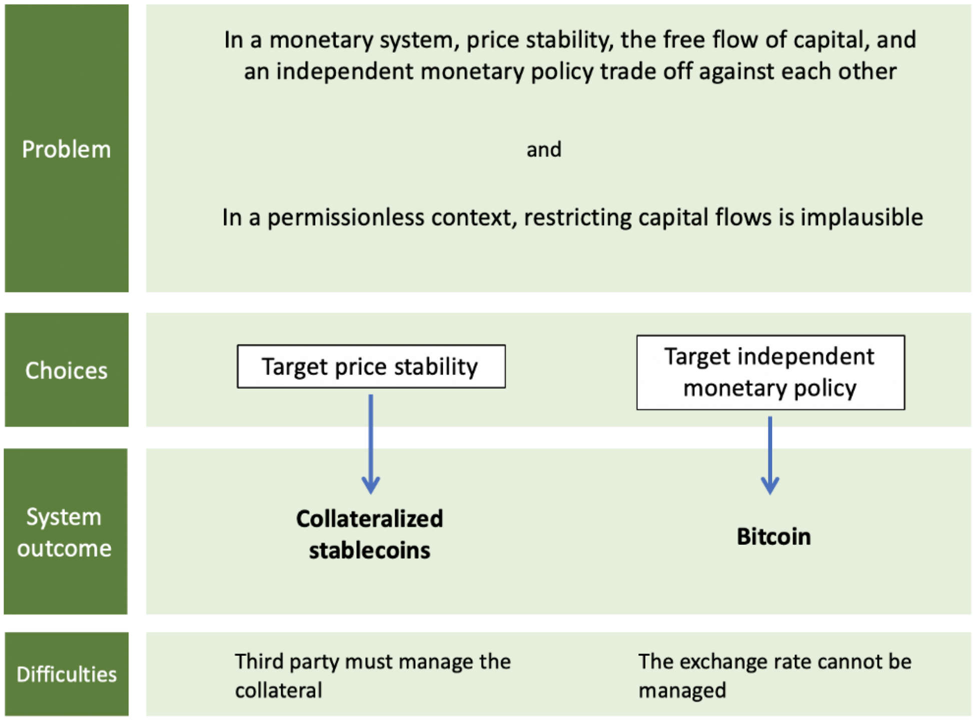
The Bank of England was infamously reminded of this constraint in 1992 when Soros and Druckenmiller realized that its peg with the German Deutschmark was fragile and could not be defended in perpetuity. The BoE had to admit defeat and allow the Pound Sterling to float freely.

A more contemporary example of this constraint is Hong Kong's current travails with its currency which is soft-pegged to the US dollar. Unfortunately for Hong Kong, the US dollar has strengthened considerably in recent years, and so the monetary authority has been faced with the unenviable challenge of meeting an appreciating price target. A capital outflow from HK to the US has compounded the difficulty.

Hong Kong selected option A on the graphic, giving up monetary authority in exchange for a free flow of capital and a pegged exchange rate. If they lose the peg they will regain monetary sovereignty (the ability to untether their interest rate policy from the US Fed's) while retaining open capital flows.

So there is an inescapable tradeoff when it comes to monetary policy. No state, no matter how powerful, is immune to it. If you want to index your currency to that of another state, you either become its monetary vassal, or you undertake the herculean task of stopping your citizens from exporting funds abroad.

So to a monetary economist, the fact that Bitcoin cannot manage its exchange rate should be quite unsurprising. It is an upstart digital nation, designed to render capital easily portable (so capital controls are out of the question), and has no authority capable of managing a peg. Bitcoin is able to exercise extreme supply discretion thanks to its asymptotic money supply targeting, but has no mechanism whatsoever to control capital flows, and naturally has no central bank to manage rates. Compare this to Libra, Facebook's new cryptocurrency, backed by a basket of sovereign currencies. Arguably, it can never become truly permissionless, as some entity must always manage the basket of securities and currencies backing the coin.



Problem	In a monetary system, price stability, the free flow of capital, and an independent monetary policy trade off against each other and In a permissionless context, restricting capital flows is implausible	
Choices	Target price stability	Target independent monetary policy
System outcome	**Collateralized stablecoins**	**Bitcoin**
Difficulties	Third party must manage the collateral	The exchange rate cannot be managed

Bitcoin bites the bullet by letting its exchange rate float freely, opting for a system design with no entity tasked with managing a peg and with sovereign monetary policy. Volatility and future exchange rate uncertainty is the price that users pay for its desirable qualities—scarcity and permissionless transacting. The bullet bitcoin bites is an unstable exchange rate, but in return it frees itself from any third party and wins an independent monetary policy. A decent trade.

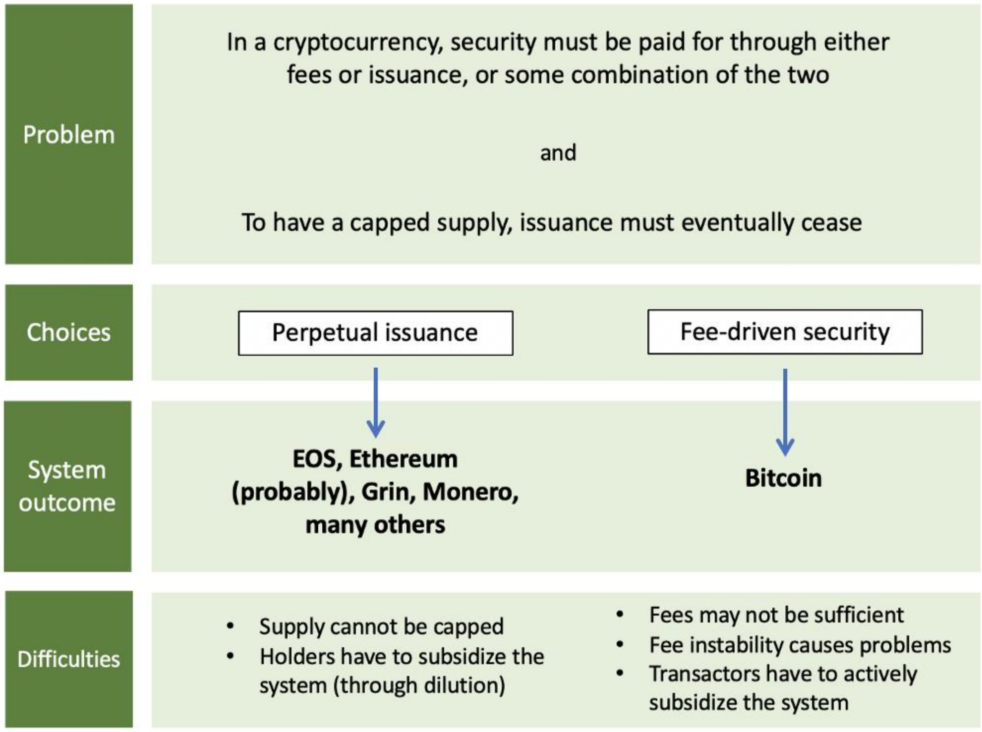
Uncapped/capped supply

One of the most heated debates within the cryptocurrency industry is whether it is possible to have a genuinely finite supply or not. This tends to turn on one's view as to whether fees or issuance should pay for security in the network. So far, no permissionless cryptocurrency has found a cost-free way to secure the network (unless you believe what the Ripple folks have to say…). Since, all things equal, holders benefit from less issuance rather than more, if you believe that transaction fees can suffice to pay for security, you might find a fee-driven security model preferable.

Indeed, Satoshi believed that Bitcoin would have to wean itself from the subsidy and transition entirely to a fee model in the long term:

The incentive can also be funded with transaction fees. [...] Once a predetermined number of coins have entered circulation, **the incentive can transition entirely to transaction fees**and be completely inflation free.

Ultimately, the choice in a permissionless setting, where security must be paid for, is quite stark. You either opt for perpetual issuance or you concede that the system will have to support itself with transaction fees.



Problem	In a cryptocurrency, security must be paid for through either fees or issuance, or some combination of the two and To have a capped supply, issuance must eventually cease	
Choices	Perpetual issuance	Fee-driven security
System outcome	**EOS, Ethereum (probably), Grin, Monero, many others**	**Bitcoin**
Difficulties	• Supply cannot be capped • Holders have to subsidize the system (through dilution)	• Fees may not be sufficient • Fee instability causes problems • Transactors have to actively subsidize the system

Given the popularity of perpetual issuance systems in new launches, a rough consensus appears to be emerging that attaining sufficient volume for a robust fee market to develop is too challenging an objective for an upstart chain.

However, Bitcoin, in typical bullet-biting fashion, selects the less palatable of the two choices—capped supply and a fee market—in order to obtain a trait its users find desirable: genuine, unimpeachable scarcity. Whether it will work is to be determined; Bitcoin will have to grow its transaction volume and transactors will have to remain comfortable paying for block space in perpetuity. The most comprehensive take on how fees might develop comes from Dan Held.

Bitcoin's Security is Fine *Fears over the declining block reward are overblown*
blog.picks.co

While no one quite knows how Bitcoin's fee model will shake out, the fact that Bitcoin has a robust fee market already with fees accounting for about nine percent of miner revenue (at the time of writing) is encouraging.

Frequent/infrequent hard forks

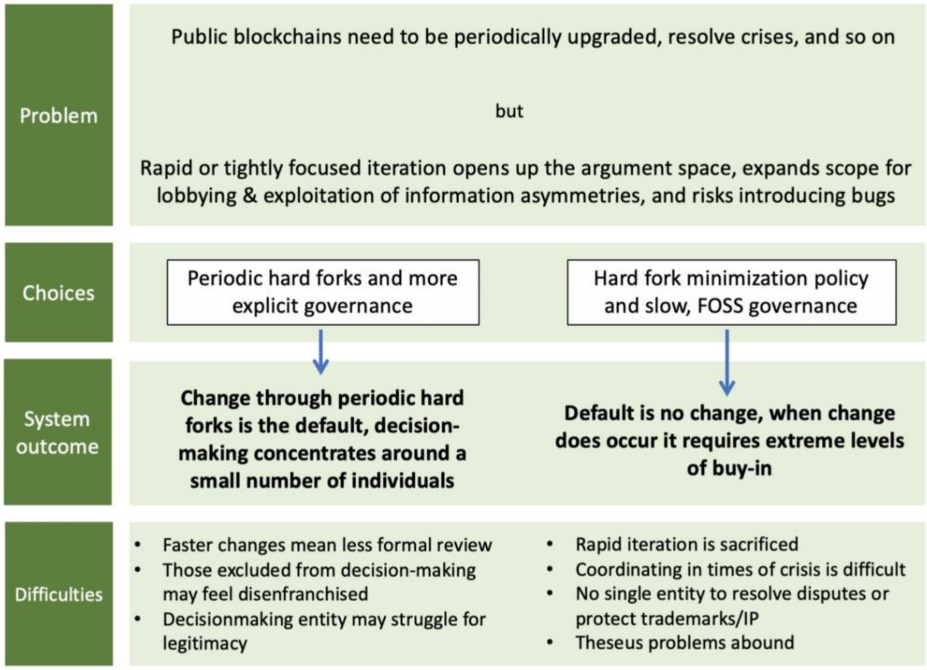
The frequency of forking among cryptocurrencies tells you a great deal about their design philosophies. For instance, Ethereum was positioned as the more innovative counterpart to Bitcoin for a long time, as it had certain advantages like a (functioning) foundation, a pot of money which could be used to finance developers, and a social commitment to rapid iteration. Bitcoin developers, by contrast, have tended to de-emphasize development through forks and generally aim to proceed through opt-in soft forks, like the SegWit upgrade. (By 'hard fork,' I mean intentional backwards-incompatible upgrades that require users to collectively upgrade their nodes. In a hard fork situation, legacy nodes might become incompatible with the new ruleset.)

In my opinion this often comes down to fundamental conflict of visions in how development should be organized; Arjunand Yassine cover the topic well in their essay.

A Conflict of Crypto Visions *Why do we fight? A framework suggests deeper reasons*
medium.com

As stated, some cryptocurrency developers have adopted a policy of regular hard forks to introduce upgrades into their systems. A regular hard fork policy is virtually the only way to *frequently* upgrade a system where everyone must run compatible software. It's also risky: rushed hard forks can introduce covert bugs or inflation, and can marginalize users who did not have sufficient time to prepare. Poorly-organized hard forks in response to crises often lead to chaos, as was the case with Verge and Bitcoin Private. Major blockchains like Ethereum, Zcash, and Monero have adopted a frequent hard fork policy, with Monero operating on a six-month cadence, for instance.

Forking with frequency is, as with many of the design modes in this post, expedient, but it comes with downsides. It tends to force decision-making into the hands of a smaller group—because the slow, deliberative governance style that characterizes Bitcoin Core is ill-suited to rapid action—and it introduces attack vectors. Developers in charge of forking can reward themselves and their inner circle at the expense of users; for instance, by creating a covert or explicit tax which flows to their coffers, or altering the proof of work function so it only works with hardware they own. As with everything in the delicate art of blockchain maintenance, concentrating power comes at a cost.



Problem	Public blockchains need to be periodically upgraded, resolve crises, and so on but Rapid or tightly focused iteration opens up the argument space, expands scope for lobbying & exploitation of information asymmetries, and risks introducing bugs	
Choices	Periodic hard forks and more explicit governance	Hard fork minimization policy and slow, FOSS governance
System outcome	**Change through periodic hard forks is the default, decision-making concentrates around a small number of individuals**	**Default is no change, when change does occur it requires extreme levels of buy-in**
Difficulties	• Faster changes mean less formal review • Those excluded from decision-making may feel disenfranchised • Decisionmaking entity may struggle for legitimacy	• Rapid iteration is sacrificed • Coordinating in times of crisis is difficult • No single entity to resolve disputes or protect trademarks/IP • Theseus problems abound

Something to note is the fact that all blockchains which are more decentralized in their administration suffer from so-called **Theseus problems**. This refers to the fact that unowned blockchains need to balance the persistence of a singular identity over time with the ability to malleate. I discuss the topic at length here:

Bitcoin's Existential Crisis *Cryptocurrencies lack leaders — they have no single source of truth. Philosophically, this can get complicated.* medium.com

Ultimately public blockchains that have no single steward that is responsible for resolving disputes have to face these problems of Theseus. So the option on the right is a painful one. But again, it is a tradeoff that Bitcoin is happy to make.

Discretionary/nondiscretionary monetary policy

If you are an artist or engineer, you may have noticed that restriction is the mother of creativity. Narrowing the design or opportunity space of a problem often forces you to discover an innovative solution. In more abstract terms, if you have more available resources, you are less likely to be careful with how you deploy them, and more likely to be profligate.

Russian composer Igor Stravinsky said it well:

The more constraints one imposes, the more one frees one's self. And the arbitrariness of the constraint serves only to obtain precision of execution.

There is a small but burgeoning literature reinforcing this phenomenon. Mehta and Zhu (2016) investigate the "salience of resource scarcity versus abundance," finding:

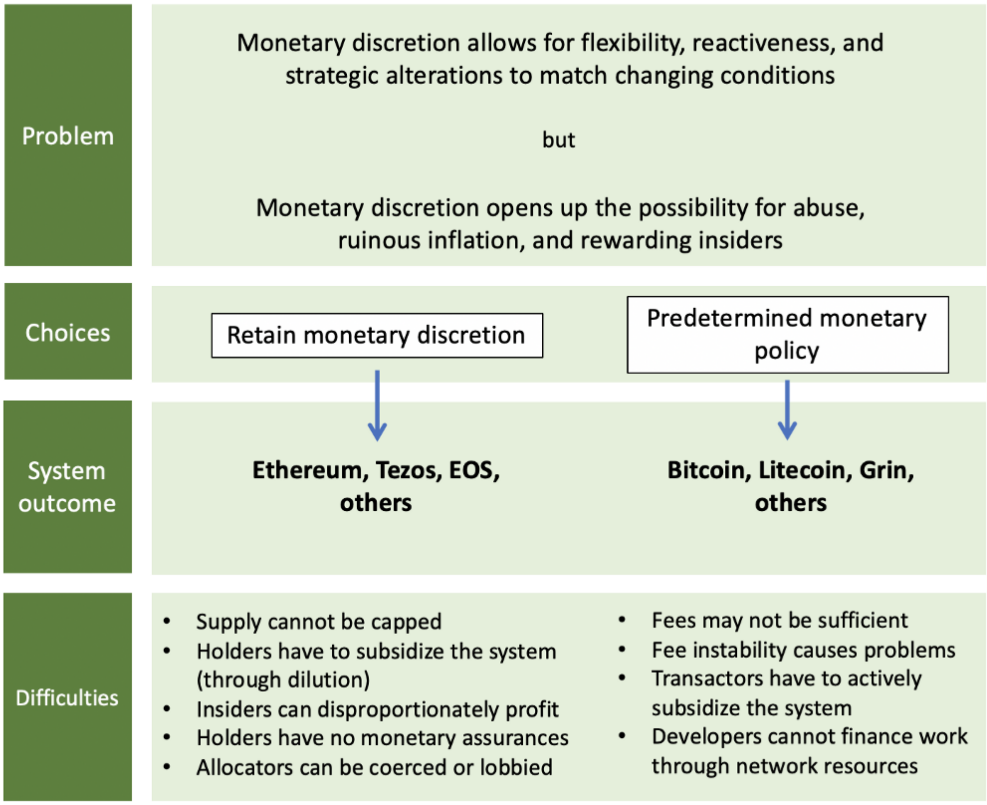
[S]carcity salience activates a constraint mindset that persists and manifests itself through reduced functional fixedness in subsequent product usage contexts (i.e., makes consumers think beyond the traditional functionality of a given product), consequently enhancing product use creativity.

Examples of this phenomenon abound. In venture financing, over-funding a startup often paradoxically leads to its failure. This is why startups are encouraged to be lean—it imposes discipline and forces them to focus on revenue generating opportunities rather than meandering R&D or time wasted at conferences. In more mature companies, an excess of cash often leads to wasteful M&A activity.

I would venture that the same phenomenon holds in the context of nations with regards to their monetary policy. If it is easy to raise capital through dilution (this is essentially how inflation works for sovereign governments), it is easy to finance wasteful ventures, like overseas conflicts. Similarly, in cryptocurrency, discretionary inflation is often presented as a positive—it is often bundled with *governance* and it gives developers the ability to finance operations, marketing, and so on. Quite simply, enabling discretion in monetary policy creates a profound abundance that the project administrators can exploit. This however comes with drawbacks: it opens the door to rent-seeking, exploitation, and wealth redistribution, all of which harm the long-term integrity of the project.

In many cases, monetary discretion—the ability to inflate supply at will when required—is presented as an innovation relative to Bitcoin. But to me, it simply recaptures the model espoused by dominant monetary regimes: a central entity retaining discretion over the money supply, periodically inflating it to finance policy initiatives. As we have seen in places like Venezuela and Argentina, governments tend to abuse this privilege. Why would cryptocurrency developers be any different?

Bitcoin's predetermined supply, a product of its radical commitment to resisting monetary caprice, is its solution to the problem. A grotesque, arrogant solution, to many opponents, but one that is critical to the design of Bitcoin. By holding this variable fixed, and iterating around it, Bitcoin aims to provide lasting, genuine scarcity and eliminate humans from decision-making altogether. This may come at a great cost. Opponents deride Bitcoin's "high" fees, although stable fee pressure will be ultimately necessary for security as the subsidy declines. And unlike nimbler projects, Bitcoin cannot fill its coffers from the spoils of inflation.



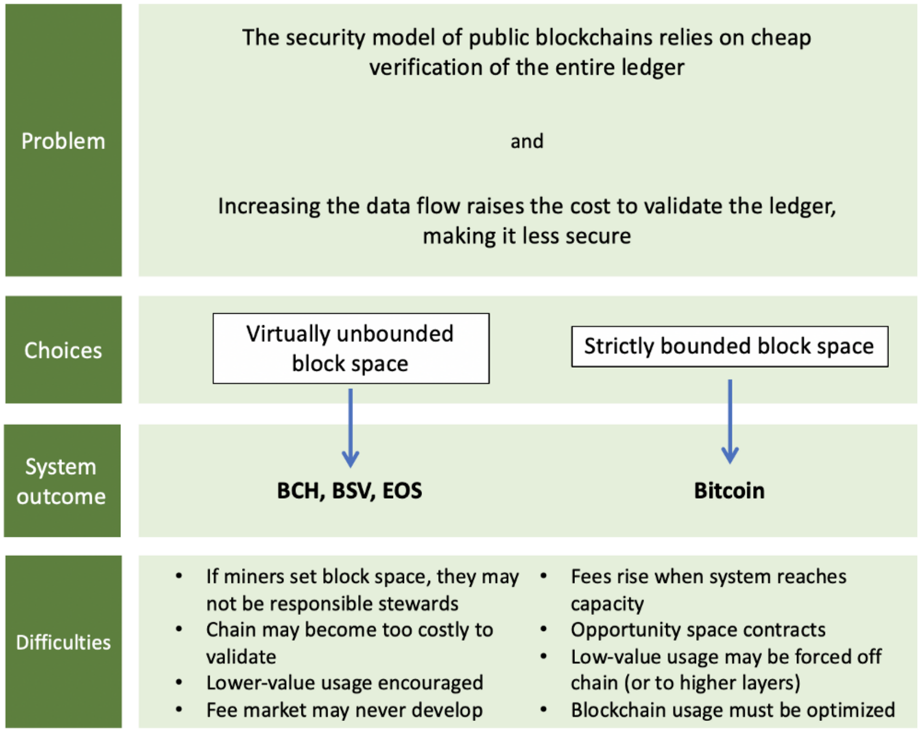
Problem	Monetary discretion allows for flexibility, reactiveness, and strategic alterations to match changing conditions but Monetary discretion opens up the possibility for abuse, ruinous inflation, and rewarding insiders	
Choices	Retain monetary discretion	Predetermined monetary policy
System outcome	**Ethereum, Tezos, EOS, others**	**Bitcoin, Litecoin, Grin, others**
Difficulties	• Supply cannot be capped • Holders have to subsidize the system (through dilution) • Insiders can disproportionately profit • Holders have no monetary assurances • Allocators can be coerced or lobbied	• Fees may not be sufficient • Fee instability causes problems • Transactors have to actively subsidize the system • Developers cannot finance work through network resources

I'll note that some of the projects in the left hand column have not actually arbitrarily inflated supply to achieve policy objectives, but they have essentially written that possibility into the social contract—that supply is a lever which can be pulled if the stakes warrant it.

It is quite simply convenient to reinsert monetary discretion into the system to finance the acquisition of mercenary developers, acquire hype with marketing, and support the operations of a single corporate entity which can allocate resources. I would argue that this is the wrong tradeoff, and the emergent, non-centrally controlled model is more resilient in the long term. If there is capital allocation, there must be an allocator, and they can always be pressured, perverted, coerced, or compromised. Bitcoin bites the bullet by doing away with inflation-based financing, choosing to live or die on its own merits.

Unbounded/bounded block space

The block space debate can also be understood in similar terms to the restricted/unrestricted point made above. The argument for bigger blocks tends to rely on the system potential if only more block space can be made available—interesting, data-heavy use cases, greater adoption, lower fees, and so on. The block space conservationists within Bitcoin staunchly resist this, arguing that a marginal improvement in usability imposes too great a cost in terms of making validation expensive.



Problem

The security model of public blockchains relies on cheap verification of the entire ledger

and

Increasing the data flow raises the cost to validate the ledger, making it less secure

Choices

Virtually unbounded block space

Strictly bounded block space

System outcome

BCH, BSV, EOS

Bitcoin

Difficulties

- If miners set block space, they may not be responsible stewards
- Chain may become too costly to validate
- Lower-value usage encouraged
- Fee market may never develop

- Fees rise when system reaches capacity
- Opportunity space contracts
- Low-value usage may be forced off chain (or to higher layers)
- Blockchain usage must be optimized

The standard proposal in forks of Bitcoin like Bitcoin Cash or BSV is that miners, not developers would set the blocksize cap—well above Bitcoin's effective ~ 2 mb cap (the 1 mb cap is a myth). However, this is problematic, as block space is an *unpriced externality.* It doesn't cost anything to a miner to raise the cap. In fact, larger miners may prefer larger blocks as they disadvantage smaller miners. However, an ever-growing ledger—with all the increased costs of validation that accompany it—imposes a very real cost on *verifiers,* node operators who want to verify inbound payments and ensure that the chain is valid. Miners' incentives are not aligned with the entities that their block sizing affects.

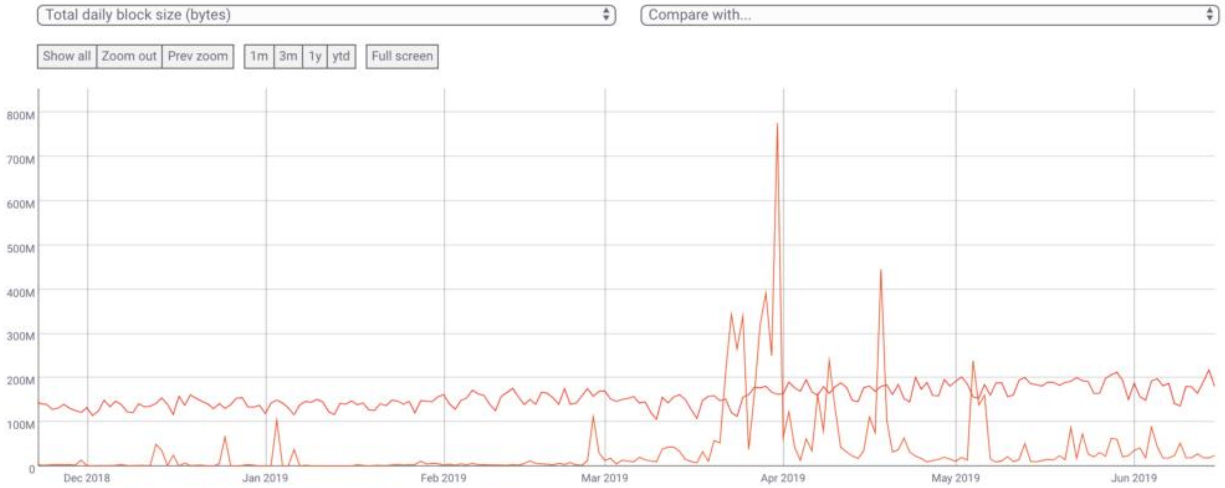
Faced with this externality, Bitcoin opts for what might appear an unpalatable choice: initially capping the block size at 1 mb, now capping it at 4 mb (in extreme, unrealistic cases—more realistically, about 2mb). The orthodox stance in Bitcoin is that bounded block space is a requirement, not only to weed out uneconomical usage of the chain, but to keep verification cheap in perpetuity.

Additionally, simple observations from economics make it clear what the outcome of an uncapped block size will be. Since there is a virtually unlimited demand to store information in a replicated, highly-available database, blockchains will be used for storage of arbitrary data if space is sufficiently cheap. The problem here is that the data stored exerts a **perpetual cost** on the verifiers, as they have to include it in the initial block download and buy larger and larger hard drives in perpetuity.

(Ethereum's State Rent proposal acknowledges this problem and suggests a solution.)

Bitcoiners, far from lamenting 'high' fees, embrace them: making ledger entries costly renders a certain breed of spam expensive and unfeasible.

In chains which commit to completely opening up block space like BSV, you end up with a baseline level of low usage (BSV averages <10k daily active addresses, compared to Bitcoin's 800k+) and occasional inorganic spikes as the chain is injected with data, making validation very difficult in the long term.

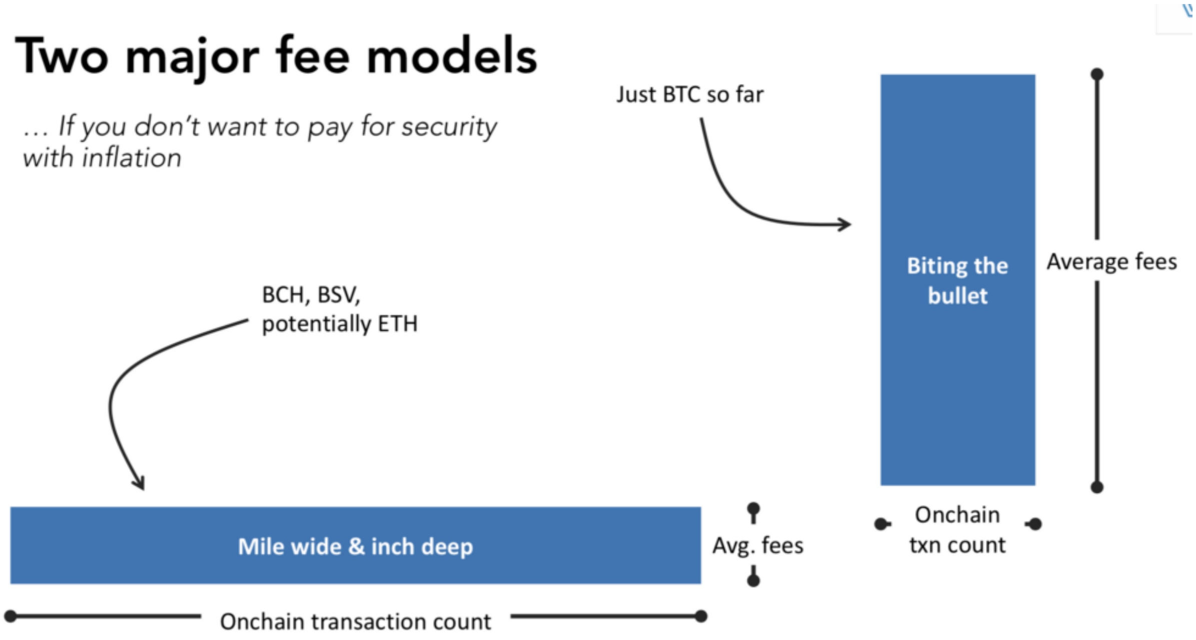


Bytes transmitted on chain per day in Bitcoin (red) vs BSV (orange). Coinmetrics

The case of EOS is an interesting one. Given that block space was made fairly cheap (even though it is technically 'priced' with an elaborate system of network resources), EOS had a lot of uneconomical, or spam usage. This is partly because the incentives to create the illusion of activity on chain were high, and the cost to do so was minimal.

So you had millions and millions of ledger entries created through the weight of economic incentives (to promote the chain or certain dApps), burdening the chain with borderline spam. This has had very real consequences. In EOS today, for instance, it is a badly-kept secret that running a full archive node (a node which retains historical snapshots of state) is virtually impossible. These are only strictly necessary for data providers who want to query the chain, but this is an example of a situation where maintaining the canonical history of the ledger becomes prohibitively difficult through a poor stewardship of network resources.

Lastly, the block space debate comes down to a question of sustainability. For a blockchain to be able to charge fees, users must value the block space. However, if block size is completely unbounded, it stands to reason that block space will be worthless. How much would you pay for a commodity that is infinite in supply? By capping block space, Bitcoin is able to sustain a market for ledger entries which will one day replace the subsidy to miners provided by issuance. Opponents contest that increasing the block size allows for more and more usage, which will eventually manifest itself in fees.



Two major fee models

… If you don't want to pay for security with inflation

Just BTC so far

Biting the bullet

Average fees

BCH, BSV, potentially ETH

Mile wide & inch deep

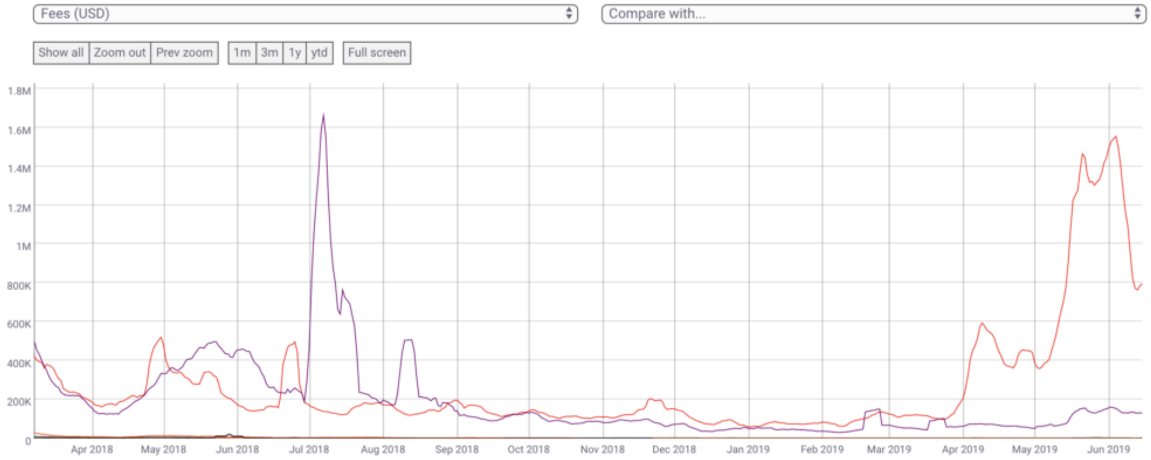
Avg. fees

Onchain txn count

Onchain transaction count

Slide from my talk at the MIT Bitcoin Expo: video here

I call this the 'mile wide and inch deep' model of the fee market. Empirically, this hasn't been borne out so far, and backers of low-fee, payment-focused cryptocurrencies may well have their hopes extinguished if a consortium chain like Libra eats up the market for payments.



Daily fees (USD) paid to miners for a variety of top blockchains. Coinmetrics

Aside from Bitcoin and Ethereum, no asset even registers on the chart. Only Litecoin can muster over $1k per day in fees. BCH, BSV, Dash, Zcash, Monero, Stellar, Ripple, and Doge are all in the hundreds of $ /day range (chart). This does not bode well for the sustainability of coins which plan to reduce their issuance on a schedule like Bitcoin's. Currently, no chains aside from Bitcoin and Ethereum appear equipped to enter a regime where fees provide the majority of validator revenue. So pricing block space and allowing a market to develop, although painful in terms of fees, is a critical feature of Bitcoin.

If there's anything I hope to communicate with this post, it's that design features of Bitcoin that appear odd, ugly, or broken tend to have good justifications beneath the surface. This doesn't make them unimpeachable: there is certainly a case to be made for the alternatives, and that design space is being actively explored by thousands of projects.

Satoshi was not an all-seeing savant, and s/he certainly failed to anticipate some of the ways the system would develop, but the tradeoffs that ended up in Bitcoin are generally quite defensible. Whether they are absolutely correct remains to be seen. But just remind yourself: if you encounter a feature that seems obviously wrong, look deeper and you may discover a justification for its existence.

Thank you to Allen Farrington and Matt Walsh for the feedback.

Bitcoin Average Dormancy

New Views of a Classic On-Chain Metric

By David Puell & Reginald Smith

Posted June 20, 2019

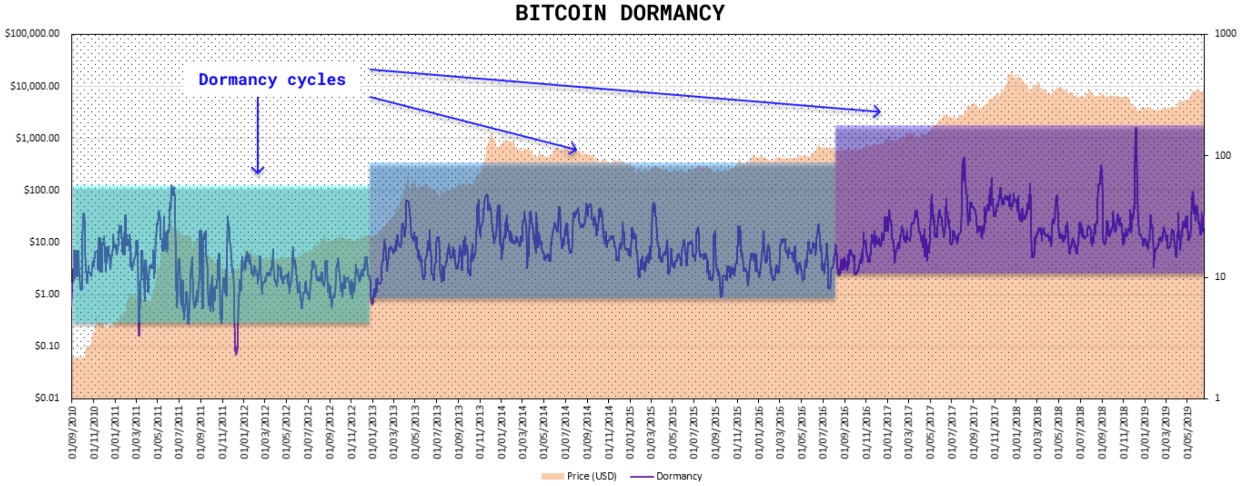
Download Reginald's research paper: Bitcoin Average Dormancy

Disclaimer: Nothing here should be considered trading or investment advice.

So what is average dormancy (or simply, "dormancy")? First proposed by this article's co-author Reginald Smith in 2018, it has not been given enough attention relative to its importance as one of the foremost metrics of BTC's long-term economic health. In summary, dormancy is the average number of days destroyed per coin transacted in any given day, as per the following formula:

$$Dormancy = \frac{Destruction}{Volume}$$

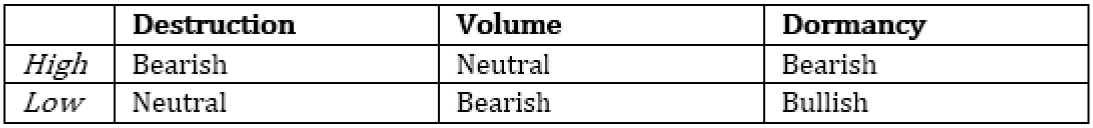
Here, destruction equals the total number of coindays destroyed, and volume equals the total number of coins transacted through the blockchain (and not at exchanges). This ratio describes the average number of days each coin transacted remained *dormant*, unmoved. The higher the dormancy, the older the coins transacted that day are on average, and the more old hands are releasing their bitcoins into circulation. In other words, average dormancy refers to *spent or realized* destruction relative to transactions.



Fearful Symmetry: Accumulation and Distribution

As pointed out in dormancy's original paper, on-chain destruction and on-chain volume equate to being perhaps the two most important metrics of Bitcoin's economic state; the reason being that, especially when compared as a ratio such as dormancy, they describe the state of what smart money is doing in the market at any given time—accumulation or distribution. Based on first principles, the following assumptions emerge:

1. Accumulation describes the act of smart money (last-resort buyers) taking cheap coins from dumb money (panic sellers), while distribution describes the act of smart money (old hands) releasing expensive coins into the hands of dumb money (bag holders). Accumulation occurs at market bottoms and distribution occurs at market tops.
2. Destruction describes the actions of mostly a single market actor: old hands selling or spending their bitcoins. Volume describes the actions of two market actors: buyers and sellers dealing with investor flows at different prices.
3. High destruction is bearish (old smart holders releasing coins into circulation) and low destruction is neutral (since in itself it implies holders are maintaining their position but not necessarily that buyers are coming in). High volume in itself is neutral (high number of transactions between both buyers and sellers) and low volume is bearish (confirming no demand for the asset as per a lack of buyer's activity). From the above, the following simplified matrix emerges:



	Destruction	**Volume**	**Dormancy**
High	Bearish	Neutral	Bearish
Low	Neutral	Bearish	Bullish

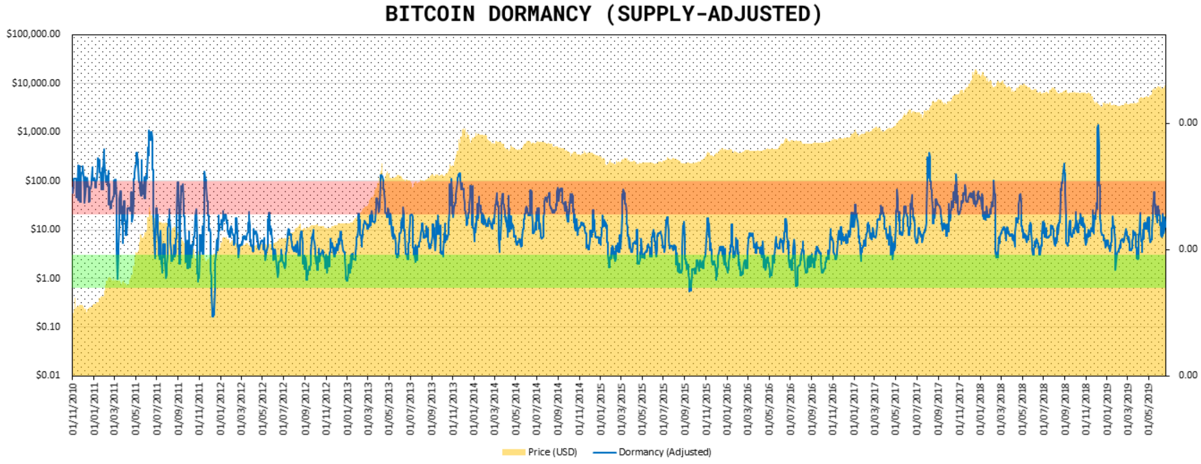
Dormancy integrates all these narratives into a single metric, by comparing both ratio components at all times, and displaying them in a simple oscillation by which, on a trending basis, high dormancy is bearish and low dormancy is bullish.

Supply-Adjusted Dormancy

Since the age of the market allows for an ever-increasing amount of destruction (the numerator of average dormancy), adjusting for supply (an increasing creation of minted coins) in the denominator seems to provide a clearer, more proportional historical oscillation that helps best visually detect the health of the market—or, in this case, dormancy per coin, calculated as follows:

$$Dormancy(Adjust.) = \frac{Destruction}{Volume \cdot Supply}$$

This formula produces the chart below:



DUA Ratio (by Reginald Smith)

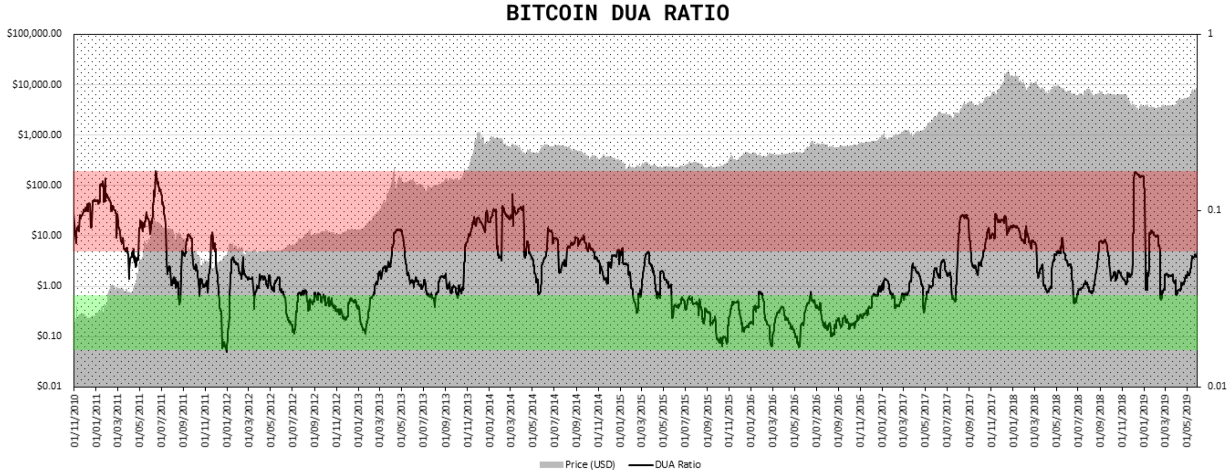
Just as with pure transaction volume and its variants like NVT Ratio, NVT Signal, or Network Momentum, the dormancy concept has opened the door into a new inflow of indicators for long-term Bitcoin market diagnostics. What follows are two examples of this.

Dormancy-to-UTXO-Age Ratio measures the relation between dormancy and the average age of all UTXOs at any given time, calculated by taking the ratio of average dormancy of the last 30 days between the average of all HODL waves in existance, as follows:

$$DUARatio = \frac{\sum_{30d} Destruction \div \sum_{30d} Volume}{\sum_{HODLWaves}(WaveMedianDays \cdot WavePercentage)}$$

In which median days represents the median time of the HODL wave age band, and wave percentage represents the percentage of UTXOs in any given age band. In this particular case, both coindays destroyed and on-chain volume are aggregated throughout 30 days to smooth out the dormancy numerator.

Since dormancy measures the average holding time of continuously on-chain trading Bitcoin, the average age of UTXO, which includes bitcoin both in the HODL and lost states, is always longer—so average dormancy is always less than the average age of UTXOs. Therefore, the ratio is always less than one.



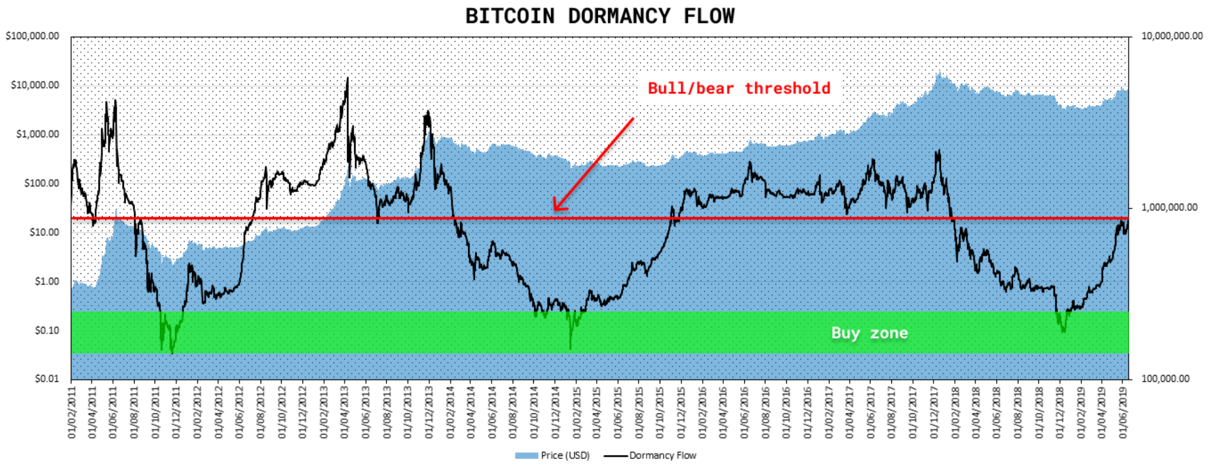
In periods where long-term holders accumulate (HODL) Bitcoin, the average dormancy is low and the average age of UTXO increases, lowering the ratio. When long-term holders offload their holdings to short-term traders, the average dormancy increases and the average age of UTXO decreases, raising the ratio. This tool is therefore useful in identifying market trends that often lead to HODL waves detecting periods of bitcoin selling by long-term holders in bull markets, and then re-accumulation after the onset of the bear market when the UTXO average age begins to rise and dormancy once again drops.

Dormancy Flow (by David Puell)

Another attempt at capturing phases in BTC's market cycles, dormancy flow is calculated by dividing current market capitalization by annualized dormancy value (USD), as follows:

$$DormancyFlow = \frac{MarketCap_{USD}}{365^{MA}(Dormancy \cdot Price_{USD})}$$

Dormancy flow provides the following chart, ideal for both bottom-catching historical global lows and assessing whether the bull market remains in relatively normal conditions:



Whenever network value remains high relative to the yearly moving average of its realized dormancy in USD, the bull market can be considered as “healthy,” since price remains high relative to the market’s annualized spending behavior. Whenever dormancy value overtakes market capitalization at lowest longitudinal levels, the market can be considered in full capitulation—a good historical buy zone.

Caveats

1. Destruction (dormancy’s numerator) is prone to false signals on daily variance. The most prominent example of this is last December, when the Coinbase exchange moved nearly 5% of Bitcoin’s total supply. To avoid misinterpreting these false positives, it is recommended to best use dormancy by looking at continuous trends in the oscillator (smoothed by medians or moving averages) as opposed to its daily noise.
2. Just like with NVT and other on-chain metrics, dormancy should be viewed with an increasing caution for major fundamental shifts in detecting on-chain activity. Several recent or future developments in the Bitcoin ecosystem will ultimately contribute, at different stages and in different degrees, to a loss of power in the signals provided by these indicators. Examples of this may include: concentration of speculative liquidity in BitMEX and other exchanges, new custody solutions for institutions, the Lightning Network, sidechains, among others.

Acknowledgements

Many thanks to Willy Woo, Adam Taché, and Murad Mahmudov for their invaluable input and support in the improvement of this piece.

Sources and Data

1. Smith, Reginal D. "Bitcoin Average Dormancy: A Measure of Turnover and Trading Activity." Ledger, February 2018.
2. *CoinMetrics.io* : Coindays destroyed, transaction volume, supply, and price data.
3. *Unchained-Capital.com*: HODL waves data.

Authors

1. Reginald Smith, independent researcher.
2. David Puell, Head of Research @Adaptive Capital.

Bitcoin is the Antivirus (Mushroom Medicine)—Part 3/4

By Brandon Quittem

Posted June 20, 2019

- Part 1 - Bitcoin is a Decentralized Organism 1/4
- Part 2 - Bitcoin is a Social Creature
- **Part 3 - Bitcoin is the Antivirus**
- Part 4- To Be Posted

We've all heard the incredible potential of a Bitcoin future. I'm certainly on board for sound money and social scalability.

However, this drama will take decades. What if Bitcoin doesn't survive long enough to realize it's full potential?

Thankfully Satoshi learned from failed attempts at private money. Bitcoin's genetic code was engineered for maximum survivability.

In this article, we're going to explore the fertile macro environment and Bitcoin's survivability through the lens of fungi.

Honey Bees, Varroa Mites, and Mushroom Medicines

In 1997 a curious Mycologist by the name of Paul Stamets observed a unique behavior demonstrated by honey bees. The bees went out of their way to consume water containing mushroom spores. "Hmm that's interesting" thought Paul.

15 years later, Paul started to connect the dots. Honey bees were dying at an unprecedented rate due to colony collapse disorder (CCD). The bees were dying in part, by infestations of Varroa Mites which transmit deadly viruses such as Deformed Wing Virus and Lake Sinai Virus.

Chemicals used in modern agriculture poisoned the bees so their immune systems are too weak to fend off the Varroa Mites. As bees travel around they spread the Mites to all nearby bees leading to a 70% decline in Bee populations since 2005.

Who cares about the bees?

Bees are a bedrock species responsible for pollinating a large percentage of our food sources (avocados, almonds, etc). If we lose the bees, there are countless downstream effects such as lost jobs, destroyed ecosystems, and reduced food security.

(Image source)

Back to our mycologist Paul, who in 2012 made a monumental realization: fungi are known to support immune systems—the bees must have instinctively known to drink the fungal water. Paul tested his hypothesis and soon after demonstrated that using a simple antivirus "mushroom medicine," we can reduce the effects of Deformed Wing Virus / Colony Collapse by 80%.

Our current monetary regime is the Varroa Mite

Our current central banking based monetary regime is just like the pesky Varroa Mites attacking our financial markets.

- Varroa Mites are hard to kill—fiat currency regimes benefit from a monopoly on violence
- They spread viruses on everything they touch—market distortions, cronyism, regulatory capture
- Negative downstream effects—capital misallocation, increased time preference, limits human productivity, increases risk of catastrophe.

Bitcoin is the antivirus (mushroom medicine) that "saves the bees."

Bitcoin (mushroom medicine) prevents the spread of our destructive financial hegemony (Varroa Mites) which will usher in a new era of human achievement (saving the bees has secondary effects such as ensuring food security).

Heading into the Great Unknown

We're heading into a period of uncertainty never before witnessed by our civilization. The fiat money experiment is on shaky ground and our social systems are beginning to break down.

Globally, we're facing unprecedented debt-to-GDP levels. The Fed, European Central Bank, Bank of Japan, and the Bank of England now appear to "own a fifth of their governments' total debt." Central banks are running out of moves.

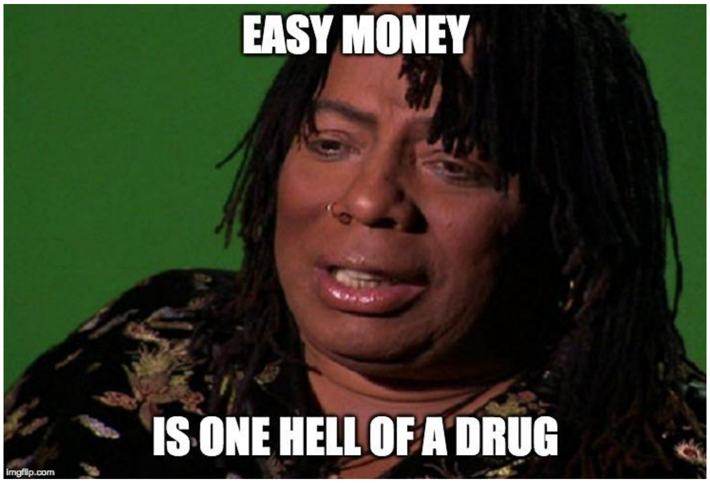
In a last ditch effort, European Central Banks are pushing negative interest rates. Are we really going to allow the hegemonic banking system to CHARGE depositors for storing our digital fiat in their insecure panopticon banks?

How about China?

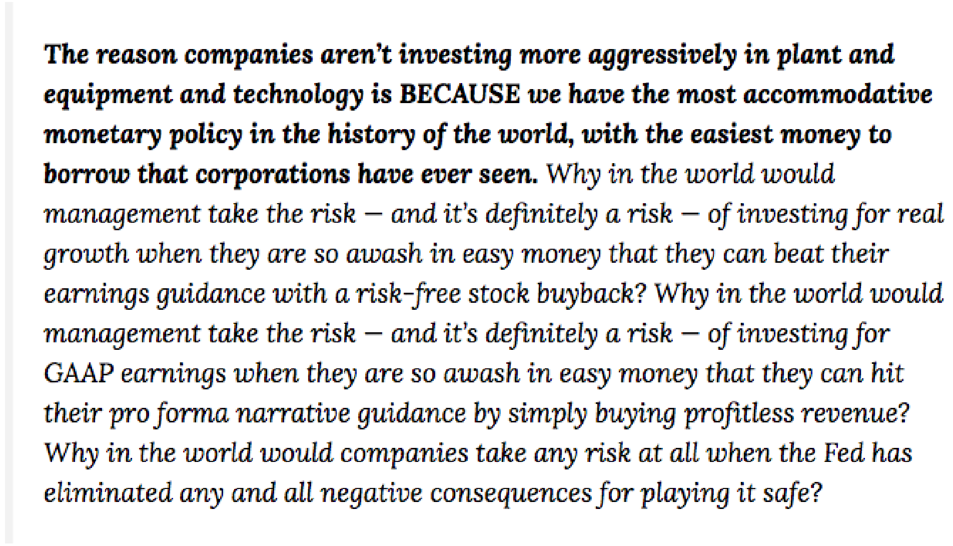
China's real estate market is shaky and long overdue for a correction. Capital controls and seeking yields in a cooling economy have led to inflated real estate prices in China. What happens when the market corrects and everyone rushes for the door? Better have a plan ₿.

And the US?

The US is currently over $22 Trillion in debt, however don't expect the US to default on their obligations. Former Fed chairman Alan Greenspan said "the United States can pay any debt because we can always print money to do that."



In an enlightening article titled This is Water, Ben Hunt explains how artificially suppressed interest rates (easy money) lead to decreased productivity and a zombification of our financial markets. This same pattern foreshadowed the 08/09 financial collapse.



> ***The reason companies aren't investing more aggressively in plant and equipment and technology is BECAUSE we have the most accommodative monetary policy in the history of the world, with the easiest money to borrow that corporations have ever seen.*** *Why in the world would management take the risk — and it's definitely a risk — of investing for real growth when they are so awash in easy money that they can beat their earnings guidance with a risk-free stock buyback? Why in the world would management take the risk — and it's definitely a risk — of investing for GAAP earnings when they are so awash in easy money that they can hit their pro forma narrative guidance by simply buying profitless revenue? Why in the world would companies take any risk at all when the Fed has eliminated any and all negative consequences for playing it safe?*

Social structures are showing weakness

Countries around the world are seeking to eliminate physical cash. Cash is a fundamental tool for privacy and is a requirement to maintain an open society. Without physical cash (or Bitcoin), citizens are at the mercy of the financial surveillance machine. A slippery slope indeed.

Can't forget China's Social Credit System. Soon China's surveillance technology will be exported all around the world.

Young people don't trust their governments or financial institutions. 40% of Americans cannot afford an unexpected $400 expense. No wonder potential Democratic nominee Andrew Yang is gaining steam in the polls while campaigning for Universal Basic Income.

An uncertain future is a perfect substrate to breed extremism. Democratic Socialism, Modern Monetary Theory (MMT), Negative Interest Rates Policy (NIRP), the war on cash, widespread consumerism, and mounting student debt are merely symptoms of a derelict regime.

Our legacy institutions are simply not equipped to deal with the complexity of the information age.

Current attempts to fix the political-economical machine from the inside are unironically powered by the "waste heat of war machine" (h/t Vinay Gupta). We need a systemic change. Something cut from a different cloth.

What if a sound money regime (Bitcoin) is an antidote to the madness?

It is my hope that in the future, we'll look back on our current "fiat banking experiment" with disgust. How could we live under such an archaic regime for so long?

Just like fungi transforms dead and dying organic matter into new life, Bitcoin will transform our decrepit banking system into a robust financial foundation upon which new growth can occur.

The Great Filter of Cryptocurrencies

Can bitcoin survive long enough to reach its full potential?

Cypherpunks, Anarchists, and Voluntarists have been trying to create private, non-government money for a very long time. In fact, modern attempts date back more than 30 years, since the early days of Chaumian Ecash, to E-gold, and B-Money.

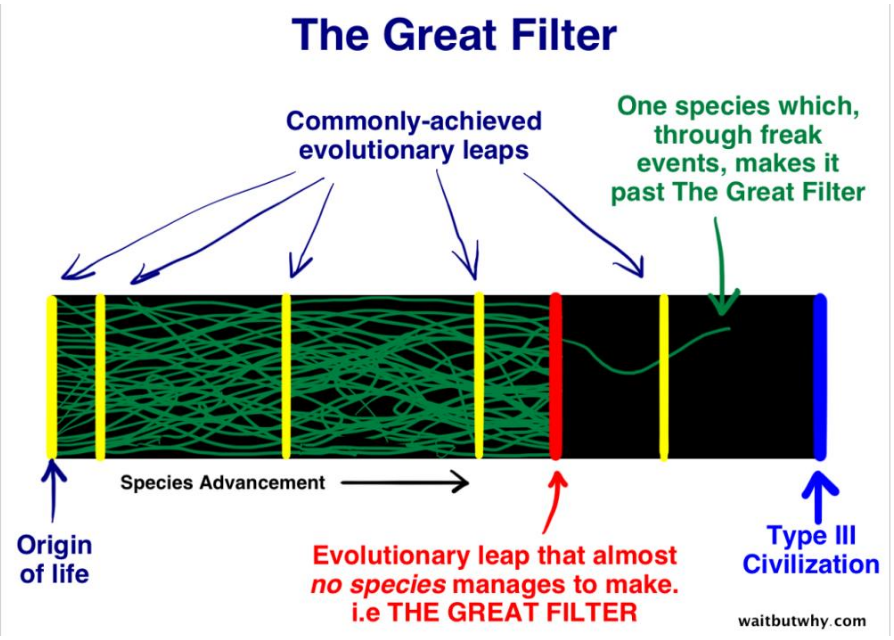
Despite moderate success of private money before Bitcoin, eventually they were all shut down by overreaching governments and/or business interests.

The Great Filter Theory

The Great Filter theory was developed after noticing our lack of success finding intelligent life in the universe. Where is everybody?

The theory predicts: during life's evolutionary process, there are some obstacles that are extremely unlikely or impossible for to overcome. That obstacle is "The Great Filter."

For example, what if every time an advanced civilization created nuclear bombs it ended up destroying itself? In this scenario, it might be statistically improbable to survive long after inventing nuclear weapons.


The Great Filter
Commonly-achieved evolutionary leaps
One species which, through freak events, makes it past The Great Filter
Species Advancement
Origin of life
Evolutionary leap that almost *no species* manages to make. i.e THE GREAT FILTER
Type III Civilization
waitbutwhy.com

(Source: The Fermi Paradox by Tim Urban which is my favorite blog)

For Cryptocurrencies, The Great Filter is surviving nation-state level attacks.

Bitcoin is the only monetary species that has a chance of surviving the great filter. *More on this below.*

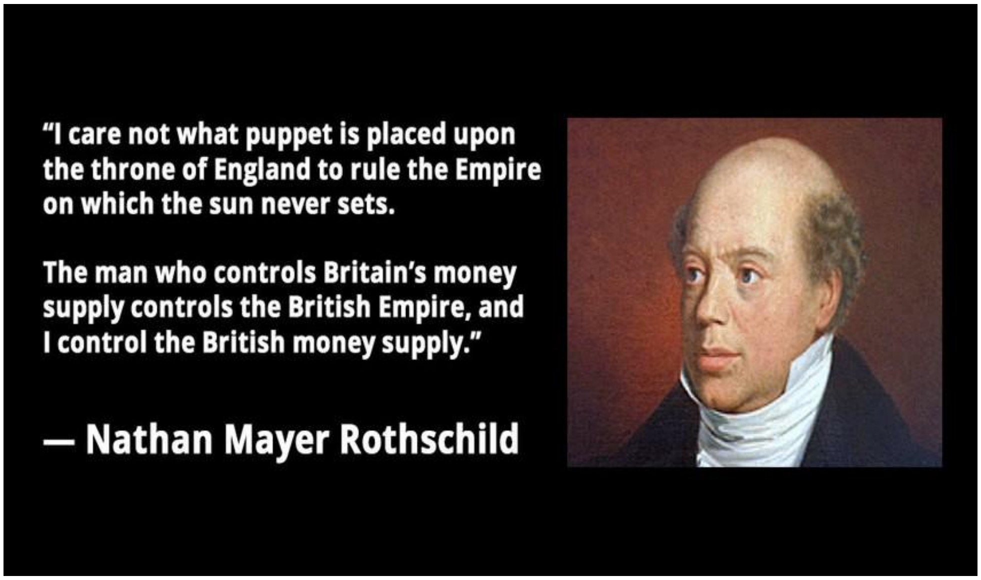
Why would a nation-state or entrenched business want to attack a competitive form of money?

In short: he who has the gold, makes the rules.

The two main benefits of controlling the money supply are the ability to inflate the money supply (shadow tax) and the Cantillon effect .

The Cantillon effect describes the uneven expansion of the money supply. When the central bank prints new money, those closest to the money (banks and big corporations) profit from new “cheap money.” By the time the rest of the population receive the new money, price inflation has already begun.

The Cantillon effect results in a wealth redistribution from the poor to the rich.



“I care not what puppet is placed upon the throne of England to rule the Empire on which the sun never sets.

The man who controls Britain’s money supply controls the British Empire, and I control the British money supply.”

— Nathan Mayer Rothschild

The government goes to great lengths to protect their monopoly

Like E-gold in the 1990s, any competing cryptocurrency can thrive in times of peace. However, when sufficiently agitated, those in power will lash out to protect their interests. History is littered with examples.

Between 2006–2008, the US government expanded the definition of the ‘money transmitter license’ (under the Patriot Act) to target E-gold. In its peak, E-gold was processing over $2B worth of purchases per year. Unfortunately, the US government took advantage of the centralized nature of E-gold, busted down the door, and shut it down.

Moral of the story? Governments do not like competition.

In fact, Congressman Sherman from California recently called for a complete ban of Bitcoin. Sherman is surprisingly enlightened. He understands Bitcoin's true mission: Creating a new global base money that cannot be weaponized by the global superpower du jour.

Today in Congress Rep. Sherman called for a bill to ban all cryptocurrencies. This is why Coin Center is needed in DC now more than ever. -@coincenter

Time For a New Strategy: Be Unstoppable

In 1984, famous Austrian Economist, Friedrich August von Hayek, unknowingly laid the foundation of Bitcoin's evolutionary strategy: be unstoppable.

"I don't believe we shall ever have a good money again before we take the thing out of the hands of government, that is, we can't take it violently out of the hands of government, all we can do is by some sly roundabout way introduce something that they can't stop."—Friedrich Hayek

With chilling foresight, Hayek predicted Bitcoin some 25 years prior.

Satoshi obviously read Hayek and he understood "The Great Filter of Cryptocurrencies"

In 2009 Satoshi Nakamoto released an implementation of Hayek's "unstoppable money." From day one, Bitcoin was engineered to survive "The Great Filter."

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

In order for the full potential of Bitcoin to be realized, it needs to be so resilient that even nation state level actors cannot successfully kill Bitcoin. This meant preventing any party from having full control over the system.

Parallels with Fungi: the most resilient species on our planet

Ancient mushrooms called Prototaxites

Over 1.3b years of evolution, fungi have perfected the art of staying alive. Unlike plants, fungi do not rely on sunlight, instead they find/create their own food. Fungi do not have a centralized point of failure making them resilient to attacks. When sufficiently perturbed, fungi steal genetic code from their ecological neighbors (Horizontal Gene Transfer).

Since complex life evolved on our planet, we've experienced 5 great extinction events where 75–96% of all life on earth perished.

During each cataclysmic event, fungi inherited the earth due to their anti-fragile nature. In an effort to survive "the great filter," Bitcoin mimics effective evolutionary strategies observed in the fungi kingdom.

Can Bitcoin Survive "The Great Filter?"

How could you kill bitcoin? Turn off the internet? Make it illegal to use? Tax it to hell?

Any cryptocurrency that cannot (feasibly) survive a nation-state level attack is pointless. Simply delaying their inevitable demise.

Satoshi designed the Bitcoin super-organism to survive "The Great Filter" and to resist corruption. This lofty goal kick-started an evolutionary path separating bitcoin from all the other cryptocurrencies and "blockchain projects."

Does this mean Bitcoin is guaranteed to survive the great filter?

Not necessarily. It's impossible to know until the day it suffers a coordinated attack by a state-level actor. However, Bitcoin is the only existing cryptocurrency that stands a chance. Let's explore some positive trends in Bitcoin's survivability toolbox.

- **Bitcoin is unregulatable**. No one person or entity in charge. Code is free speech. Each country has their own competing jurisdiction.
- **Game theory protects Bitcoin from a global coordinated attack.** Nation states compete with each other. Unlikely to see top nations cooperate. If the US bans BTC, China has incentive to adopt. Nations not benefiting from the current USD regime have incentive to adopt BTC.
- **Bitcoin's PoW protects the ledger with an "energy shield."** By anchoring Bitcoin to real economic value (energy), the only way to change the ledger is to "re-do all the work" aka spend the same amount of money in the form of electricity. h/t @danheld
- **Bitcoin inspires a religious fervor from its supporters**. Ideologically motivated "hardliners" act as an immune system. Surviving the scaling wars (NYA/S2X) demonstrates this. Bitcoiners "provide cover fire" until Bitcoin gets through the door. (h/t Bitcoin Sign Guy)
- **Bitcoin can route around ISP censorship.** Bitcoin has a growing network of alternatives to the mainstream internet (mesh networks, HAM radios, and satellites). Maybe even routing transactions through a mycelial network(theoretically possible).
- **Bitcoin is an idea, ideas are eternal.**Bitcoin spreads like a mind virus. Even if somehow the current form was "killed," the idea will live forever. "This Snow Crash thing—is it a virus, a drug, or a religion?" Juanita shrugs. 'What's the difference?'" h/t @nealstephenson
- **Bitcoin's privacy improvements reduce taxability.**CoinJoins and other privacy technologies will minimize the ability for governments to attack Bitcoin through predatory tax legislation. Thank you @wasabiwallet @SamouraiWallet
- **Bitcoin minimizes the ability to cheat.** Bitcoin doesn't rely on trust. Think "can't be changed" instead of trusting that a system "won't be changed." Bitcoin recognizes leaders, formalized governance, and concentration of power as attack vectors waiting to be exploited.
- **Nation states underestimate Bitcoin.** This buys time for Bitcoin to get stronger + harder to kill. The hegemonic banking system is digging their own grave with shovel made of 100% pure hubris. If only we had a ₿ackup plan

So far, we haven't seen any serious state level attack on Bitcoin. However, if Bitcoin continues to absorb value there is an incentive to attack it. In the future, we'll call this period in Bitcoin's life the "great peace."

Alternative Game Theory: Honey Badger Lives Here

Bitcoin only needs to convince a few super powers that the reward of adopting it outweighs the risk of attacking it.

This game theory is similar to having a sign in front of your house that says “Security system installed” or “big angry dog lives here.” Doesn’t matter if you actually have a dog or security system, the threat alone acts like a deterrent to would-be attackers.

Bitcoin has a sign in the front yard that says “Beware of Honey Badger.” This sign reminds nation states that they cannot easily kill Bitcoin.

If nation-states attempt to destroy their monetary competition, they’ll highlight the very need for bitcoin in the first place. And yet, the longer they wait, the stronger Bitcoin becomes.

The “Blockchain Industry” is a Red Herring

First, it’s important to understand that blockchainers, stable coiners, security tokenizers, and corporate chainers do NOT compete with Bitcoin. They taxonomically branched off and are attempting to satisfy a separate niche.

By and large, the “blockchain industry” is a Red Herring, leading businesses and governments to false conclusions. It serves as a distraction and unwillingly provides cover fire for Bitcoin.

Does that mean we should shun the blockchainers? No. They simply mistake Blockchain Hype (Mushroom) for Bitcoin (Mycelial Network).

We should first attempt to educate them as most people were not born Bitcoiners. That being said, deliberate scammers deserve to be flamed.

How the “blockchain industry” helps Bitcoin…

Blockchainers tie up government resources, train future developers, confuse incumbent businesses, and lull banksters to sleep.

Banks like JP Morgan will train hundreds of blockchain developers. Eventually they’ll discover Bitcoin and say goodbye to boring bank coin & and instead join the peaceful revolution. JP Morgan is funding their own demise? How poetic.

Zuckerberg will soon put a “crypto wallet” in everyone’s pocket. Instead of competing with Bitcoin, ZuckBucks may actually attempt to compete with USD. Either way, it gets people comfortable with non-state money on their phone similar to WeChat and Alipay. The first widespread censorship of ZuckBucks will nicely demonstrate the need for BTC in the first place.

Blockchainers and scammers claim Bitcoin is old and can't scale. It's Beanie Babies and myspace. They paint Bitcoin has a friendly, but limited-use fungus, that "brought us the blockchain."

While the blockchain zeitgeist chases their tail, Bitcoin is quietly growing underground, fusing with the "roots" of the legacy finance system, building resilience, recruiting volunteers, infecting curious minds like a cordyceps mushroom, and preparing for "The Great Filter."

If we're lucky, Blockchainers will distract global superpowers just long enough for Bitcoin to become "too big to fail."

Let's Wrap Up

Did you enjoy part 3? Part 4 is coming out soon where we will explore Bitcoin as a catalyst for human evolution. Here's Part 1 and Part 2 in case you missed them.

Part 4 teaser: Let's assume Bitcoin fulfills its destiny as the global monetary base. What are the effects of unleashing a globally accessible, technologically advanced, open, ideal money? Bitcoin enables humanity to reach the heavens. Bitcoin is space money. Bitcoin is the renaissance.

Follow me here on medium and twitter to be notified when part 4 is released. Come say hello on twitter, my DMs are open.

Thanks for reading, Brandon

PS: Lots of people have asked for resources to learn more about fungi.

- I suggest watching Paul Stamets on Joe Rogan's podcast.
- If you only have 17 minutes, check out Paul Stamets TED Talk:6 Ways Mushrooms can Save the World.
- Curious how the forest communicates? Radiolab's Free Tree to Shining Tree

Acknowledgments:

- Thanks to Nic Carter,Gigi,Robert Breedlove, and Danielle Diamond for reviewing earlier drafts.
- Thanks to the Bitcoiners who supports these wacky ideas.
- Thanks to everyone who tags me in fungi related content on Twitter (I really do love this)

- Thanks to Paul Stamets for inspiring my love for Mycology. The Bitcoin community welcomes you whenever you're ready.

Tweetstorm: The Bitcoin Common Tongue

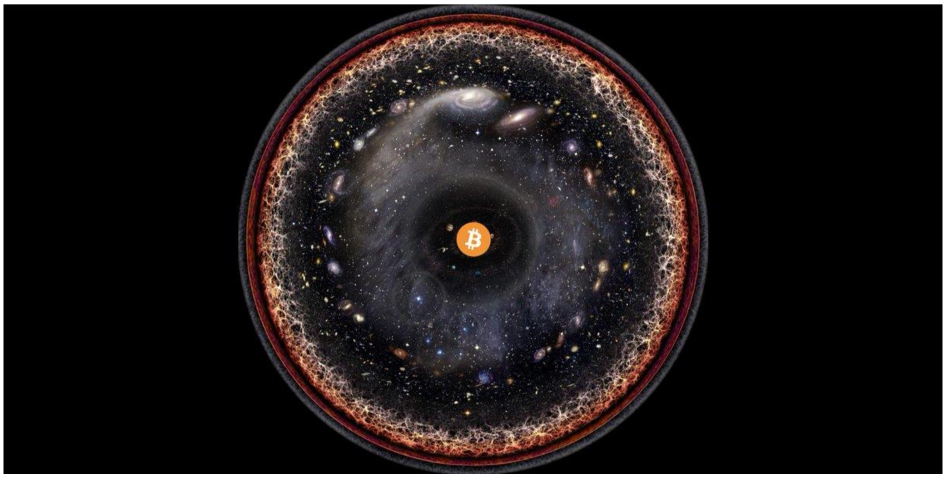
By Robert Breedlove

Posted June 20, 2019

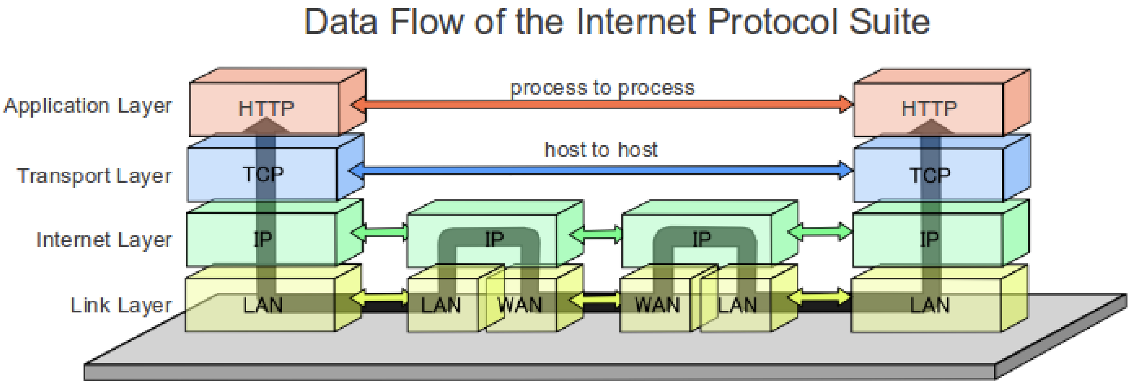
1/ As ambassadors of #Bitcoin, I believe we must speak the common tongue and avoid esoteric language so that our message can penetrate minds far and wide. Here, I will shed some light on the Bitcoin and cryptoasset universe in an exoteric nutshell. Let's begin…

Thread ⬇

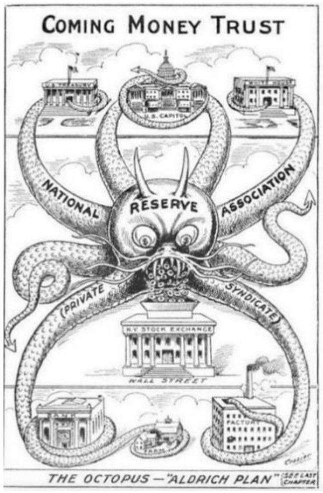
2/ When we look at the cryptoasset universe, there are two distinct hemispheres: 1) Bitcoin and 2) everything else, which are commonly known as Alternative Cryptoassets or Alts



3/ Bitcoin is more akin to the internet itself, which is composed of an open-source protocol stack called the internet protocol suite (consisting of http, TCP/IP, etc.)



4/ In the same way the internet is a set of open protocols for exchanging information, Bitcoin is a set of open protocols for exchanging value. Hence its common nickname "the internet of value"



5/ Bitcoin can be thought of as the latest layer in the internet protocol suite and, we believe, will grow to touch everything and everyone that the internet touches today

6/ This perspective also gives us a useful analogy when thinking about how one could stop Bitcoin: The analogous question is: 'How does one permanently turn off the entire Internet worldwide?'

7/ Bitcoin is free market money competing against monopoly money (pun intended). Bitcoin is disintermediating the market for money, which today is monopolized by central banks

8/ In the other half of the cryptoasset universe, we have Alternative Cryptoassets (also called Alts or Altcoins)

9/ Alts have adopted the open-source technology underpinning Bitcoin to attempt to compete against it directly, disintermediate other markets, or enable new markets

10/ So far, the use cases for Alts are mostly unproven (with the possible exception of Ethereum) and Bitcoin is positioned to capture the vast majority of the value created during this entire wave of innovation

11/ Alts are venture capital investments that can be launched at extremely low cost and are subjected to little, if any, professional due diligence (hence their other nickname - shitcoins)

12/ Some alts may one day succeed meaningfully, however these venture-style investments are much more risky than Bitcoin

13/ Intriguingly, although Bitcoin is a modern innovation, to understand its value proposition fully we must first dive deep into the history and nature of money…

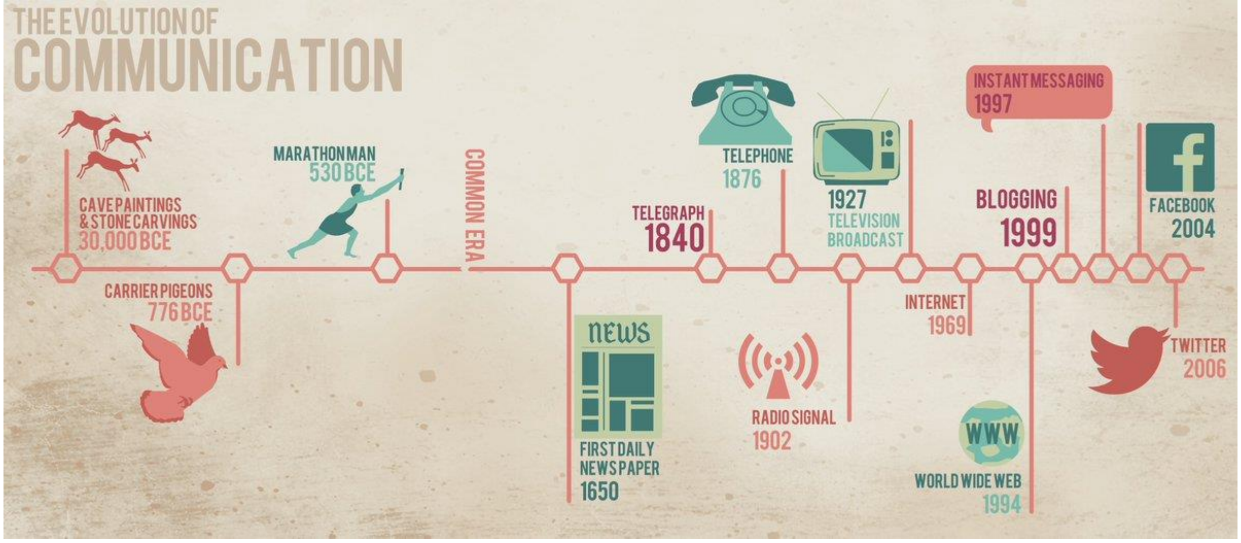
14/ Throughout history, money has evolved many times – it has taken the form of seashells, salt, cattle, stones, precious metals and most recently government paper

15/ Monetary technologies are always in competition with one another and undergo market-driven natural selection which gives rise to new forms of money and leads old forms to extinction

16/ Monetary evolution, a market-driven technology selection process, is somewhat similar to the evolutionary process we see in telecommunications technologies:

17/ No matter what technology is used to accomplish it, the purpose of telecommunications remains the same: to communicate information across space and time

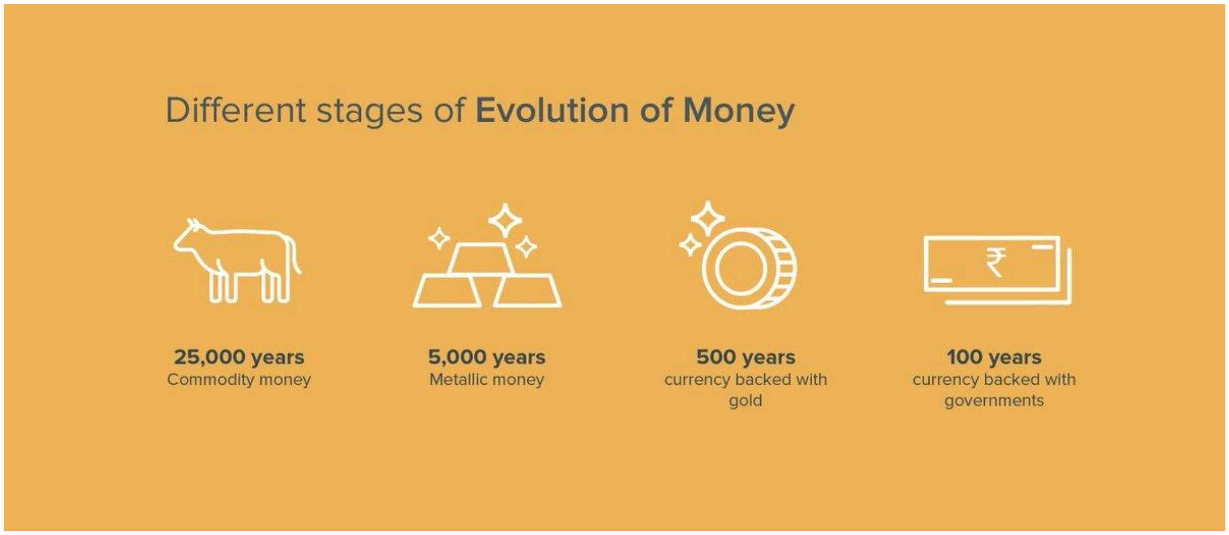
18/ However, the telecommunications technologies we use to communicate evolve over time (from cave paintings to carrier pigeons to newspapers to telegraphs to telephones to digital media)



19/ As newer telecommunications technologies are invented that provide higher speed, fidelity, reliability, traceability or mobility – they become the dominant means of communicating information across space and time

20/ Similar to the purpose of telecommunications, the purpose of money also remains the same: to communicate value across space and time

21/ However, the monetary technologies we use to communicate value also evolve over time (from seashells to salt to cattle to stones to precious metals)


Different stages of Evolution of Money
₹
25,000 years
Commodity money
5,000 years
Metallic money
500 years
currency backed with gold
100 years
currency backed with governments

22/ As newer monetary technologies are invented that provide higher hardness, divisibility, portability, durability or recognizability – they become the dominant method of communicating value across space and time

23/ Money has many characteristics, but the primary trait which determines whether it succeeds or fails in the free market is called 'Hardness' (on which we will now focus)

24/ Hardness is the difficulty to produce an incremental unit of the monetary instrument (ie. the energy expenditure necessary to mine an ounce of gold or produce a US dollar, for instance)

25/ Hardness is quantified by the stock-to-flow ratio. Stock is the existing money supply. Flow is the newly produced money supply over a given time period. The higher the stock-to-flow ratio, the Harder (or sounder) the money

26/ Each time an additional monetary unit is created, the other monetary units become less scarce and lose purchasing power, an effect commonly called inflation (the inverse of the stock-to-flow ratio)

27/ Inflation, a euphemistic term, is actually the dilution of monetary value and an insidious form of taxation without representation. Inflation can be easily understood with a baseball card analogy:

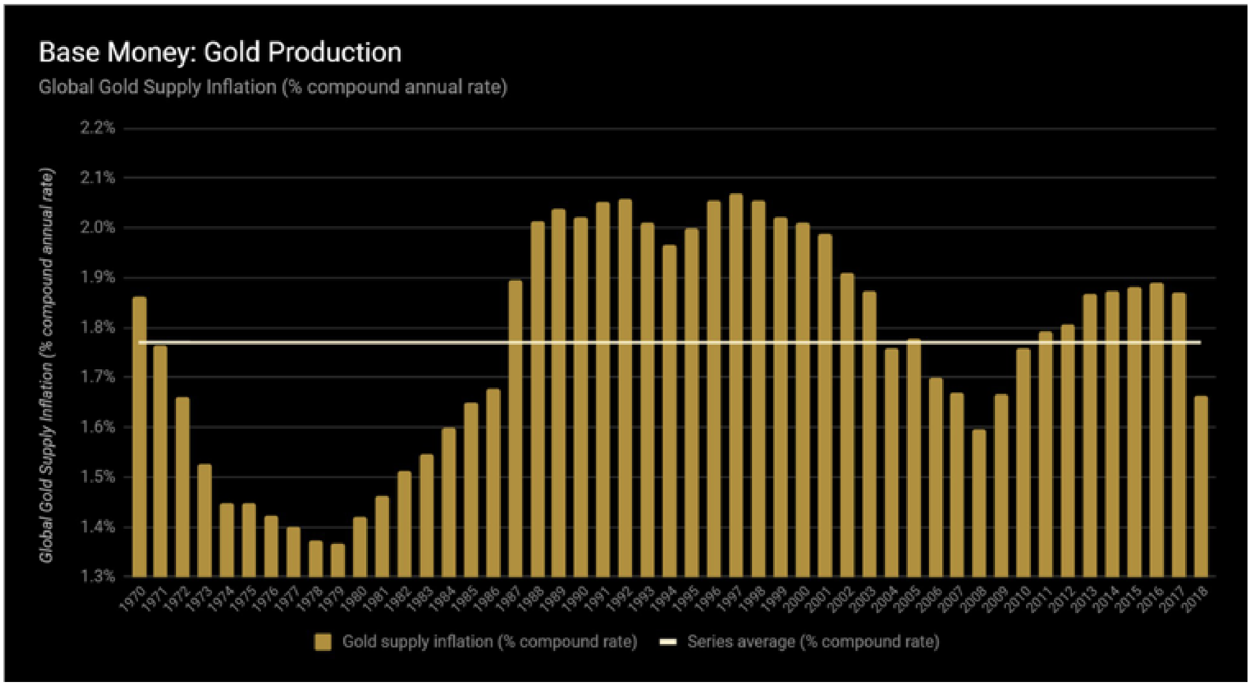
28/ If I have 1 of the 100 Babe Ruth rookie baseball cards in the world, each time someone discovers another Babe Ruth rookie card mine becomes less rare and therefore less valuable. The same is true with money, each time a new unit is created all other units decline in value

29/ In a free market, people naturally and rationally choose to store their wealth in the monetary technology which is hardest to inflate (by mining, printing, counterfeiting, etc.)

30/ Gold eventually became global standard for money precisely because of its Hardness (as quantified by a superior stock-to-flow ratio)

31/ Gold is virtually indestructible, so nearly every ounce ever mined throughout history remains extant today (high stock)

32/ Gold is rare in the earth's crust and it takes time and energy to extract it (low flow)



33/ The Hardness of gold resulted in it outcompeting silver several times throughout history and is the reason silver is almost entirely demonetized today. This competitive dynamic is easily explained from a game theory perspective:

34/ Since gold is harder than silver, anyone who profits from silver production (where marginal revenue > marginal cost) will seek to store their profits in the hardest form of money available, thus triggering investment flows from silver (or any other softer money) to gold

35/ However, gold has one major drawback, the divisibility problem: Gold is heavy and difficult to deeply subdivide, which makes it difficult to use as a medium of exchange (ie. buying coffee with gold coins is not practical)

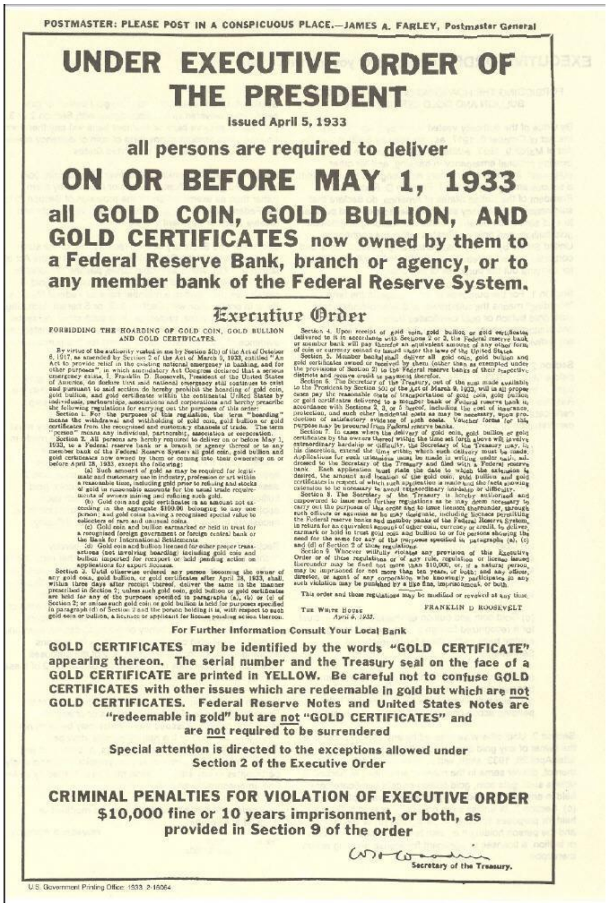
36/ Gold's divisibility problem is what gave silver some marginal utility as a medium of exchange throughout history whereas gold was more typically reserved for settling large transactions

37/ Eventually, national governments stepped in and solved the divisibility problem of gold by issuing bank notes (essentially paper IOUs), which are light and easy to transact with, that were fully redeemable for gold

38/ This caused the centralization of gold within bank vaults which became too tempting for governments and their newly formed central banks to resist expropriation of, thus catalyzing the fractional-reserve banking practices now ubiquitous in the modern world economy

39/ As governments created more bank notes than they could support with their gold reserves, they started revoking bank note redeemability for gold, thus implementing the 'money backed by nothing' we all use now - fiat currencies

40/ A brief history of fiat currencies: In 1933, executive order #6102 required all US citizens to exchange their gold holdings for US dollars under the threat of up to 10 years imprisonment



POSTMASTER: PLEASE POST IN A CONSPICUOUS PLACE.—JAMES A. FARLEY, Postmaster General

UNDER EXECUTIVE ORDER OF THE PRESIDENT

Issued April 5, 1933

all persons are required to deliver

ON OR BEFORE MAY 1, 1933

all GOLD COIN, GOLD BULLION, AND GOLD CERTIFICATES now owned by them to a Federal Reserve Bank, branch or agency, or to any member bank of the Federal Reserve System.

Executive Order

FORBIDDING THE HOARDING OF GOLD COIN, GOLD BULLION AND GOLD CERTIFICATES.

By virtue of the authority vested in me by Section 5(b) of the Act of October 6, 1917, as amended by Section 2 of the Act of March 9, 1933, entitled "An Act to provide relief in the existing national emergency in banking, and for other purposes", in which amendatory Act Congress declared that a serious emergency exists, I, Franklin D. Roosevelt, President of the United States of America, do declare that said national emergency still continues to exist and pursuant to said section do hereby prohibit the hoarding of gold coin, gold bullion, and gold certificates within the continental United States by individuals, partnerships, associations and corporations and hereby prescribe the following regulations for carrying out the purposes of this order:

Section 1. For the purposes of this regulation, the term "hoarding" means the withdrawal and withholding of gold coin, gold bullion or gold certificates from the recognized and customary channels of trade. The term "person" means any individual, partnership, association or corporation.

Section 2. All persons are hereby required to deliver on or before May 1, 1933, to a Federal reserve bank or a branch or agency thereof or to any member bank of the Federal Reserve System all gold coin, gold bullion and gold certificates now owned by them or coming into their ownership on or before April 28, 1933, except the following:

(a) Such amount of gold as may be required for legitimate and customary use in industry, profession or art within a reasonable time, including gold prior to refining and stocks of gold in reasonable amounts for the usual trade requirements of owners mining and refining such gold.

(b) Gold coin and gold certificates in an amount not exceeding in the aggregate $100.00 belonging to any one person; and gold coins having a recognized special value to collectors of rare and unusual coins.

(c) Gold coin and bullion earmarked or held in trust for a recognized foreign government or foreign central bank or the Bank for International Settlements.

(d) Gold coin and bullion licensed for other proper transactions (not involving hoarding) including gold coin and bullion imported for reexport or held pending action on applications for export licenses.

Section 3. Until otherwise ordered any person becoming the owner of any gold coin, gold bullion, or gold certificates after April 28, 1933, shall, within three days after receipt thereof, deliver the same in the manner prescribed in Section 2; unless such gold coin, gold bullion or gold certificates are held for any of the purposes specified in paragraphs (a), (b) or (c) of Section 2; or unless such gold coin or gold bullion is held for purposes specified in paragraph (d) of Section 2 and the person holding it is, with respect to such gold coin or bullion, a licensee or applicant for license pending action thereon.

Section 4. Upon receipt of gold coin, gold bullion or gold certificates delivered to it in accordance with Sections 2 or 3, the Federal reserve bank or member bank will pay therefor an equivalent amount of any other form of coin or currency coined or issued under the laws of the United States.

Section 5. Member banks shall deliver all gold coin, gold bullion and gold certificates owned or received by them (other than as exempted under the provisions of Section 2) to the Federal reserve banks of their respective districts and receive credit or payment therefor.

Section 6. The Secretary of the Treasury, out of the sum made available to the President by Section 501 of the Act of March 9, 1933, will in all proper cases pay the reasonable costs of transportation of gold coin, gold bullion or gold certificates delivered to a member bank or Federal reserve bank in accordance with Sections 2, 3, or 5 hereof, including the cost of insurance, protection, and such other incidental costs as may be necessary, upon production of satisfactory evidence of such costs. Voucher forms for this purpose may be procured from Federal reserve banks.

Section 7. In cases where the delivery of gold coin, gold bullion or gold certificates by the owners thereof within the time set forth above will involve extraordinary hardship or difficulty, the Secretary of the Treasury may, in his discretion, extend the time within which such delivery must be made. Applications for such extensions must be made in writing under oath, addressed to the Secretary of the Treasury and filed with a Federal reserve bank. Each application must state the date to which the extension is desired, the amount and location of the gold coin, gold bullion and gold certificates in respect of which such application is made and the facts showing extension to be necessary to avoid extraordinary hardship or difficulty.

Section 8. The Secretary of the Treasury is hereby authorized and empowered to issue such further regulations as he may deem necessary to carry out the purposes of this order and to issue licenses thereunder, through such officers or agencies as he may designate, including licenses permitting the Federal reserve banks and member banks of the Federal Reserve System, in return for an equivalent amount of other coin, currency or credit, to deliver, earmark or hold in trust gold coin and bullion to or for persons showing the need for the same for any of the purposes specified in paragraphs (a), (c) and (d) of Section 2 of these regulations.

Section 9. Whoever willfully violates any provision of this Executive Order or of these regulations or of any rule, regulation or license issued thereunder may be fined not more than $10,000, or, if a natural person, may be imprisoned for not more than ten years, or both; and any officer, director, or agent of any corporation who knowingly participates in any such violation may be punished by a like fine, imprisonment, or both.

This order and these regulations may be modified or revoked at any time.

FRANKLIN D ROOSEVELT

THE WHITE HOUSE
April 5, 1933.

For Further Information Consult Your Local Bank

GOLD CERTIFICATES may be identified by the words "GOLD CERTIFICATE" appearing thereon. The serial number and the Treasury seal on the face of a GOLD CERTIFICATE are printed in YELLOW. Be careful not to confuse GOLD CERTIFICATES with other issues which are redeemable in gold but which are not GOLD CERTIFICATES. Federal Reserve Notes and United States Notes are "redeemable in gold" but are not "GOLD CERTIFICATES" and are not required to be surrendered

Special attention is directed to the exceptions allowed under Section 2 of the Executive Order

CRIMINAL PENALTIES FOR VIOLATION OF EXECUTIVE ORDER $10,000 fine or 10 years imprisonment, or both, as provided in Section 9 of the order

Secretary of the Treasury.

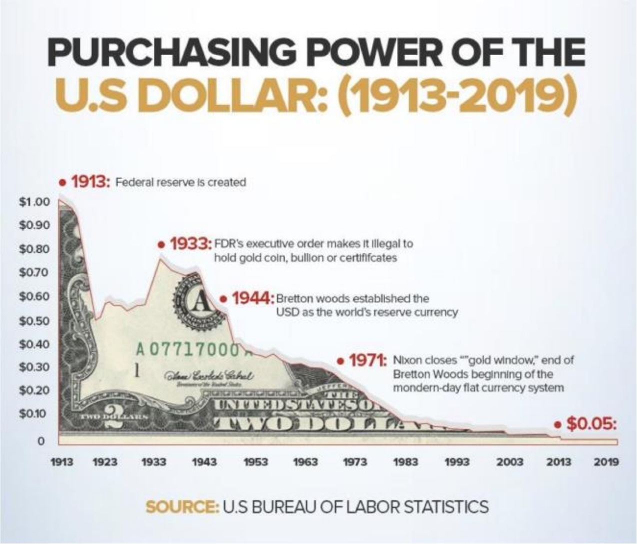
U.S. Government Printing Office: 1933 2-16064

41/ During WWII, The US became a safe haven for European gold hoards as a means of protection from Nazi plundering, thus positioning it to rewrite the rules of the global economic order

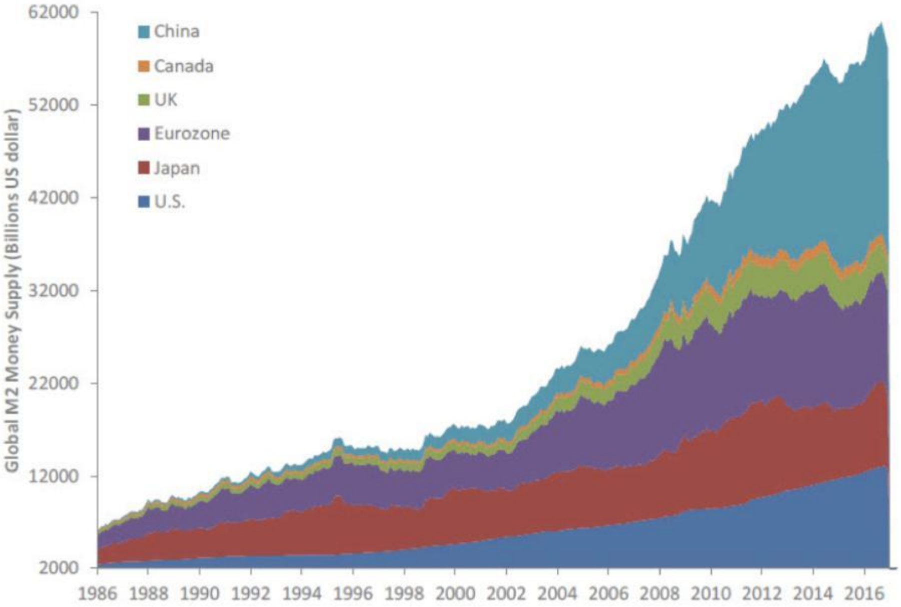
42/ At the conclusion of WWII, The US established itself as the global central bank, in which all international currencies would be pegged to the US dollar, which itself was to be pegged to gold, at the Bretton Woods Conference

43/ In 1971, US President Nixon unilaterally cancelled the direct international convertibility of the US dollar to gold and promised that the US would eventually return to the Gold standard, which of course never happened, leaving the world on a fiat standard

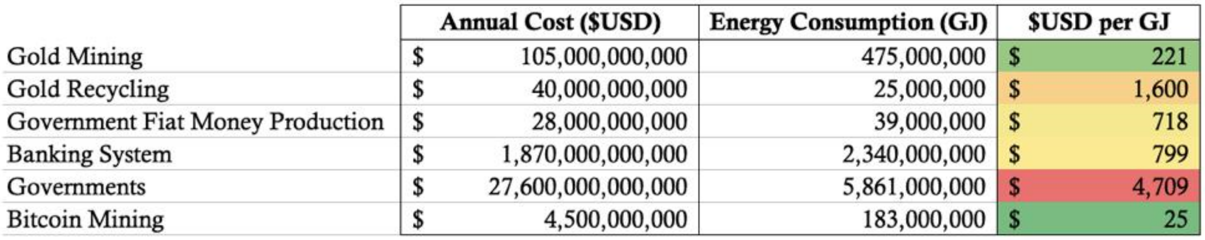
44/ So today, the world is dominated by government fiat money which is backed by absolutely nothing and is in fact the Softest form of money that has ever existed (the cost to produce an additional unit of fiat money is near-zero)



45/ In the wake of the 2008 Great Recession, when central banks all over the world were busy printing more fiat currencies to reflate their respective economies, Satoshi Nakamoto released an open-source software project into the world called Bitcoin

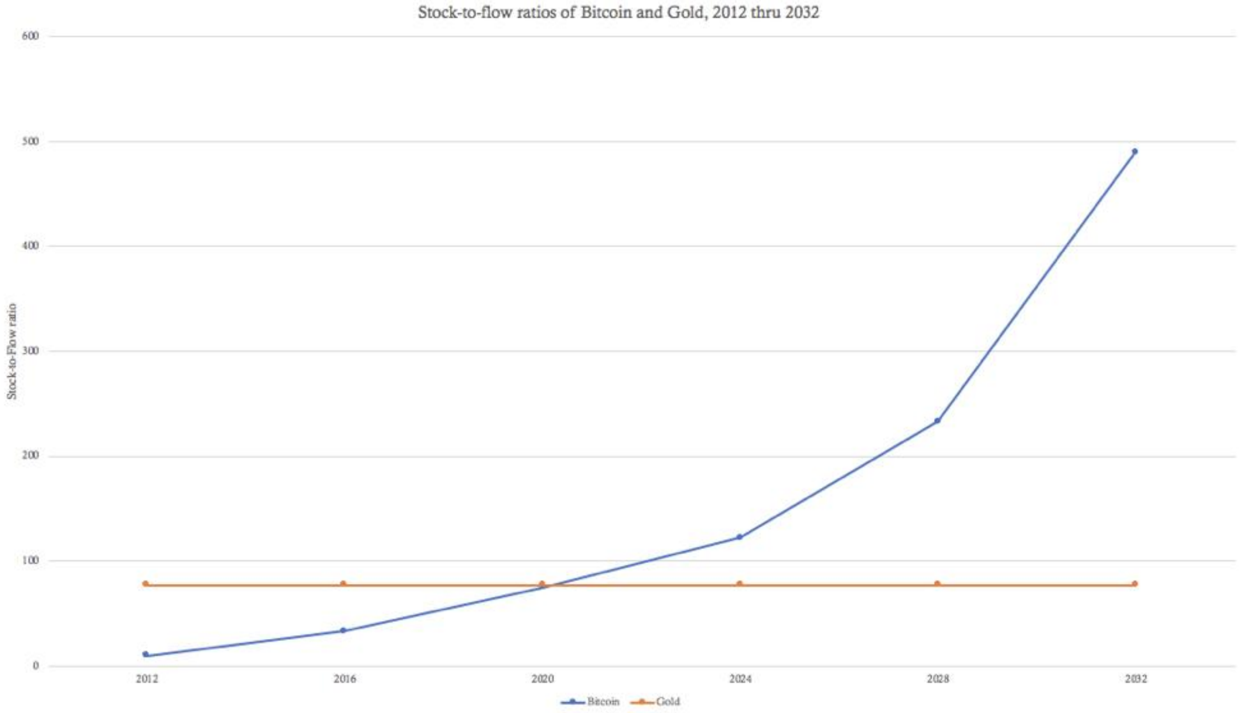


46/ Bitcoin is the Hardest form of money that has ever existed. This momentous innovation is made possible by an ever-rising production difficulty that requires expenditure of real world energy (in a process called proof-of-work or mining)



	Annual Cost ($USD)	Energy Consumption (GJ)	$USD per GJ
Gold Mining	$ 105,000,000,000	475,000,000	$ 221
Gold Recycling	$ 40,000,000,000	25,000,000	$ 1,600
Government Fiat Money Production	$ 28,000,000,000	39,000,000	$ 718
Banking System	$ 1,870,000,000,000	2,340,000,000	$ 799
Governments	$ 27,600,000,000,000	5,861,000,000	$ 4,709
Bitcoin Mining	$ 4,500,000,000	183,000,000	$ 25

47/ Bitcoin's stock-to-flow ratio increases inevitably every 4 years will surpass that of gold in May 2020. Bitcoin's monetary policy is enforced by unbreakable cryptography, hence the inevitability (as sure as 1+1=2)



48/ Bitcoin is also the world's first incarnation of an asset with perfect price inelasticity of supply, as changes in its price have absolutely no impact on its supply flow. This means increases in demand for Bitcoin can only be expressed in its market price

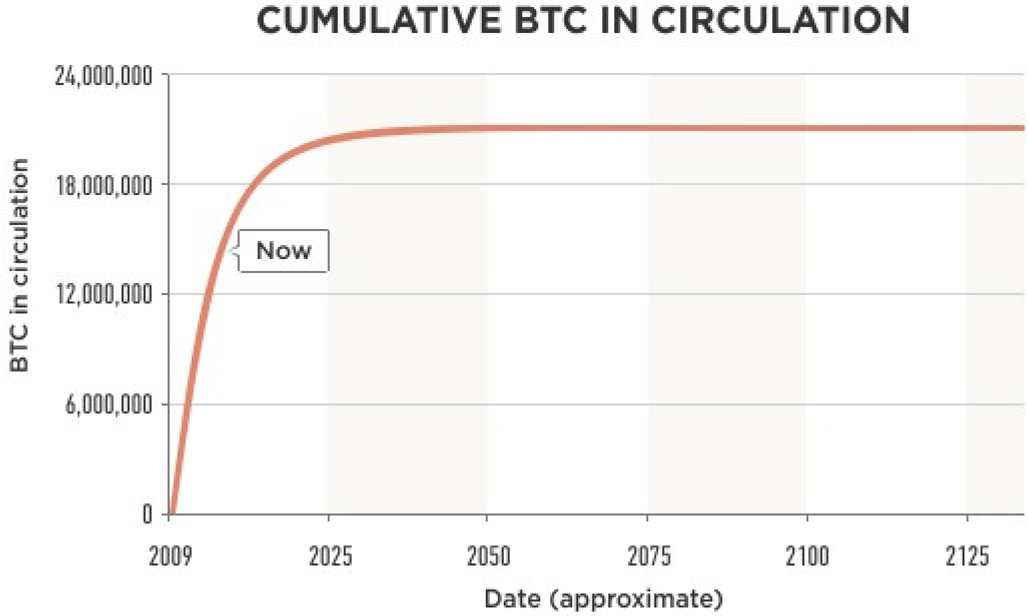
49/ If the price of gold increases, its new supply flow will increase as new miners enter the market and new methods of gold mining becoming economically feasible (since the gold miners can sell their product at a higher price), thereby decreasing its stock-to-flow ratio

50/ With Bitcoin, no matter how much its price increases, it is absolutely impossible to create any new supply flow beyond its mathematically enforced and universally transparent production schedule

51/ Bitcoin is also the world's first instance of 'absolute scarcity' as its monetary policy is fixed, only 21M units will ever exist. Before Bitcoin, only time itself was absolutely scarce (the formula for Bitcoin's fixed monetary policy is pictured here)

$$\sum_{i=0}^{32} 210{,}000 \frac{50}{2^i}$$

52/ This means that its stock-to-flow ratio will continue to increase and eventually become infinite when the last Bitcoin is produced sometime in the middle of the 22nd century



53/ Bitcoin's monetary policy (its new supply flow schedule) is becoming the most trusted in the world as it is fully transparent and unchangeable

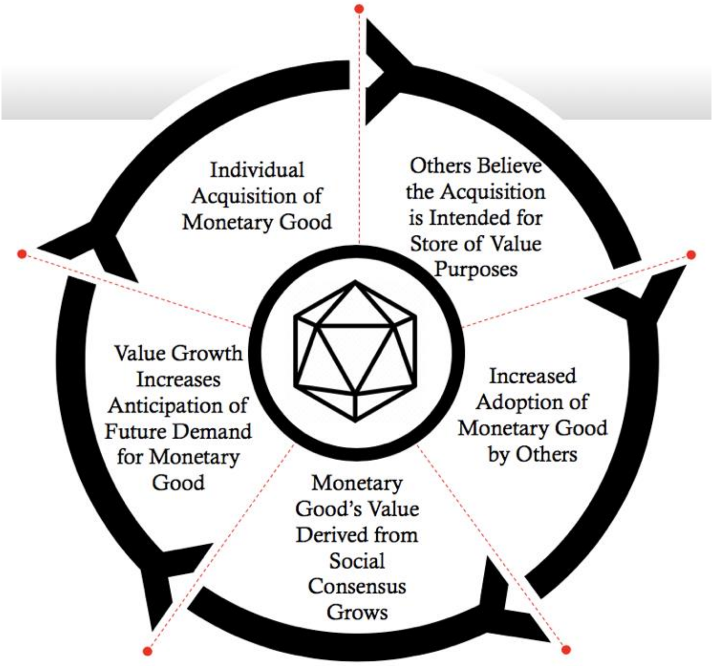
54/ Bitcoin runs countervailing to government monetary policy which is uncertain, opaque and subject to change based on the whim of bureaucrats

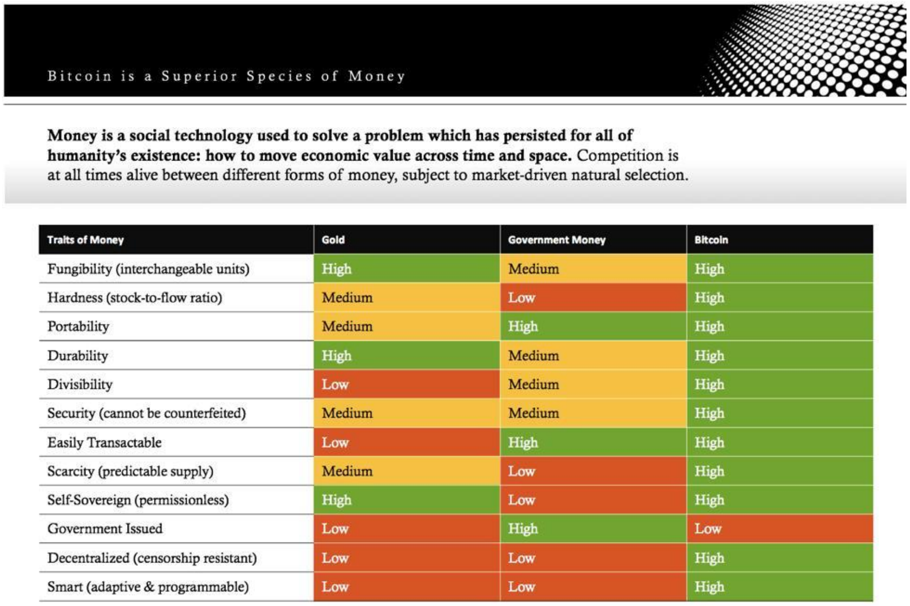
55/ Essentially, we each must decide if we are to trust the whimsical nature of self-interested bureaucrats or the inviolable nature of mathematics to manage our money supply

56/ So we have Bitcoin, the Hardest form of money in history, competing directly with government money, the Softest form of money in history…

57/ Game theory and history shows us that people will naturally and rationally seek to store their wealth in the Hardest money available to them. This emergent market behavior is based on the anticipated decisions of others and will eventually spiral into an adoption frenzy

58/ So long as Bitcoin continues to exist (and without even considering its other superior traits as a form of money) we believe it will continue to outcompete gold and government money in the free market and appreciate in value


Individual Acquisition of Monetary Good
Others Believe the Acquisition is Intended for Store of Value Purposes
Increased Adoption of Monetary Good by Others
Monetary Good's Value Derived from Social Consensus Grows
Value Growth Increases Anticipation of Future Demand for Monetary Good

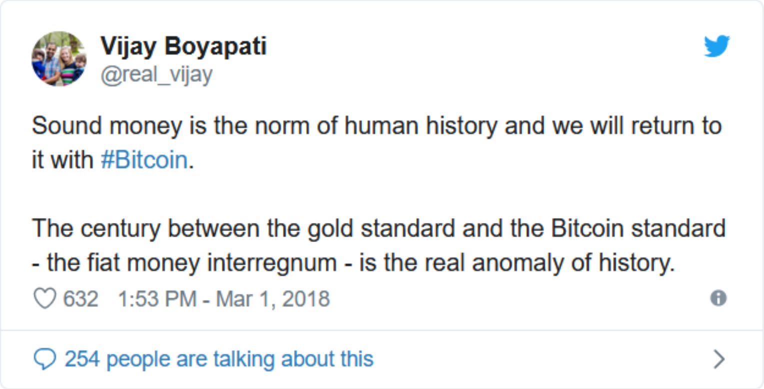


Bitcoin is a Superior Species of Money

Money is a social technology used to solve a problem which has persisted for all of humanity's existence: how to move economic value across time and space. Competition is at all times alive between different forms of money, subject to market-driven natural selection.

Traits of Money	Gold	Government Money	Bitcoin
Fungibility (interchangeable units)	High	Medium	High
Hardness (stock-to-flow ratio)	Medium	Low	High
Portability	Medium	High	High
Durability	High	Medium	High
Divisibility	Low	Medium	High
Security (cannot be counterfeited)	Medium	Medium	High
Easily Transactable	Low	High	High
Scarcity (predictable supply)	Medium	Low	High
Self-Sovereign (permissionless)	High	Low	High
Government Issued	Low	High	Low
Decentralized (censorship resistant)	Low	Low	High
Smart (adaptive & programmable)	Low	Low	High

59/ Hard money, as selected on the free market, reigned for the first 4,900 out of 5,000 years of human commercial history and we are witnessing its reemergence in the rise of Bitcoin



Vijay Boyapati
@real_vijay

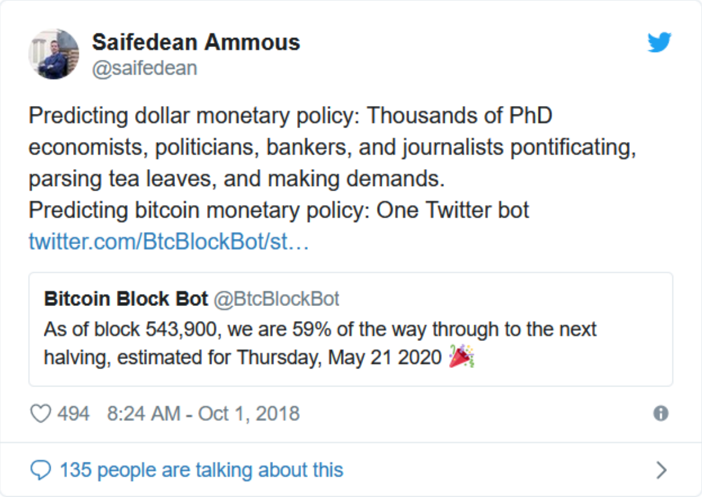
Sound money is the norm of human history and we will return to it with #Bitcoin.

The century between the gold standard and the Bitcoin standard - the fiat money interregnum - is the real anomaly of history.

♡ 632 1:53 PM - Mar 1, 2018

254 people are talking about this

60/ Bitcoin is the most credible monetary policy in human history disrupting the most untrustworthy monetary policies in human history



Saifedean Ammous
@saifedean

Predicting dollar monetary policy: Thousands of PhD economists, politicians, bankers, and journalists pontificating, parsing tea leaves, and making demands.
Predicting bitcoin monetary policy: One Twitter bot twitter.com/BtcBlockBot/st…

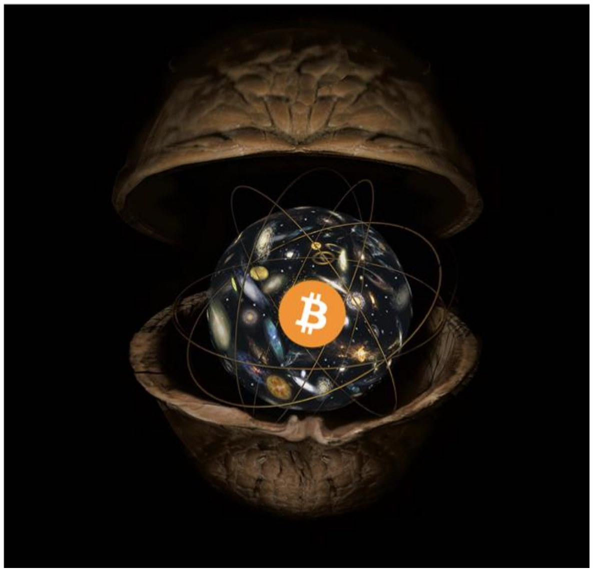
Bitcoin Block Bot @BtcBlockBot
As of block 543,900, we are 59% of the way through to the next halving, estimated for Thursday, May 21 2020 🎉

♡ 494 8:24 AM - Oct 1, 2018

135 people are talking about this

61/ A bet on Bitcoin is that the competitive dynamics inherent to the market for money will continue to play out in the same way they have throughout all of history

62/ Thank you for reading. This is the Bitcoin and cryptoasset universe in a nutshell.



With Gratitude: @real_vijay @saifedean @bquittem @danheld @naval @NickSzabo4 @nic__carter @MartyBent @pierre_rochard @APompliano @cburniske @MarkYusko @CaitlinLong_ @timevalueofbtc @nntaleb @stephanlivera @WhatBitcoinDid @dergigi @hasufl @MustStopMurad @misir_mahmudov @mises 🙏

You can follow @Breedlove22 .

Money, Banking, Bitcoin, Libra

By Allen Farrington

Posted June 22, 2019

Money

There is a common misunderstanding of Bitcoin as a 'payment mechanism', and hence that it somehow ought to capture *all payments*. I am not really sure, but I suspect this comes from a dogmatic application of *the three essential characteristics of money_as typically taught in macroeconomics 101: _unit of account, store of value,* and *medium of exchange.* I think this is rather silly and that, really, money is just universal credit. How it works or what extra characteristics it has is beside the point. The former attitude leads one to say things like: *it's too volatile,_and _, it's too hard to trade with*, and then immediately jump to, *it can't be money*, while conveniently ignoring the multitude of other amazing and entirely novel things it can do: for example, it has a guaranteed inflation schedule that cannot be manipulated, transaction fees are either non-existent or regressive, it is totally agnostic to geography or identity, settlement time is rarely over one hour, it is completely transparent, it is a network that is *never* down and cannot be hacked, it is programmable (to a small degree—more on this later), and more. Better even than the abstraction of 'money', a less common but more intelligent approach is to treat Bitcoin as a better version of gold. After a century or so of relentless devaluation of previously gold backed fiat currency we are not used to thinking of the relevance of gold to money or finance. But its legacy is still imprinted on the banking system, and so it is with banks I will begin.

Before getting to the more exciting possibilities it is worth tackling head on why Bitcoin almost certainly *can't_be used for payments all on its own. Bitcoin cannot handle the necessary throughput, _by design*: amending the block size or block confirmation time would be a trivial exercise and could solve this 'problem' instantly, but would make the blockchain itself unacceptably large as a data structure such that very few parties could run full nodes and authenticate the chain, reintroducing the centralisation that is essential to the social core of the enterprise to begin with. 'Fixing' Bitcoin by making it 'scale' would really break it altogether (which is why most copycats are entirely pointless)

How to scale Bitcoin (without changing a thing) *Why Bitcoin banks need to prove their solvency* medium.com

The implicit trade-off of foregoing practical payment applications may be overcome by second-layer protocols such as Lightning, further abstractions and generalisations as in the Polkadot network, or Bitcoin-backed assets, all of which I will discuss below, but not with Bitcoin itself. The constant furore over Bitcoin 'failing to scale' obscures a point that has been really been understood in the core Bitcoin community for almost its entire existence. Hal Finney, the legendary cryptographer and cypherpunk who was the second ever miner of Bitcoin and received its first transaction from Satoshi, gave what really ought to have been the final word on this in the Bitcoin forum in 2010:

"Actually there is a very good reason for Bitcoin-backed banks to exist, issuing their own digital currency, redeemable for Bitcoins. Bitcoin itself cannot scale to have every single financial transaction in the world be broadcast to everyone and included in the block chain. There needs to be a secondary level of payment systems which is lighter weight and more efficient. Likewise, the time needed for Bitcoin transactions to finalize will be impractical for medium to large value purchases. Bitcoin backed banks will solve these problems. They can work like banks did before nationalisation of currency. Different banks can have different policies, some more aggressive, some more conservative. Some would be fractional reserve while others may be 100% Bitcoin backed. Interest rates may vary. Cash from some banks may trade at a discount to that from others. ***George Selgin*** *has worked out the theory of competitive free banking in detail, and he argues that such a system would be stable, inflation resistant and self-regulating. I believe this will be the ultimate fate of Bitcoin, to be the "high-powered money" that serves as a reserve currency for banks that issue their own digital cash. Most Bitcoin transactions will occur between banks, to settle net transfers. Bitcoin transactions by private individuals will be as rare as … well, as Bitcoin based purchases are today."*

While I think Finney was mostly directionally correct, the picture will likely become far more complicated than what he imagined here, due a combination of both higher 'layers' of Bitcoin and interoperability with other protocols, which I discuss below, and the possibility of integration Bitcoin into FX markets to serve a range of business needs.

FX is a gigantic industry that isn't necessarily cheap. Common pairs such as Dollar to Pound have very liquid markets and very tight spreads (for trade participants, but not even necessarily for consumers) but to consider an extreme example, moving Indonesian Rupiah into Peruvian Sol will likely be very expensive and may invalidate the business case behind the desired move. The more contrived the example, the longer it will take, also. Were both Bitcoin and a range of local fiat exchanges to be liquid enough, this would be far preferable for almost every FX transaction imaginable, possibly only excluding the interchange of Dollars, Pounds, Euros, and Yen. The reason is simple: it rarely takes more than one hour to transact Bitcoin, and is often more like 10–15 minutes. Also, the cost is utterly negligible compared to FX, and is actually regressive: miner fees (if they exist at all) are determined by how congested each block is with the data of individual transactions, which is unrelated to transaction value. And notice that volatility doesn't matter either: only market liquidity does. Even Bitcoin is not volatile enough to create an exposure risk over the space of 15 minutes, and it will become less so the more it is used as a kind of meta-currency or settlement-commodity (or however else it helps to conceptualise it) rather than a speculative asset. What matters far more is that there are adequately liquid exchanges in the relevant currencies. If there are several markets between Bitcoin and the Dollar, and several more between Bitcoin and the Rupiah and the Sol, that are deep and liquid enough to prevent any arbitrage triangles emerging, then the problem should be solved. What would stymie this would be dramatically different exchange rates for Bitcoin in different exchanges such that value couldn't *really* be transferred in the first place—but volatility is largely irrelevant.

This isn't necessarily an argument in favour of Bitcoin appreciating, since the holding period I am stipulating is only as long as it takes to receive a transaction and flip it back to fiat. However, what would be really interesting is if an equally deep and liquid industry in Bitcoin futures developed, with the notional posted in fiat. What this would mean is that there would then be a use case to hold Bitcoin on the balance sheet of a company that expects to have to do a lot of FX trading or cross-border fiat settlement, especially that cannot be predicted with any precision. The likely volatility absent any futures would make this an extremely risky idea, but with a futures market, a company could maintain a float of Bitcoin that is fully hedged to their preferred fiat, so that the process of engaging in FX and settlement is sped up and cheapened even further. You would never need to rely on fiat exchanges potentially being inaccessible when you need them most; you tap directly into the Bitcoin network, and only return to the fiat exchange when convenient. Most excitingly of all, this market would probably make a lot more sense as part of a prediction market, itself based on another smart-contract platform blockchain, than it would if run out of an investment bank's prop trading desk. We then come back to familiar questions of which system is more trustworthy, and how valuable it is to have a counterparty for legal reasons, etc.

On Prediction Markets and Blockchains *Why are prediction markets so accurate, why do they lend themselves to blockchain, and what does blockchain do for…*
medium.com

Banking

The final tumble down the rabbit hole gets us to Bitcoin backed banks. (but if the rabbit hole is a fractal, is there ever a final tumble? anyway …) If you have a global settlement layer with highly liquid markets, then why not hold this asset in reserve and issue digital cash against it? Such digital cash might not even need to be blockchain-based, since you get the trust benefits from the Bitcoin the bank holds in reserve; you should be able to know the bank has adequate capital because you can check the blockchain, and you can redeem it whenever you like. Or maybe you can't because you don't have a demand deposit, but you can enter some kind of smart contract as to what exactly you can do with your savings and how you are rewarded for lending your capital. We get the blooming of a thousand flowers in banking experiments contrary to fractional reserve: entrepreneurs can actually try something different and see how the market reacts rather than just the occasional academic whining about it. Again, not predicting this will happen, just that it will be possible.

Bitcoin backed banks are worth pondering for a little longer, as both their risks and potential strike me as being widely misunderstood. Starting from first principles, there are two separate risks in running a bank, and most cryptonerds only seem to be concerned with one. A bank, as opposed to just a depository institution, is necessarily an asset manager that succeeds on the basis of directing capital towards profitable enterprise (this direction may be extremely *indirect,* but even mortgages rely on this happening somewhere in the monetary ecosystem) The risk managed by the reserve ratio is simply that the bank screws up the promises regarding liquidity made to the loaners of funds in the process of maturity transformation—in other words that they misjudge the true maturity of liabilities. The reserve is a buffer against that happening, but is a distinct concern from the risk of making bad loans—in other words that they misjudge the true quality of assets. Another conceptualisation of the difference is the risk of badly managing working capital as opposed to invested capital, or liquidity as opposed to solvency. You can take your pick.

The liability maturity risk is presumably greatly improved upon by Bitcoin due to its auditability. This seems to be well understood and has been interestingly explored. But the asset quality problem seems more pertinent to the concept of an entirely new kind of money and bank, whereas a lot of hardcore Bitcoiners seem to mistake the second risk for the first and misunderstand both risks in the brave new world. In a sense a wallet is a depository institution, so if you want to avoid illiquidity from the liability maturity risk, you can, which you can't really do with regular money unless you hide it under your mattress. That's one of the serious problems of being forced to live within an opaque and corrupt financial system; you are forced to shoulder that risk whether you want to or not, and of course the existence of 'lenders of last resort' makes it even worse.

In cryptoland, this problem is naturally avoided because the 'money under the mattress' situation is not weird at all. If anything, it is the natural state. But the fallacy here is assuming that the removal of the liability maturity risk via auditability immediately translates to the removal of the asset quality risk too, which it does not. If the bank makes enough bad loans (interestingly this quantum is determined by what it would take to wipe out the reserves, so the risks are related, just in a subtler way than is commonly understood) then it doesn't matter how auditable everything is—the depositor is not getting anything back. It won't matter whether it's gold or Dollars or Bitcoin or magic internet money *backed* by gold or Dollars or Bitcoin or whatever. If it's really a bank and not just a depository institution, and enough loans go bad, then the money is gone.

So that's the risk, but there are opportunities too. To the best of my (admittedly limited) knowledge, the furthest this idea really gained traction was with the distinction between a checking and savings account, but even that difference is mostly trivialised by having money that is basically exclusively digital anyway. Regardless, you could have a structure whereby there are different classes of deposits, or perhaps the nature of the deposits depends on some parameter (the auditable reserve ratio being an obvious contender) It could also be the performance of the loans; you could get transparency on where exactly your funds have gone (or it's a choice as a depositor as to what class of savings product you take) and both your access to the funds and your interest is somehow programmatic, or dynamic. Really, it could be whatever conceived of reason makes the bank function better, or more appealingly given different customer profiles. This seems to me to be the really intriguing part of Bitcoin backed banks.

For Bitcoin maximalists, this line of thought can even be framed in a way that implicitly mocks the more delusional CS types who have promised us the world with their 'Bitcoin + X' contrivances. What many of these amount to is just financial engineering via software engineering. More advanced, transparent, and democratic financial engineering than any investment bank ever provided, but financial engineering nonetheless. Whereas you need actual economic productivity for this to ever matter, for which sound money certainly helps. Keynes had a line that reflected this well,

"*Of the maxims of orthodox finance, none, surely, is more anti-social than the fetish of liquidity, the doctrine that it is a positive virtue on the part of the investment institutions to concentrate their resources on the holding of 'liquid' securities. It forgets that there is no such thing as liquidity of investment for the community as a whole.*"

Despite being highly questionable on economics, Keynes had a remarkable intuition for finance. Liquidity means nothing if the liquid asset doesn't contribute to economic productivity over at least the term of the debt that financed it, and preferably much longer, which is something a system of Bitcoin-based banking might materially enhance …

Bitcoin

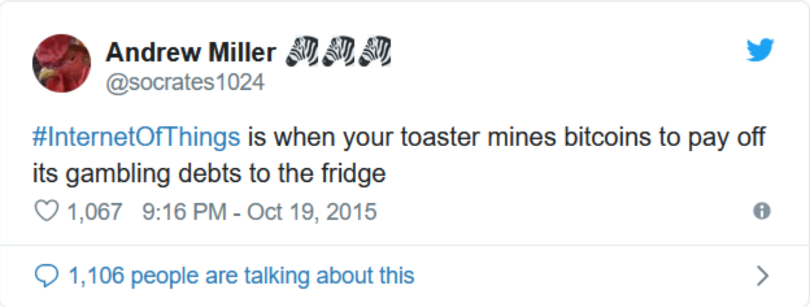
The core thesis behind these speculative ideas is that there are no necessary or sufficient criteria for 'money'. As I alluded to above, anything that enhances the ability to create and circulate universal credit will do. There is no need for maximalism when we can observe what seems to work following countless independent experiments. If you wanted a slogan for this, how about, ‘unbundling money’, or ‘decentralising capital’? If the functions I suggest, or any others, come into existence, it will not be precisely because, *Bitcoin is better money*, but because Bitcoin introduces desirable and entirely novel features into the process of storing and transferring value, which can then be used to create credit. Bitcoin cannot transact instantly, cannot support more than around 7 transactions per second (averaged over the settlement period), cannot be reclaimed in cases of fraud, and can’t really be used to buy much stuff at all, at least currently. Fiat currency on existing payment rails can. But fiat currency (over any payments rails) cannot be sound money, cannot be guaranteed to always be online, cannot be transferred for free, cannot be programmed, cannot be audited, and if online cannot be permissionless. Bitcoin can.

With all this in mind, I will briefly cover two blockchain projects that have the potential to extend the capabilities of Bitcoin and, implicitly, any other robust public blockchain: The Lightning Network and The Polkadot Network. Bitcoin has almost certainly won the race to be sound money. Nothing truly ‘competes’ with it. But it also need not exist entirely on its own. Just as nobody gets excited bouncing packets around the network layer of the Internet, but really enjoys watching Netflix, Bitcoin will have truly succeeded when you have no idea you are using it. And so, the most important thing to take from this discussion is not an endorsement of Polkadot or Lightning specifically or exclusively, but to get the reader thinking about the broader concept of layered and interoperable protocols, of which there are - and will be - many. I only mention Lightning and Polkadot because I know the bare minimum about each to say something sensible. Apologies if it’s still questionable …

The Lightning Network is what has come to be known as a ‘layer 2’ protocol, in that it sits ‘on top of’ Bitcoin in a more or less metaphorical sense. I won’t go too far into the technical details here but what this means is that Lightning is a peer-to-peer network of Bitcoin transactors, whose transactions are not being recorded in the Bitcoin blockchain but which are subject to a cryptographic system enforcing *eventual* settlement in the blockchain. The goal of the project is to get around Bitcoin’s ‘scaling problems’ without corrupting the Bitcoin protocol itself. It is early days, but transactions on the Lightning network appear to be instant, basically free, and scale well with the size of the network. There is also an ingenious incentive system that allows honest and cooperative parties to continue to transact off the blockchain indefinitely, but for dishonest parties to be punished by a financial loss that is settled on the blockchain immediately. Counterparty risk is completely removed by all parties staking collateral that they will programatically lose if they lie.

This may sound too good to be true, and in a sense, it is. There are two enormous caveats relating to any real-world application. The first is that the service is clearly only as useful as Bitcoin itself. In addition to the technical issues with scaling, another obvious reason people don't regularly transact in Bitcoin (although some do) is the volatility of the price relative to fiat. Lightning solves the key technical problem with transacting in Bitcoin, but not the key financial problem. If anything, it might make it worse, as the second caveat is that involvement in the network requires placing some amount of Bitcoin in a kind of cryptographic custody—ideally slightly larger than the maximum expected net negative balance of the participant at any single moment during the period of participation. This both increases the exchange rate risk—which, recall from above, didn't originally exist for many uses cases of Bitcoin as a currency proxy—and creates a potentially enormous working capital drain on any business wanting to implement this payments channel. Perhaps weirdly, it is not a zero-sum working capital drain across the economy; one participant's accounts receivables are not another's accounts payable. Everybody has accounts receivable from having sunk collateral into the Bitcoin blockchain to enable the incentive mechanism that prevents them from interacting with the network dishonestly. In summary then, nearly free and instant payments, but for a different kind of price.

Consider, however, that this price may very well be worth paying if it enables behaviour not previously possible. Who would want to transact for free? We don't really know because it has never been possible to send less than around $10 without the fee being an exorbitant portion of the transaction. In mimicking tipping at the very least, online micropayment ecosystems could enable fairly large markets, or expand already large ones. Who would want to transact instantly? Visa allows between 40 and 60 thousand transactions per second. Bitcoin allows 7. Lightning allows billions. To ask a better question, then, who would want to transact billions of times per second? Machines. This is a whole other (probably fractal) rabbit hole that I will leave it to the reader to go down on their own if they so desire. But as Andrew Miller of the ZCash foundation put it,



Andrew Miller 🦓🦓🦓
@socrates1024

#InternetOfThings is when your toaster mines bitcoins to pay off its gambling debts to the fridge

♡ 1,067 9:16 PM - Oct 19, 2015

1,106 people are talking about this

*The Fractal Rabbit Hole of Bitcoin. Great idea by **Miles Suter**. Not so great graphic design by me.*

Who wants to transact instantly *and* for free? Well, the W3 Consortium abandoned an effort in the mid-90s to extend HTTP to enable Internet native payments—I wouldn't be at all surprised if this is revived if or when Lightning proves it can scale.

Polkadot is an interchain protocol, among other things enabling interoperability between blockchains. They refer to this as a 'heterogeneous multi-chain framework', which intriguingly ought to work for blockchains of all kinds: public, private, whatever Libra is, or some new thing not yet invented. The obvious analogy is between intranets and the Internet, with Polkadot providing a kind of universal data transfer API (I'm not sure how wedded I am to this analogy, but for those familiar with it, Polkadot strikes me as very similar to Mulesoft, but open and public, rather than within an organisation, and for all manner of blockchains) The functioning of this communications layer abstracts away from the conceptualisation I put forward here of the transferable data on a blockchain constituting a balance exchanged for a computational service, to the idea of a 'message', which is a data transfer of any kind between blockchain nodes. This may or may not be a token transfer. Furthermore, the transfer may be between wallets (or contracts, or however they are stylised) on different blockchains. In fact, Polkadot encourages this. I mentioned above that Bitcoin is 'programmable to a small degree'. It is not worth explaining exactly why or how this is the case—although actually the small degree to which it *is_the case is what lets Lightning work—but an exciting implication of Polkadot is that it really needn't be _at all*; the programmability can exist somewhere else, on some other blockchain, and tied to Bitcoin via Polkadot.

The implication is that novel ideas around the utility of markets for scarce data need not come in the shape of endless fully formed decentralised computers that really only exist for one specific task. They can be far lighter, but if they require a store of value, they can tie in Bitcoin; if they need free and instant payments, they can tie in Lightning; if they need smart contract execution, they can tie in Ethereum, Tezos, EOS, etc. An analogy to cloud computing is apt. If you have an idea for an app, you may choose to let AWS deal with the infrastructure of storage and compute, within which you can run Kubernetes and Docker; you can let Stripe deal with payments, which you can implement directly, or perhaps go through Wix, in which case Stripe and AWS may well be working in the background; you can build your front-end store on Shopify, or maybe the whole thing, in which case Shopify will do all of the above for you, and so on and so forth, up and up the interlocking layers. The situation in cryptoland is not quite as generous, in that the services you need are not guaranteed to exist, or if they do exist, they are not guaranteed to be effective or robust. But Polkadot will hopefully at least let you utilise them extremely easily.

I find this particularly exciting for Bitcoin—and the idea of money and banking in general—because of what money *means*: universal credit. Almost any activity can be designed to have a monetary component, which is really only to say that people value the time devoted to their labour, while others value the product of that labour, very probably in the form of capital that will multiply *their_labour, and so on and so forth, up and up the interlocking layers. Therefore, Bitcoin—the most secure form of value settlement ever invented—and Lightning—which builds on top of this layer to provide free and instant transfer of that value—can potentially be used in combination with Polkadot to provide either a value-storage or payments functionality to any kind of wonderful, _free and open source, new kind of computer, decentralised corporation that can be imagined*:

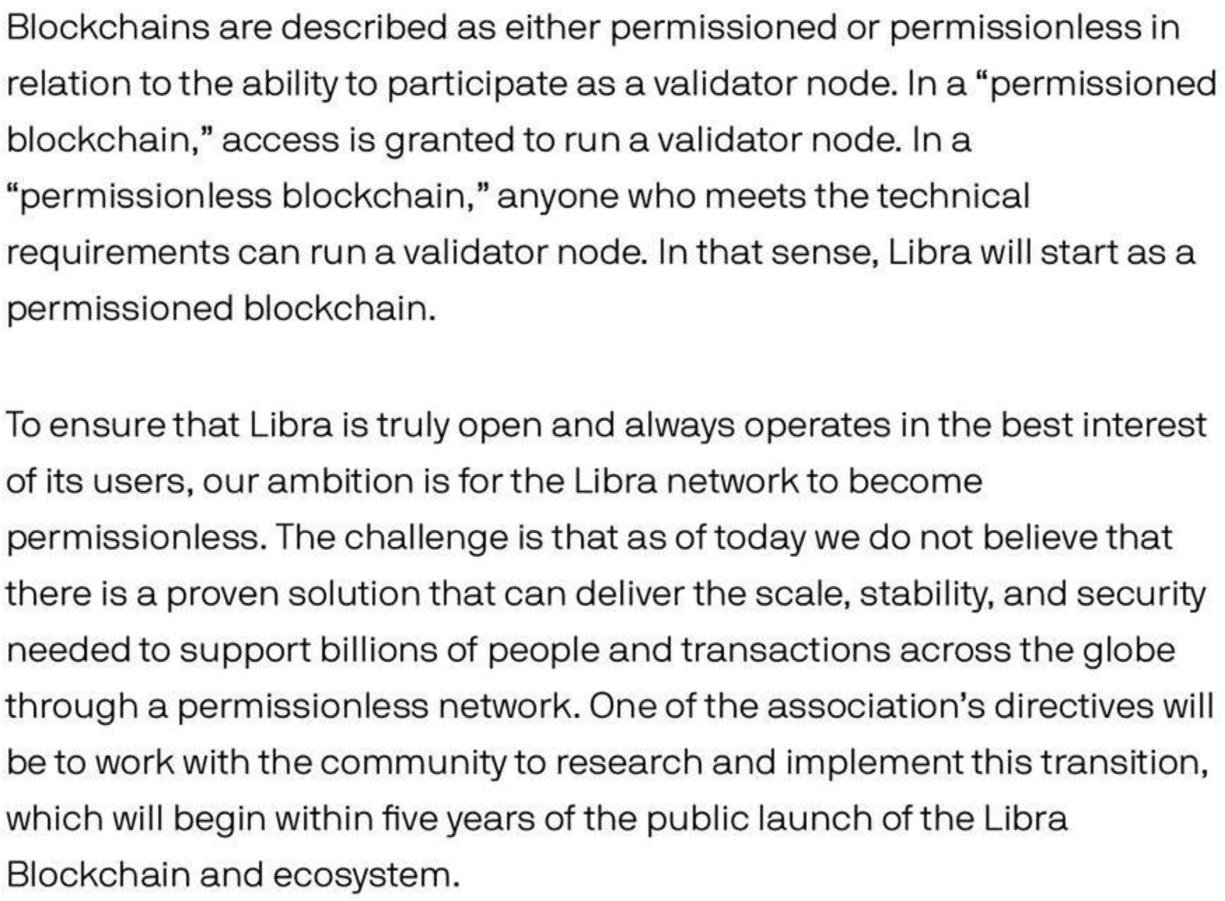
The Conceptual Blockchain *blockchains are combinations of three concepts: a new kind of computer, an open source software project, and a…* medium.com

Photo by **Con Karampelas**, via Unsplash

Libra

Of course, this all brings us to Libra. I have three main points to make in order to adequately compare Libra to money, banking, and Bitcoin. We might call them the good, the bad, and the ugly, although unfortunately I won't treat them in that order. The bad is that the Libra data structure is a database, not a blockchain, and the Libra consortium is a hedge fund, not a network of nodes. The good is that Libra will acclimatise billions of people to digital bearer assets, and may be a force for great social good in the short run. The ugly is that it will be a force for great social evil in the long run.

That Libra is not a blockchain is really just a technicality, but it is worth disabusing anybody who has been fooled by clueless journalists. Libra is a distributed ledger that is an attempt to mashup the most palatable parts of Bitcoin, Ethereum, and Ripple, but none of the parts that make them truly revolutionary. It is very technically interesting, and if it works, it will be an incredible technical achievement, but it is not a blockchain. This matters for more than linguistic reasons; the Libra data structure *may* be open and *may* be private, but will definitely not be neutral or permissionless, and the tokens will not be sound. This wouldn't be worth stressing so much if both the officialand technical white papers didn't constantly misuse the words 'blockchain' and 'cryptocurrency'. After each of the following extracts, I provide a translation,

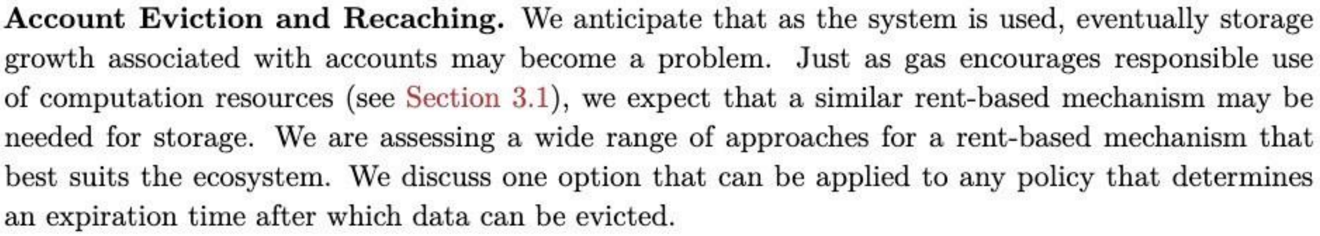


Blockchains are described as either permissioned or permissionless in relation to the ability to participate as a validator node. In a "permissioned blockchain," access is granted to run a validator node. In a "permissionless blockchain," anyone who meets the technical requirements can run a validator node. In that sense, Libra will start as a permissioned blockchain.

To ensure that Libra is truly open and always operates in the best interest of its users, our ambition is for the Libra network to become permissionless. The challenge is that as of today we do not believe that there is a proven solution that can deliver the scale, stability, and security needed to support billions of people and transactions across the globe through a permissionless network. One of the association's directives will be to work with the community to research and implement this transition, which will begin within five years of the public launch of the Libra Blockchain and ecosystem.

"Libra is a permissioned database. We will think really hard about how to transition it to a permissionless database but unfortunately we don't really like the only known way to do that."

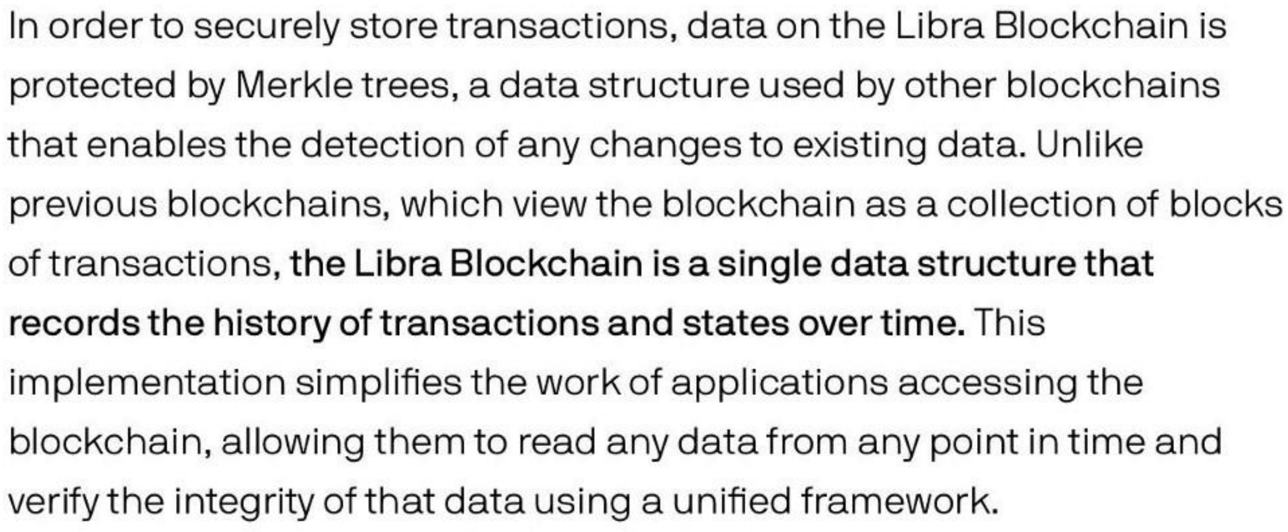
And,



Account Eviction and Recaching. We anticipate that as the system is used, eventually storage growth associated with accounts may become a problem. Just as gas encourages responsible use of computation resources (see Section 3.1), we expect that a similar rent-based mechanism may be needed for storage. We are assessing a wide range of approaches for a rent-based mechanism that best suits the ecosystem. We discuss one option that can be applied to any policy that determines an expiration time after which data can be evicted.

" *There are some really difficult unsolved problems in the theoretical underpinnings of scaling open blockchains. We also don't know how to solve them.*"

And,



In order to securely store transactions, data on the Libra Blockchain is protected by Merkle trees, a data structure used by other blockchains that enables the detection of any changes to existing data. Unlike previous blockchains, which view the blockchain as a collection of blocks of transactions, **the Libra Blockchain is a single data structure that records the history of transactions and states over time.** This implementation simplifies the work of applications accessing the blockchain, allowing them to read any data from any point in time and verify the integrity of that data using a unified framework.

"Just to be extra clear: the Libra blockchain is a database of validator-signed ledger states with a Merkle tree of the historical states - not a blockchain."

Given Libra the data structure is not a blockchain, we must then wonder what the Libra consortium is, given it is clearly not a network of nodes. *A collection of transaction validators* is accurate enough, but a little dry. It is a lot more revealing to describe it as a hedge fund.

The way it looks like the Libra 'token' will come into existence will be in exchange for deposits from users. You will send the consortium fiat over existing payment rails, and they will mint some 'Libra' and give it to you, and you can cash in your Libra for fiat and they will 'burn' the fake money and return your fiat (the feature of having different names for the data structure and the tokens is not one of the better parts of other blockchains implemented here). The 'nodes' are really processing centres, in that they need to contribute a minimum of computing power to handle the transactions being submitted. It all sounds very communitarian until you realise that what is in it for them is interest on the deposits of real assets 'backing' the digital assets issued. In order to maintain price stability, these deposits will be invested in the government bonds of the fiat currencies against which Libra is desired to be stable.

This is worth pondering as it is really quite incredible. Libra is going to have zero cost of capital on funds it will lend at the risk-free rate. Despite strictly speaking being total nonsense, the 'risk-free rate' *ought* to be the lowest rate it is possible to borrow at, hence governments borrowing at this rate and not an even lower one. Because Libra has an even lower borrowing cost (none), it can *lend* at the risk-free rate and earn an arbitrage profit on what will almost certainly be the largest pool of capital ever collected by a corporation. In the above vein of banking theory, it is worth considering that Libra will only need petty cash / liquidity / working capital / however you want to conceptualise it, of the most extreme net negative redemption of Libra to fiat, multiplied by the settlement period of government debt, which in most cases is one or two days. This will almost certainly be utterly trivial compared to the market valuation of minted Libra at most times, and given the intention to charge transaction fees, may actually be completely irrelevant since fees can be dynamically matched to real time outflows even while remaining miniscule. So Libra will be an almost artificially highly leveraged hedge fund. What's more, it will be a perfectly safely leveraged one, because the assets will be both the highest quality in existence and perfectly liquid. Neither banking risk will exist. This is astonishing.

How it achieves this hedge fund like status is worth exploring because it is the source of both the great social good and great social evil that will likely follow— assuming it works, or is allowed to work. My hunch is it won't be allowed to work at all, so I would take much of the juxtaposed utopianism and *dys* topianism below with a pinch of salt.

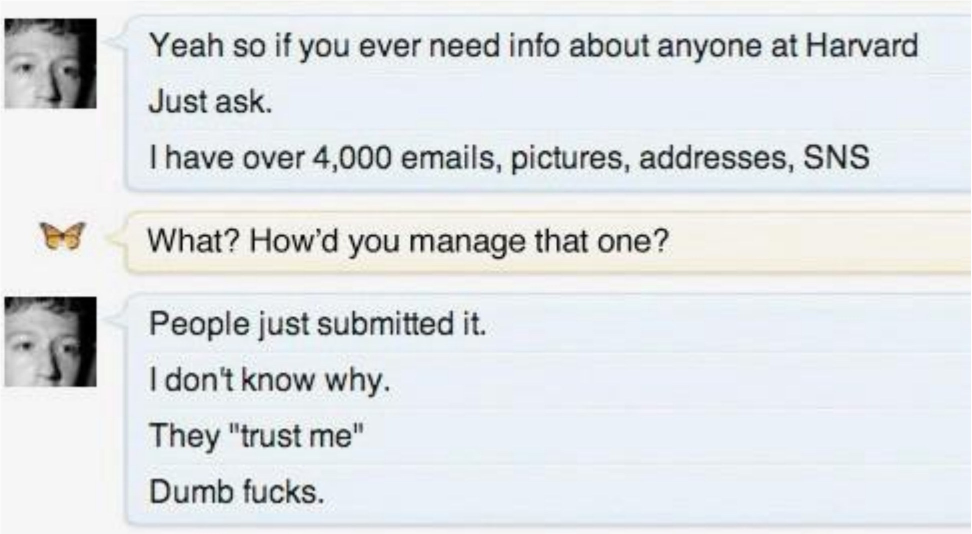
Every Libra bought will either represent a Dollar/Pound/Euro/Yen given to Libra and invested in government debt denominated in those currencies, in which case who cares, or it will be something else, in which case things get very interesting. A WhatsApp user will transfer their Indian Rupee, let's say, to Libra in exchange for digital money. Libra will then sell Rupee for Dollar on the FX market to gain the fiat to back the Libra. This will cause the Rupee to depreciate relative to the Dollar/Pound/Euro/Yen, making it more difficult to raise capital in Rupee and easier in Dollars, making Libra *even more* viable as a medium of exchange, on top of the worldwide networked marketplace in which it is already exclusively accepted by fiat. The role Libra will be playing is the FX broker-dealer that 'dollarizes' emerging markets and immediately provides an economy in which the the hybrid Dollar/Pound/Euro/Yen can be spent.

This could initially be a great social good, for three reasons. Firstly, we should not underestimate the dramatic difference this could really make to the billions of unbanked around the world who can afford a phone but not a bank account—and the hundreds of millions more who have bank accounts that achieve nothing given their monetary wealth is consistently inflated away. Additionally, the smart contract elements of Libra could allow for programming of cross border business logic that would previously have been impossible due to combinations of illiquidity, inflation, and capital controls. Facebook's rhetoric around empowerment, while suspicious to the point of hilarious given its coming from Facebook, is probably entirely accurate in this case. This could be tremendously beneficial to those living in monetary regimes that are inept, corrupt, or both.

Secondly, Libra is arguably a necessary experiment in the development of the banking of digital assets. It is a simple and natural step to first trial a digital asset backed by fiat that, however philosophically flawed, is actually used as money currently. There are fewer degrees of freedom than a bank of a novel digital money backed by Bitcoin, and yet the lessons learned will obviously be relevant, be they technical, economic, or social. This will be truer the more genuinely open Libra turns out to be, since the experiment will not be of the viability of Libra and banking of digital assets alone, but of every other open system that connects to it to incorporate Internet-native money, contracts, and so on. Libra will be psychologically safer to build on to begin with, but via the likes of Polkadot will open the door to Bitcoin, Ethereum, and more.

But the third and most important reason is that in addition to developers and entrepreneurs, Libra will acclimatise billions of regular people to digital bearer assets. Minds.com founder Bill Ottman put it well in a recent interview, " *it's not Bitcoin, it's not Ethereum, but maybe it's a weird bridge? It's a weird bridge which you don't necessarily know whether or not it will collapse as you are walking over it*." The acclimatisation will be particularly important when the dream of dollarized digital money *collapses_into the nightmare of corporate neo-feudalism. Some readers may have winced at my positive invocation of 'dollarization', given its connotations of monetary imperialism. They would have been right to do so had they thought my enthusiasm was unequivocal. But notice I only ever said 'could', not 'will'. This _could* be a great social good, but it will likely devolve into a great social evil. If you think the monetary imperialism of the United States of America is bad, wait until you see the monetary imperialism of a corporation that actually makes a profit.

If you believe that Facebook will never use your activity with Libra to better serve you ads, you are delusional. They won't do it right away, for sure. They said so in the white paper. But there is absolutely nothing about this technology that enforces this promise. It's a promise from this man:



Yeah so if you ever need info about anyone at Harvard
Just ask.
I have over 4,000 emails, pictures, addresses, SNS

What? How'd you manage that one?

People just submitted it.
I don't know why.
They "trust me"
Dumb fucks.

n.b. this is real, not a joke or a fake. **see here** for more.

What is particularly perverse is that Facebook has a legal obligation to its shareholders to follow this path. The board of directors will be failing in their fiduciary responsibility if they do not encourage Mark Zuckerberg to direct Libra to behave in this way. Which, of course, he can. Libra is not an open, permissionless, neutral, private, sound money like Bitcoin. It is corporate money. It will work better than government money but it will turn out to be even more insidious. If you are actually adding value with your service relative to a useless competitor your customers previously had no choice but to use, you generate an enormous amount of goodwill you can later rapaciously exploit.

Which means there will be mass surveillance and data leaks. Even without leaks there will be deanonymization of the transactional graph. There will be purges, and censorship, and confiscations of wealth. Facebook will control enough economic activity to dictate monetary policy to economically weaker nations. This won't be in the form of direct confrontation—it will be a system upgrade that *optimises* something or other that within a few days sees yet more value sucked into lowering the cost of funding the governments of the largest economies in the world—those that have meaningful power over Facebook, the corporation—and a few days after that the power of every other government to affect the economic goings on within their own borders. Shades of this may sound ideal and romantic, but this is not a stripping of the power to interfere with the activity of willing individuals—it is a *transfer* of that power to Silicon Valley.

Much of the above few paragraphs consist of the worst possible dystopian outcome. I seriously doubt anything like all of this will happen in its entirety, but there will come a point when it becomes obvious that it *could* happen. The steps to roll back Libra's power to ensure that it doesn't happen will not be pretty. And the fallout will see a great many disillusioned people turning to money that *is* open, permissionless, neutral, private, and sound.

Which is what we wanted all along.

Thanks to Nic Carter for help with editing, and Andreas M. Antonopoulos for his recent talk in Edinburgh, which inspired parts of this post.

follow me on Twitter @allenf32

Full Reserve Banking with Bitcoin

By Tamas Blummer

Posted June 28, 2019

Unchecked inflation of money supply through fractional reserve is creating a mess in the world we live in. Bitcoin could overcome this mess implementing this proposal!

Fractional Reserve Banking

The fiat currencies we use nowadays come into existence by someone borrowing them. To illustrate the mechanics let's consider the case of Bob who buys a house with a mortgage loan. This implies the following series of events:

1. Bob signs a mortgage contract with Alice the banker.
2. Alice ensures that she has the right to sell the real-estate in case Bob would fail to follow terms of the contract. How she achieves this depends on jurisdiction, not relevant here.
3. Alice credits the account of the seller of the real-estate with the selling price, that is also the notional amount of the mortgage.
4. Bob regularly pays installments that cover interest and partial redemption of the mortgage until the notional amount is fully paid back through the redemptions.
5. If all goes well till end then Alice forgoes the right secured on the property, if not she uses the right to recover her loss.

This is all fine, but there is a disturbing detail in step 3. where does Alice have the money from that she debits to the seller? In our current banking system Alice simple creates it. Yes, this is completely legal until Alice does not violate a long list of checks mandated by banking regulators, mostly aimed to ensure that the amount of money Alice creates does not exceed a high multiple of her own capital and deposits under her control. This is called fractional reserve banking. The money created this way will be gradually destroyed again through Bob's redemption or if he fails by the forced sell price.

If you think this is crazy, then consider that even the money Alice has is created the same way. Alice actually borrows that money from the central bank whereby she provides some collateral. The collateral may well be a so called ABS that re-packaged Bob's mortgage agreement with many others.

There is no hard limit on the amount of money such system can create. The soft limits are regulated ratios and the bank's capability to get people signing further loans that they can also honor, so the bank can afford to pay interest to the central bank. The later is not a hurdle nowadays as some central banks lend at 0% interest.

Wait, it gets even more crazy. Credits that fail, reduce the value of bank's collateral and thereby would force them to reduce their own borrowing from the central bank which would curtail their ability to create credit which would slow down the economy and therefore cause even more credits to fail. To avoid that central banks got more creative recently and begun to buy assets that represent troubled credits at prices no one else would pay, thereby pumping or at least maintaining their value. They even invented a "Modern Monetary Theory" to justify all this.

It is evident that such a system is bound to create an ever increasing amount of debt and the measures that central banks do to underpin it only delay the inevitable collapse of the scheme at latest at the point where all prices of credit become meaningless. Guess what, we are pretty close to that. A huge fraction of government debt is trading at prices that makes them yield negative returns. That is the sum of interest and redemption does not cover the selling price.

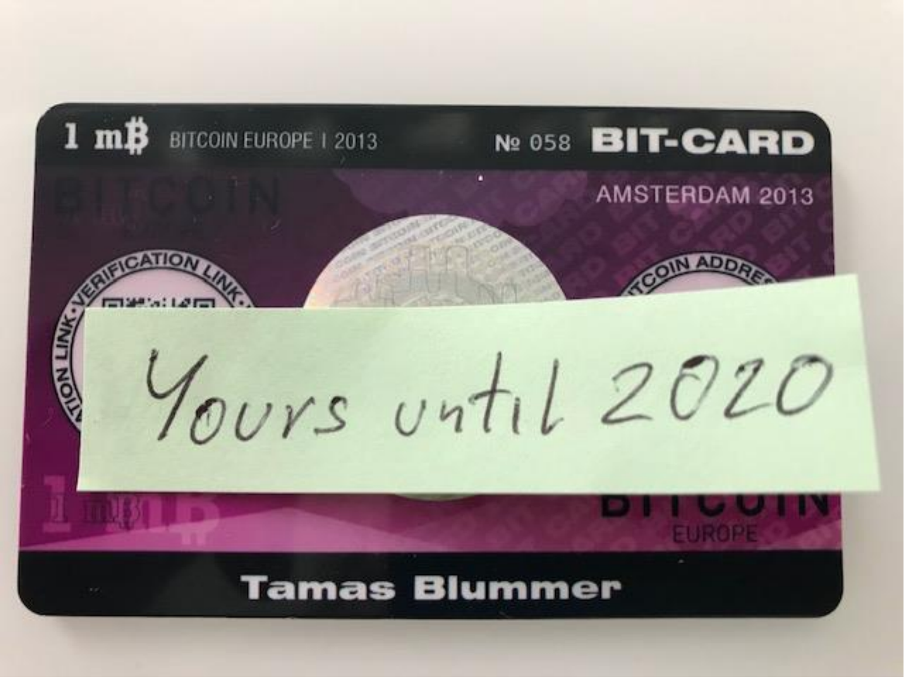
All above was an introduction, so you understand why we need an alternate way of doing lending, so a Bitcoin economy does not end up in the same trap.

Full Reserve Banking

Full Reserve Banking is where banks are no longer allowed to extend loans in excess of their own capital. Before gold receipts were introduced, this was the way banking worked.

Not only historians have interest in full reserve banking, but is seen by many people including some economists as an alternative to fractional reserve banking that we should stop for previous reasons. The most prominent move into this direction was a recent popular vote in Switzerland to mandate full reserve banking to all Swiss banks, that achieved 24% support of voters.

Bitcoin credits



Bitcoin as is is digital cash. It does not mandate any form of banking it might be used in. Although there is a fixed supply of Bitcoins nothing yet enforces a limit on credit denominated in Bitcoins. This could lead to the very same problems in a Bitcoin economy, we currently see elsewhere.

We have seen repeatedly that e.g. Bitcoin exchanges operated a fractional reserve scheme, some collapsed as customer demanded their deposit and some are still getting away with it.

One way to keep check on Bitcoin businesses is requiring proof of reserves, that is like a public audit cryptographically proving that the Business had at a certain time point access to a number of Bitcoins.

Proof of Reserves is not much better than traditional audits as it does not give a guarantee of ongoing ordinary business, just shows a picture that could have been painted temporarily for the time point of the audit.

Credit Covenants

The best solution would be if every Bitcoin credit would carry its own proof that it is covered by reserves all the time.

It turns out that this is technically possible with implementation of the proposal I posted today to the Bitcoin developer mailing list. There you have the technical details, for which I give a higher level description here.

On the technical level Bitcoins exist as unspent transaction outputs UTXOs. Transactions merge and split UTXOs to new UTXOs. One could consider an UTXO a coin of certain amount. An coin can be spent by someone if able to satisfy any of conditions that the coin is programmed to accept.

Giving credit to someone means transferring coins to him and hoping to get them back. Such a deal requires trust, since the borrower could be dishonest or bankrupt by the time the credit should be re-paid.

It was a great option if we could programmatically ensure that the coins will be paid back. We can achieve this by assigning a condition to the coin such that the lender can take it again later. Next we have to ensure that this condition is inherited by any coin that arises from splits or merges of this borrowed coin.

The technical means to do that is to assign a credit covenant to the coin that forces descendant coins to offer the same option to be taken later by the lender.

Do coins encumbered with a credit covenant have a value? They represent exclusive but temporary access to a scarce resource. I intuitively think yes, but the answer will be given by the market. An analogy to support my intuition is land that is not sold but rented for a longer term. If land is scarce then people will pay to take over a previously agreed rent contract.

The idea of covenants was first introduced in a paper suggesting a solution for Bitcoin Vaults. I generalized the idea to be compatible with the taproot proposal and provided examples how it can be used to technically enforce full reserve banking on the mailing list.

I know hope that the community understands the importance of full reserve banking and that we developer work together to complete and deploy this proposal on the network.

Correction: the first discussion of covenants is probably this post on bitcointalk.org.

Tweetstorm: Bitcoin is Secure Money

By JW Weatherman

Posted June 29, 2019

1/

"… all money mankind has ever used has been insecure in one way or another.

This insecurity has been manifested in a wide variety of ways, from

counterfeiting to theft,

but the most pernicious of which has probably been inflation."

-@NickSzabo4

2/

This is why should abandon the muddled term "sound money" and instead say "secure money."

#bitcoin is the first secure money.

This is a massive milestone for humanity.

3/

Bitcoin isn't special only because it's digital or is scarce (stock to flow) or is easily verified or…

It's special because it has ALL of the necessary attributes of an asset ideally suited for use as money.

In other words it's hard to steal. It is secure.

4/

Inflation is theft from savers.

Counterfeiting is theft from buyers.

Fractional reserves is theft from depositors.

Taxation is theft from producers.

Storage and transportation costs are high when it's easy to steal from savers.

5/

Gold and Fiat have known critical security flaws.

Bitcoin doesn't.

Bitcoin is so much easier to secure than anything prior it deserves the distinction

"Secure money"

6/

If a more secure money is discovered it will certainly be digital (because that's far easier to secure)

So Bitcoin will simply copy those useful attributes

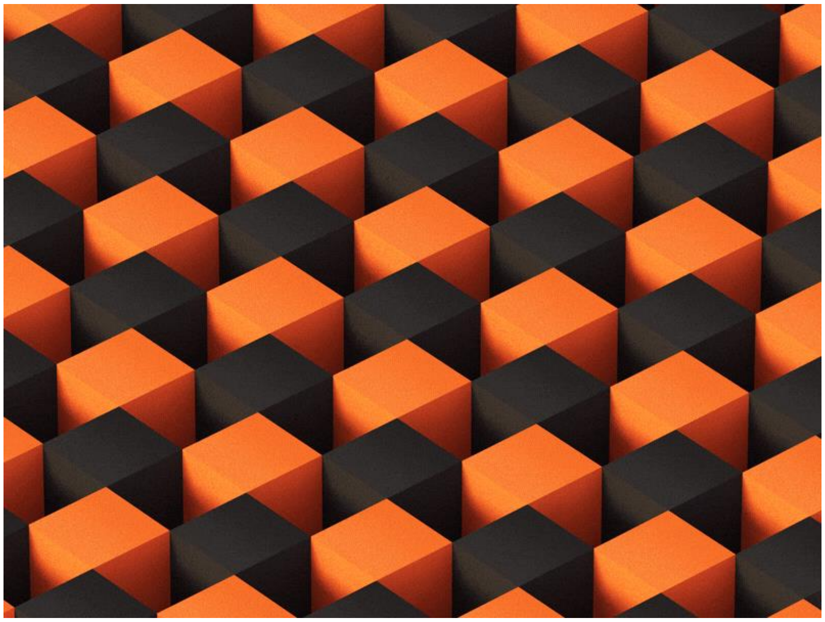
While retaining the UTXO advantage

So as long as history endures we will have a "secure money" called #bitcoin

Statechains: Non-custodial Off-chain Bitcoin Transfer

By Ruben Somsen

Posted June 4, 2019



This article introduces Statechains, a novel layer two scaling protocol for Bitcoin with some unique features. We'll go through its strengths and weaknesses, look at how it integrates with the Lightning Network, and discuss the privacy implications of combining it with Blind Signatures.

I first unveiled my concept of Statechains by presenting it at Scaling Bitcoin in Tokyo. Since it was a technical conference, my presentation was not focused on a general audience. As a result, it has largely gone under the radar, which is a shame because it's a unique layer two protocol with useful features that can strengthen the Bitcoin ecosystem. Hopefully this article can convince you of its merits. Note that this article is high-level and won't have all the technical details. If you want those, please refer to the talk, paper, and mailing list post.

Statechains are a layer two protocol, meaning it enables the transfer of value without burdening the Bitcoin blockchain. This can help with scaling and save fees. Unlike Lightning it is not trustless, but it maintains a high degree of censorship resistance (more so than federated sidechains) due to the fact that withdrawing on-chain is permissionless.

The basic idea behind Statechains is that you lock up money between two parties in a 2-of-2 multisig: the **Statechain entity** and the user. When the user wants to transfer the money (the entire UTXO), they simply hand over their private key, which we call the **transitory key**, to the intended recipient.

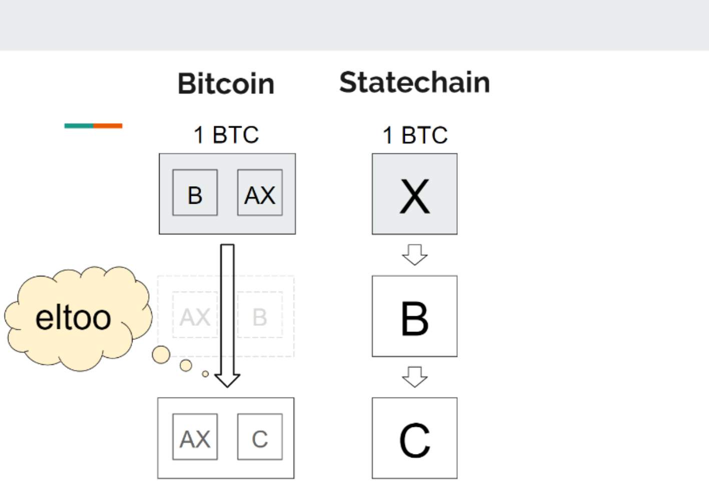
And that's basically it. There is a lot more complexity operating in the background to decrease the potential for cheating, but in a nutshell this is the core concept, and as you will later see, it's deceptively powerful.

Non-custodial, because the Statechain and Bitcoin blockchain get updated in tandem (atomically)

In essence, the money is controlled by the Statechain entity and *all* the users who know the transitory key. The Statechain entity could theoretically move the money in cooperation with _any_of the users, but simply promises to only cooperate with the _last_user that received the transitory key. One thing the Statechain entity _cannot_do, is move the money on their own.

Let's take a look at the weaknesses. If the Statechain entity goes offline, loses their key, or refuses to cooperate, is the money gone? No. Every time the money changes owner, an off-chain transaction is also generated. This allows the last recipient of the transitory key to redeem their coins on-chain without the assistance of the Statechain entity. The Statechain entity simply cannot hold your money hostage.

Each time the money moves on the Statechain (B to C), an off-chain Bitcoin transaction is created. We use eltoo to ensure that only the final recipient can withdraw the money, without the help of the Statechain entity.



Can the Statechain entity still cheat by colluding with one of the previous users that know the transitory key? Yes they can, but chances of this happening are minimized for the following reasons:

- We keep the Statechain entity honest by making sure they disclose every signature they make (via clever use of Adaptor Signatures). Any attempt to cheat by the Statechain entity would immediately become apparent.
- The Statechain entity isn't actually a single entity, but a federation — a group of members (e.g. 8-of-12 multisig) of which a majority has to agree in order to cheat. This security model is comparable to federated sidechains such as Liquid, with the added benefit that users can withdraw _without_permission.
- Every UTXO has a different transitory key and a different set of prior users. To steal all the coins, the Statechain entity (or a hacker) would have to find prior

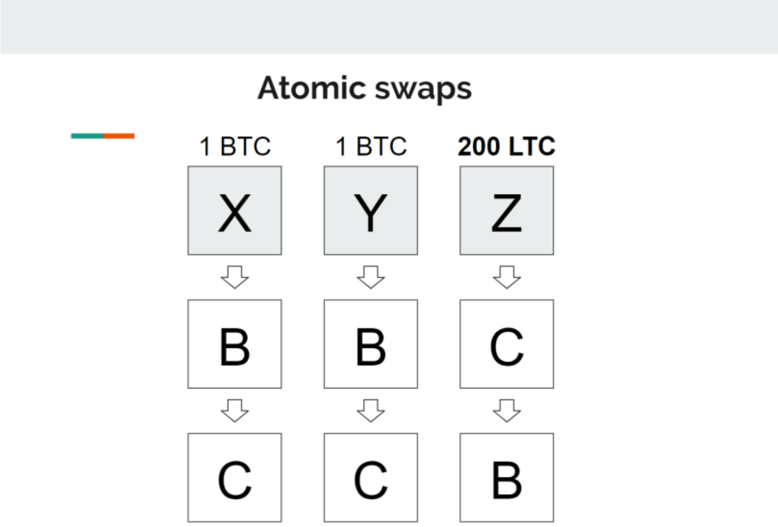
users that are willing to collude for every UTXO. In the unlikely event of theft, it is therefore likely that only a subset of coins gets stolen.

Are Statechains custodial? Surprisingly, they are *not*. This is one of the key distinguishing features of Statechains. If a court ordered the Statechain entity to confiscate someone's coins, they simply wouldn't be able to comply, since they only have one of the two keys. They can't freeze the assets either, because the owner can always redeem the coins on-chain without their help. There is also no risk of fractional reserve, forcing hard forks upon users, or other issues that are commonly associated with custodial control.

One unique feature of Statechains is that it operates at the level of the UTXO. This has some interesting consequences:

- UTXOs are transferred in full: if you lock up 1BTC into a Statechain, you have to transfer that full amount, but bigger UTXOs can always be traded for smaller ones (e.g. 2x 0.5BTC for 1BTC)
- You can swap multiple same-value UTXOs with users, which is equivalent to a coinjoin to increase privacy, particularly when done over Tor
- Lightning channels can be opened on top of Statechain UTXOs in order to enable smaller payments (see the next section for details)
- Betting/oracle protocols that require UTXO ownership can be performed efficiently (e.g. 2-of-3 multisig,Discreet Log Contracts)
- Non-fungible colored coins on the Bitcoin blockchain can be transferred off-chain via Statechains (e.g. RGB)
- User verification of payments scales better than sidechains, because coin history is linear, so you only need to verify the history of the exact coins that interest you

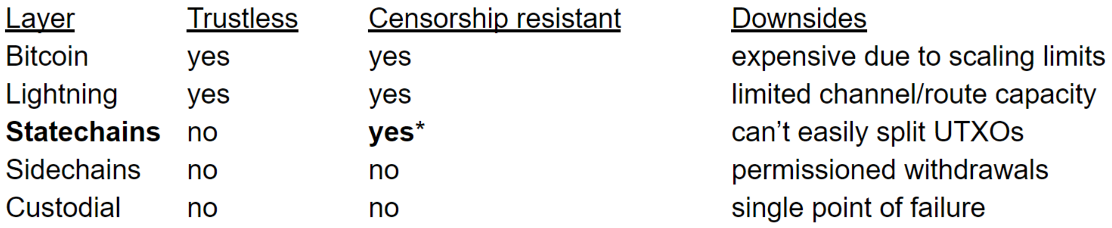
The key insight here is that anything that requires creating one or more new Bitcoin UTXOs, can now be done off-chain via Statechains. It's also worth noting that Statechains are chain-agnostic, meaning it's possible for a Statechain entity to manage UTXOs from different blockchains and allow users to trade between them (not unlike a DEX).



An example of a swap with different assets. User B trades his 2BTC for 200LTC with C.

As I recently argued on Twitter, Bitcoin has no choice but to scale via the second layer. It is therefore absolutely crucial that this kind of technology gets built. We need many different layers that make different trade-offs, so people can pick the layer that best suits their needs.

Here is an (admittedly over-simplified) overview of where Statechains fit in:



Layer	Trustless	Censorship resistant	Downsides
Bitcoin	yes	yes	expensive due to scaling limits
Lightning	yes	yes	limited channel/route capacity
Statechains	no	**yes***	can't easily split UTXOs
Sidechains	no	no	permissioned withdrawals
Custodial	no	no	single point of failure

It could be argued that a layer cannot be truly censorship resistant if it isn't trustless — the coins could still potentially get stolen, even if unlikely.

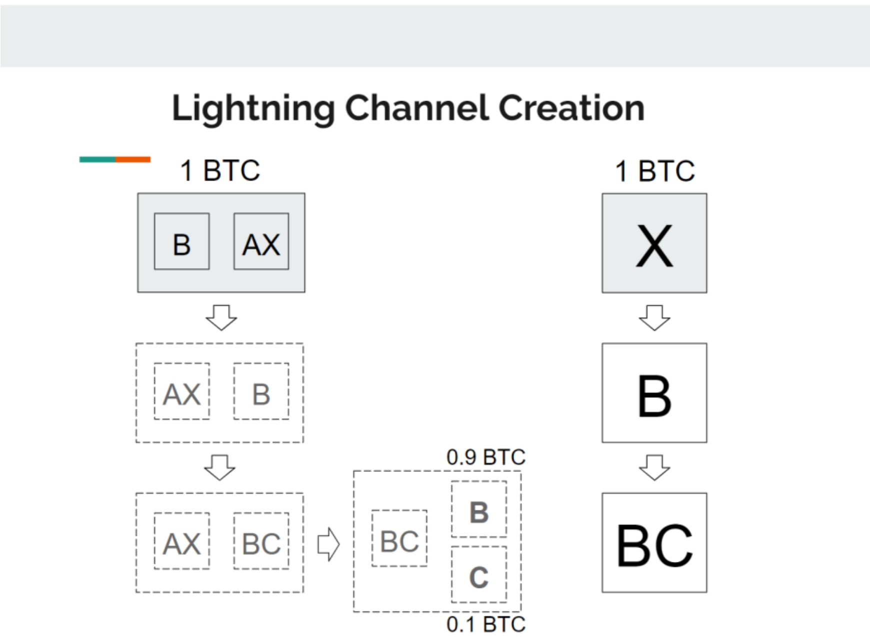
In short, Statechains are novel in the sense that they allow you to change UTXO ownership off-chain, while preserving a large degree of censorship resistance due to the ability to withdraw on-chain. It is non-custodial, which naturally reduces risk and makes it easier for the Statechain entity from a regulatory point of view. The end result is a unique layer two protocol with its own distinct strengths and weaknesses.

Statechains and The Lightning Network

One particularly powerful feature which I already alluded to but deserves further examination, is the interoperability between Statechains and the Lightning Network. In order to open a channel on the Lightning Network, you need to obtain a UTXO on the Bitcoin network and share its ownership with someone via multisig. Statechains provide this exact functionality: any UTXO that exists on a Statechain can be turned into a Lightning channel at any time.

The beauty is that this is kept completely hidden from the Statechain entity. All the entity sees is that the entire UTXO got transferred, but they are entirely unaware that this is actually a 2-of-2 multisig Lightning channel. The two protocols are kept completely separate. The Statechain entity doesn't need to be involved, even when forced on-chain closure occurs.

The channel can be opened on the Statechain without the help or awareness of the Statechain entity.



By utilizing Statechains, you get to open and close channels off-chain at minimal costs. Is your channel too small? No problem. You can simply transfer your existing channel over to a larger UTXO. This can be particularly powerful considering it's hard to know ahead of time how much capacity will be needed in a channel. Now you can cheaply experiment, and once you have a stable channel, you could choose to effortlessly move the channel over to the base layer by exiting from the Statechain.

Another really potent consequence is that Statechains enable you to on-board people onto the Lightning Network instantly. If you have money on a Statechain, you can immediately send a portion of it to a friend by turning the Statechain UTXO into a shared Lightning channel. And if your friend prefers to minimize their exposure to the Statechain entity, you could directly move the channel on-chain.

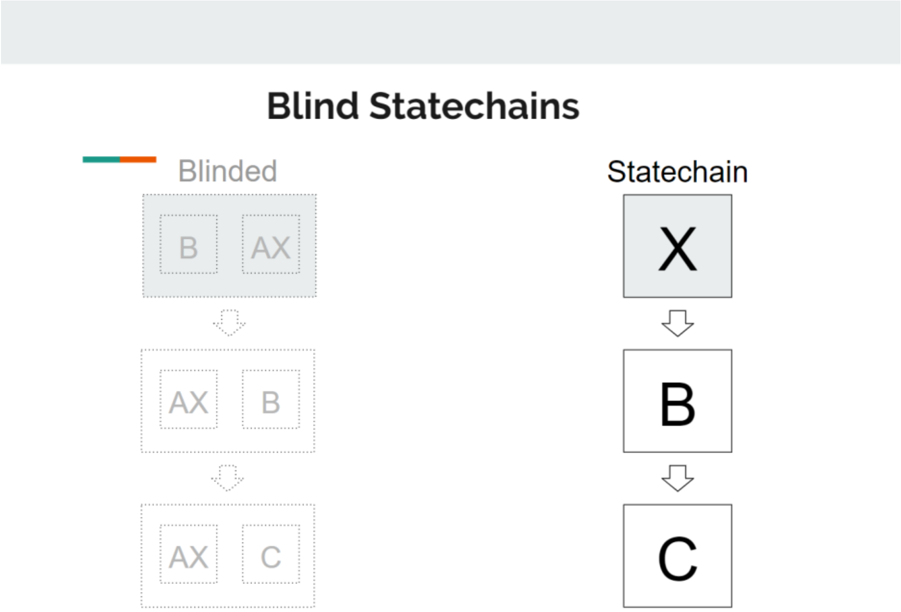
One more interesting feature that Anthony Towns and Olaoluwa Osuntokun alerted me to, is that when you open a Lightning Channel factory via a Statechain, adding or removing people from the factory can occur without on-chain friction, making it far more flexible.

Enhanced Privacy with Blind Statechains

Statechains, as described thus far, limit the control the Statechain entity has over its users, but does allow the entity to learn a lot about every transaction, and most of this information gets transparently published for the world to see. Engaging in the Statechains equivalent of coinjoin helps mitigate this to a large extent, but we can do even better!

Blind signatures can make the Statechain entity completely unaware of what they're signing. The transactions would become entirely unseen — it would literally not be possible to tell whether the entity is facilitating the transfer of money, or if they're signing something else. You're essentially blindly changing the signing rights over a private key without changing the key itself, which undoubtedly has use cases other than cryptocurrency.

The Statechain entity is signing blinded messages — it does not know whether these are Bitcoin transactions or something else entirely.



Not only would this increase the privacy of the system, but it also really challenges the legal definition of what it means to "process" a payment. All the Statechain entity would do is blindly sign messages at the request of a chain of users. A user gets to request one signature and also appoints a new user that gets to request the next one. All requests and corresponding blind signatures are transparently published.

For those who are familiar with the details in the paper, the key difference compared to regular Statechains is that users are expected to unblind and verify the chain of signatures prior to accepting a payment, because the Statechain entity can no longer ensure that what it's signing is correct. If one of the previously requested signatures in the history is incorrect, the recipient simply rejects the payment. Unblinding can be done by anyone who controls the transitory key (thanks to Jonas Nick for checking my transitory key hashing method for unblinding).

In a sense, Blind Statechains are a variant of Chaumian cash, but it actually manages to move one step beyond it. Chaumian cash makes it impossible for a server to know who is receiving the money, but if the server refuses you service, you essentially lose the asset. With Blind Statechains the server doesn't even know whether it's transferring money, it doesn't know who is receiving it (particularly when combined with coinjoin), AND it cannot stop you from redeeming its value on-chain on the Bitcoin blockchain.

Finally, it is worth noting that the Statechains protocol is the culmination of a bunch of technologies by many developers. As the author, my contribution was limited to creatively putting them together for the novel purpose of transferring UTXO ownership (more specifically: key signing rights) off-chain. Credit goes to the creators of Sidechains, Schnorr Signatures, Adaptor Signatures, Blind Signatures, eltoo, Graftroot, and undoubtedly many more works that have inspired me but I am failing to recall.

Thanks to Adam Gibson , Bryan Bishop , and Calvin Kim for the article review and comments.

My more in-depth Statechains talk from Scaling Bitcoin '18 in Tokyo. Also check out the paper.

The Political Theology of Crypto

By Erik Cason

Posted June 11, 2019

“All significant concepts of the modern theory of the state are secularized theological concepts.”-*Carl Schmitt, Political Theology* Crypto is a religion insofar that statism is also a religion.

Both rely on a belief and faith of their respective systems to actualize the value of their laws in a meaningful way. Within contemporary legal systems, the value of law is actualized through people who are invested with the authority of law, and the ability to enforce the law with direct legal violence—for better or worse. Within crypto systems, the rules are enforced by the code alone—there is no subjective character about it, nor any violence that needs to be applied.

What allows for the operation of both of these systems is the ‘oath’ that has been taken to consecrate the laws of each system. In legal systems, man is bonded to the law through his oath and obligation to it; within cryptosystems, it is the private key that bonds the code to the outcome.

Each system must enforce the rules of their systems accordingly to actualize the value of their system of law, or the system must have the possibility of exceptions to any rules; in which case all contemporary law proves its ‘situational’ nature. As Schmitt says, “ *For the legal system to make sense a normal situation must exist, and he who is sovereign definitely decides whether this normal situation actually exist.* “

Contemporary systems of legal power comprises of the oaths of men, who can break their oaths as easily as they are stated. The authority of any and all men has the same weight and power as temporal is their nature; and so it must be the same for the laws of such men. Men have proven over millennia that they cannot keep their word to the law, and thus shows the very base corruption of any system of law created by the oaths of men and enforcement via violence. With the infinite ‘exceptions’ men of power may always make for themselves, and how anyone can be deprived of the law through the label of ‘enemy’, we see the abyss in which all law will fail before its actualization.

The oaths of machines are something fundamentally and distinctly different from that of men. Machines cannot lie. They are semantically incapable of it: it is impossible.

Due to the very nature and being of what their language/code is and how it must express itself, the machines have their entire existence as a form of communication at stake and enmeshed in the code/language itself.

For the reason that, " *the oath can function as a sacrament of power insofar as it is first of all the sacraments of language"* it becomes messianic tool of the economic ontology within a digital globalized capitalist society. There is no methodology of sovereign exception within code; the oaths of machines towards their semantic obligations **must** be fulfilled because they are entirely enmeshed with the communication itself. There is no possibility of an exception within the code because the law of code is not interpreted, but compiled. The code operates under a binary methodology of truth-as-its-being and nothing else. This creates a totally new strategy of 'law', as there is no longer the need for enforcement of any kind, or the violence that must go with it.

By the nature of what code is, there is no room for any kind of exception.

The reason that such a beautiful and imperious system like Bitcoin can exist is because of the way that the private key functions within cryptographic systems as a fundamental and inviolable sacrosanct of power. The private key consummates a form of power that assures, proves, and protects its privacy with no exceptions beyond the math which creates it. This is not for our unwillingness to violate such systems, but because of the total imperium of mathematics to which such systems are beholden.

To crack a private key is to violate the laws of physics themselves.

No human or machine has any power to move the mathematics that animates cryptography beyond its limits. The ontological form of the 'language' of cryptosystems are direct truth-bearing statements using cryptography as their *lex*. Each and every bitcoin transaction is a statement of truth regarding the social ownership of the coins. The only way that it is possible for coins to be exchanged is through the exposure of the private key, and nothing else.

It is from the inviolability of the mathematics which animates cryptography that a new form of economic, social, and political power has been created: cryptosovereignty. By rendering the violent physical force of the state legal machine and other barbaric adversaries useless, crypto creates a kind of value that is totally and completely outside of the control of any and all states through a liturgy of math which renders the physical world repaginate. It is the creation of a new kind of socio-political digital-economic commonwealth which is the resounding and messianic answer to the question: *quis custodiet ipsos custodes?*

Exception of the State

To take Carl Schmitt's dictum from the beginning of this essay, we can invert it in the same way that Walter Benjamin does in his Critique of Violence for another perspective to be offered:

"Just as in all spheres God opposes myth, mythical violence is confronted by the divine. And the latter constitutes its antithesis in all respects. If mythical violence is lawmaking, divine violence is law-destroying; if the former sets boundaries, the latter boundlessly destroys them; if mythical violence brings at once guilt and retribution, divine power only expiates; if the former threatens, the latter strikes; if the former is bloody, the latter is lethal without spilling blood."*Walter Benjamin, Critique of Violence* To see a uniquely different path towards a ***real form of common-wealth and law*** through cryptographic systems of power that fundamentally banishes the force of violence from having bearing on these systems. To exchange the power of violence to enforce the law, for the power truth to bare the law, is to commit the most revolutionary act that has even been done. For without the power of violence to have bearing on the system of wealth, a radical new form of economic power is birthed into the world, with the resounding thunder of, "*Fiat justitia, ne pereat mundus.* " Through a total and radical incapacity to use violence as an enforcement mechanism of cryptosystems through protecting people's privacy directly through cryptographic protocols; cryptocurrencies completely banish the state apparatus and violent force from the monetary systems of cryptocurrencies. Crypto absconds from the law, the state, and all their various forms of violence that must consummate all law by blinding such legal systems from the outset–anonymizing and homogenizing all actors within the system to protect everyone's identity from the outset. This allows for a truly common form of wealth to be created where all actors within the system are equals, and no person has any sort of special power over the system–all participants are truly equal.

The power-knowledge of what crypto truly is decrypts an immanent and ancient form of power that unites magic, religion, and law into a single language once again. Crypto unlocks an ancient form of political theology which uses the power of truth to ensure that the 'laws' of the system cannot be broken. As I have stated before, this allows for anyone to invert the Hobbesian dictum of sovereign power from *"Auctoritas, non veritas facit legem" (* Authority, not truth makes legitimacy *)* into *"Veritas, non auctoritas facit legem." (Truth, not authority makes legitimacy)* Through the absolute glory of the power of truth, and the total demand of the math which consummates such a form of power proves itself continuously with its unbreakability and the absolute value it has to protect one's wealth from any law, violence, or other. By the virtue of truth, and our capacity to recognizing the value of a system of economic exchange in which the state cannot capture, or violently destroy; we understand the true power and political theology of such a system.

Through giving our lives, our fortunes, and our sacred honor over to this new form of common-wealth that is beyond the temporal power of any state laws or government to destroy or steal from us; we create, together, a new form of value and wealth that has the potential to change everything. The tradition of the oppressed teaches us that the "emergency situation" in which we live is the rule. Our understanding of what crypto is, why it was invented, and how it protects us through the knowledge it imparts has us arrive at a concept of history which corresponds to this. It is now clear that the task before us is the introduction of a real state of emergency; and our position in the struggle against technological fascism will thereby improve.

The Sovereign, the Subject, and Crypto-power

By Erik Cason

Posted June 24, 2019

Political life in the digital panopticon

“The obligation of subjects to the sovereign is understood to last as long, and no longer, than the power lasteth by which he is able to protect them. For the right men have by nature to protect themselves, when none else can protect them, can by no covenant be relinquished.” -Thomas Hobbes, Leviathan

To understand the power of cryptography, we first must understand what sovereignty is and how it functions in modren society. What exactly is sovereign power in the digital age, and how exactly does it project its power into the world of flesh and steel? What is the process of the execution of power in this non-physical space, and how is it directly applied to the subjects of a commonwealth?

Through using the perspectives of Giorgio Agamben, Carl Schmitt, and Michael Foucault we can see that in the current paradigm of law is not that of legality, but of raw authoritarian force ~~of law~~. The law today functions only through the sovereign exception that is the rule. If sovereign power is suppose to be the protection and guarantee of access to the law, then we must ask what does it mean when anyone, or anything, can be put outside and beyond the law for whatever ‘emergency’ the sovereign may decide?

The origin of sovereign power, as stated above, is nothing more than the protection that can be offer to one another within a society and the laws that consecrate such protection. People meaningfully give up their individual power to a supposed sovereign who can offer a kind of protection that none other can offer. However, the convent that can never be relinquished is nothing other than direct protection. Protection is a totalizing concept–it exist in a binary field. The personal and absolute demand for protection ***for oneself by oneself*** goes beyond any convent; it is something that can never be relinquished for it is life itself. Every human has a natural right to protect their lives and to given themselves fully to their own safety and security. There is no god, government, or person who can ever take that away for any reason, no matter what ‘emergency’ there may be.

Over the course of the last several centuries, the slow chipping away of all essential rights through every kind of transgression through the emergency decree has hollowed out the very meaning of ‘rights’ under the guise of law. Today anyone can be placed outside and below the law, while allowing for others to stand over and above the law. This is the State of Exception, it is the core sovereign function at play within the law, and how state agencies always find themselves and their actors beyond the reach of the law. The law is always-already suspended—just look at the facts of the world and the avarice, corruption, and barbarism from which state agencies function. This is why police kill and it is not called murder, and why politicians steal and it is not called theft, and why militaries commit war crimes and it's called collateral damage. The state can commit any crime it desires, and it can always absolve itself for any reason it sees fit.

All States have re-established *bellum omnium contra omnes (*' The war of all against all') as *bellum se ipsum alet* ('the war that feeds itself'). The true nature of sovereign power is not to end the war of all-against-all as a great peacemaker, but rather to subject populations to the parasitic nature of a continuous total war that encompass all of biological life.

Identity and subjugation

" Isn't power a sort of generalized war which assumes at particular moments the forms of peace and the State? Peace would then be a form of war, and the State a means of waging it."–*Foucault, Truth and Power*

Peace is the mode of surveillance through which the state wages a constant war against all people at all times using police, agents, consultants, CCTV, and so many more modules of control to act as the eyes and ears of the great panopticon we call global society. It is through the 'gaze' of the panopticon that the identity of the subject can be formulated, and then process of selection can begin. The sovereign may label one as enemy, for liquidation, or friend, for continuous exploitation in the camps of life under the slogan 'arbeit macht frei '.

Through the mode of war that the state calls 'peace', and the laws, police, regulations, surveillance and nearly infinite other *technik* of repressive state apparatuses uses to actively wage this war, statism creates the conditions for its permanent unconditional rule. With the ungodly amount of data that we each produce, China is just the first of all states to implement the panopticon that has created the digital camps.

Through the never-ending war of 'nationalistic peace' under the slogan of 'emergency' that demands we are all labeled and tracked, our identities as enemy or friend is decided under the sovereign decision. The state of emergency is always-already ruling by the very nature of its ability to be called upon at anytime for any reason for any amount of time the sovereign deems 'dangerous'.

The ability of the law to cloak the absolute nature of sovereign power that is enshrined at its center is the very predicament that puts all people outside of the law, and all government agents beyond all law. The Patriot Act is this surmised into a single law which can label any human alive as 'enemy combatant' thus branding their flesh with the label of death, _ Homo Sacer,_ that which ensures they will never encounter the law, just be placed outside of it. Just as important, this also creates a class of men who enforce the law, which allows for them to subjectively choose when and where to put into force the law, which can always excludes them.

Through this form of law (the state of emergency which opens the sovereign exception) both figures—the sovereign and the subject—find their natural, final places outside and beyond the law. The Sovereign is omnipotent, and has the full responsibility to decide on everything in regards to The Subject. Not just one's biological and physical life, but the very form, make-up, language, memory, cognition, norms and all of the features that encompasses our total being as a human life. The subject is entitled to nothing, not even to die at their own will, as the state believes the naked biological life of its citizen owes its very existence *as a subject* to the Sovereign alone, and may only die at the sovereign's approval.

Identity and the Camps

"The state serves as the decisive political entity which possesses an enormous power: the possibility of waging war and thereby publicly disposing of the lives of men. The _jus belli_contains such a disposition. It implies a double possibility: the right to demand from its own members the readiness to die and unhesitatingly to kill enemies"–*Schmitt, On the Concept of the Political*

These two figures are the most extreme and isolated figures that are found within the law only through their capacity to be acknowledged to be beyond the law in a state of total unbracketed war. Both the sovereign and the subject are placed in a zone of indistinction beyond the law where the 'crisis' or 'state of emergency' allows for the sovereign decision to rule totally without remainder because of the *jus belli* within the decision.

This is possible due to the primacy of identities within the friend/enemy distinction in direct contrast to whatever crisis. The subject, through their being itself (Dasein), their existence and what is at stake in their existence contrasted against the state, creates the emergency. And in the same vein, the sovereign through their being itself (Dasein) is the only response, or decision, which postulates itself as 'The Final Solution' for the crisis that always creates "others" to be exploited, raped, and liquidated.

As the Jew created the Nazis' 'emergency' by their very existence in the world, and thus impelled the Final Solution, so too does anyone else's existence by the very possibility of being the 'other' people under the sinister glare of a sovereign beyond the law. The Other is he who can be made into a non-human—and not just in the sense of being below the law, but above and beyond it too. Both are beyond the law for the singular identifier, a being-in-the-world that subsumes the law itself placing naked, raw life as the final objective of power.

Both the subject and the sovereign have the immediate signature of a primary identity as friend or enemy labels from the state based upon whatever 'emergency' may be declared. This makes both the sovereign and the subject beyond being seen as human by the law for the very nature of how they are both addressed in the final hour of sovereign law. Even the very event of the signification of each–the Jew with their armband star of David, and the Nazi authority with their signifying armband of legal power–demands the openly labeling of friends and enemies alike for the process of selection; work or death.

These primary identities that are inscribed upon us from the outside, and displays there is no remnant outside of that of those identities. Our role, identities, and names have already been chosen for us; and testify for our lives before a seemingly omnipotent sovereign power hellbent on controlling everything. It is through this function of identity, and how the state perceives everyone in terms of a paranoid and schizophrenic delusion that all must be labeled friend or enemy for the safety and security of the 'commonwealth' is the very nature in how the digital panopticon is created. However, what it also displays is that all that we have left in common of our commonwealth is the guilt and shame of a people who no longer have law, only the camps.

This is how the sovereign above the law, and the subject below it. Both have primary identities that put them beyond law into a space of pure sovereign decision. Our identities as a subject or a sovereign supersede our flesh—it is how the human body has totally fused into the body politic—the double identities we live, as both biological beings and political objects are fused into one through the total subjugation of our bodies, minds, and lives to the temporal power we call law. We are bonded to the empty, idiotic labor of a oligopolist capitalism; our morals to corrupt governments and dead gods; and our private affairs to corporate panopticon machines seeking to know everything so we can be sold back to ourselves. All of this horror is carried out in the name of safety and security under the banner of the state's corrupt peace of ash and blood; a false throne of shattered bones, gnashed teeth, and rivers of blood for the temporal and mutilated god they call law.

The Fracturing of The Body Politic

It is within the fusion of our biological bodies to the political body that we can see the extinguishment of the ability to create active *civitas* as a real political possibility today. By living lives as *only* subjects underneath the law (which may as well have us be slaves), and not as *citizens* who can consummate, constitute, and create their own law and agreements with *each other*; we not only find that we are below the law, but that we are also the Man from the Country who will never have access to the law.

This is the same fusion that creates a zone of indistinction where *zoe* is fully expropriated into *bios*; where the polis is obliterated and man becomes totally alienated from both his politic being and his biological body—now he is a vacant and empty machine ready to be exploited, and subjugated to the infinite exploitation of a worthless and hollow life as a total object for the free use of states which believes themselves to be a gods beyond any men or morals. **While this has allowed for the state of exception to become a broad and sweeping legal concept that encompasses all law; it has also created the path towards liberation through showing the total banality of the current socio-political-economic situation of the world. Through the full deprivation of any form of rights to all citizens through the state of exception being applied blankety, we can see the true nature of any form of contemporary sovereign power is TYRANNY**.

The Emergency of Cryptography

"The tradition of the oppressed teaches us that the "emergency situation" in which we live is the rule. We must arrive at a concept of history which corresponds to this. Then it will become clear that the task before us is the introduction of a ***real*** *state of emergency; and our position in the struggle against Fascism will thereby improve." - Walter Benjamin, On the Concept of History*

The history of computers is the history of cryptography, which in turn is the history of the tactical development of communication under the conditions of total unbracketed war. Cryptography is the culmination of the understanding of the phenomenon of " *bellum omnium contra omnes"* and offers a kind of science to which men can *'protect themselves, when none else can protect them,'* and most importantly *'by no covenant be relinquished.'* The history of all hitherto existing society is the history of class struggles, and the final epoch of all class struggle will be one carried out in the field of total unbracketed WAR where " *bellum omnium contra omnes"* offers its decrypted meaning. Nature opens the messianic path through the real state of emergency that is *homo homini lupus* and the infinite grotesque promise of what that should mean to each and every individual human.

Crypto is the culmination of a cognition of history which recognizes the economic nature of privacy and secrets in the total struggle of all against all, and the respective role that states have always played within that struggle. In all systems of government, the possibility of a ‘state of emergency’ that will always create ‘other’ people who can be killed but not sacrificed, exploited but not robbed, and in bondage but not slaves; is always real, possible, and is a hideous fact of what the 20th century was. Crypto is a history which understands the infinite violence that all sovereign powers have entitled themselves to for ‘Final Solution’ of legal means against man, nature, and life as we know it at all cost—including the rule of law.

It is this recognition that the law is created through *only* legalized violence; not majesty, consensually, or consanguinity; but only the most crass, brutish, and nauseating barbarism that we see what it truly is. It is a life lived at the foot of the castle under the bloody sign and seal of “security and safety” for the exploitation of all people by all people under the prattling murmur of ‘ *arbeit macht frei, arbeit macht frei’* …

It is once we understand that our political problems are *first* economic problems that our position in the struggle against panoptic fascism will vastly improve.

The Final Decision of Cryptography

“The sovereign is he who decides on the exception.” —Carl Schmitt

Crypto commands that the code alone to be sovereign.

There is no possibility of exception.

Due to this explicit fact that digital expressions exist solely in the realm of ideas, in a *non-physical space through mathematical expression* it cannot be subjugated to the same physical forces of violence that sovereign rule must always entail. Crypto leaves no remainder for any kind of exception.

Crypto is subject to the laws of mathematics alone.

There is no sovereign exception, nor can there be one. The vicious magnanimity and imperium to which cryptography holds mathematics as its only sacrosant and law allows for it to consecration the glory of a singular God to whom there are no exceptions within his machine of physics, his immanent laws of the universe, and His passion for a form of wealth that is beyond the power of any group of men.

What we need, however, is a political philosophy that isn’t erected around the problem of sovereignty, nor therefore around the problems of law and prohibition. We need to *cut off the King's head: in political theory that has still to be done.–Foucault, Truth and Power*

Crypto presents a political theory which decapitates the sovereign's head with the resounding declaration of _ fiat justitia, ne pereat mundus_ . It does this by not engaging the the classic stratagem of law, prohibition, and sovereignty that all law demands. Crypto engages in a radically new system of common-wealth and law through using cryptography as the base technique of this new form of digital social agreement. Through this a new form-of-life, where all people can have their wealth be protected from any form of violence through the power of cryptography; a messianic possibility is opened.

This allows for something that all people, whether they admit it or not, know in their heart of hearts: that things could be different, that radical change is really possible, and that we could live with happiness and peace. We could live not only without hunger, but also probably without fear, and freely as well. And yet, at the same time—and all over the world—the social apparatus has become so hardened that what lies before us as a means of possible fulfillment presents itself as radically impossible.

Together we must choose to make the collective decision to create the real and final state of emergency that will be the final existential threat to the state by refusing their corrupt money, hollow laws, and false idols. Together we can choose to create a new form of social life, common-wealth, and law together that is outside and beyond the power of any state or government to destroy. Together we can deactivate state law, and shatter the paradise of legal violence in order to consummate a new form of economic, social, and political life that is beyond the power of any states, any laws, and any violence the state will use to try to destroy it. For with each blow that they will deliver, crypto will only get stronger, and prove its inviolable nature more resoundingly, while also showing just how corrupt and wicked those in positions of sovereign power are.

"The sovereign is the point of indistinction between violence and law, the threshold on which violence passes over into law and law passes over into violence." —Giorgio Agamben, Homo Sacer

Through a glitch in the matrix that creates the image of sovereign power through its physical form; we also find the Achilles' heel from which there is an opening to create Leviathan's downfall.

Sovereign power cannot actualize the law if it does not have a physical space to render violence within. It needs a physical body it can subject, dehumanize and objectify into an enemy who deserves no law, and must be destroyed in order to display its power. If sovereign power cannot find a physical body or space in which it can carry out it punishment, it risks displaying the incapacity of the law without violence, the sovereign without his subject, the emperor without clothes.

Blinding the Sovereign

The State is superstructural in relation to a whole series of power networks, that invest the body, sexuality, the family, kinship, knowledge, technology and so forth. True, these networks stand in a conditioning-conditioned relationship to a kind of 'meta-power' which is structured essentially round a certain number of great prohibition functions; but this meta-power with its prohibitions can only take hold and secure its footing where it is rooted in a whole series of multiple and indefinite power relations that supply the necessary basis for the great negative forms of power.–Foucault, Truth and Power

In order for legal power to secure a footing, the first engagement of power must be one of identification. Through identification, the physical form can be found, and power projected on to the subject in any of the nearly infinite ways the panopticon can through the gaze and its power. Once identified, the selection can begin. The subject can then be labeled as 'friend' for exploitation in the camps or enemy for destruction and liquidation. However, through the digital medium of this space, which can *only and explicitly* be expressed in non-physical medium, there is a territory in which the subject can abscond into a total anonymous existence of its own creating. In making the final turn away from the panoptic machine, and giving oneself entirely as anonymous citizen of the digital cosmos, man once again finds the ideals from which he can create the new order of the ages once again.

Through using cryptography to create a novel and fair economic game of wealth, bitcoin rediscovered the sovereign power that is hidden at the center of what a commonwealth really is: The commonality of wealth to all, with no one able to control or change the system for the betterment of some at the cost of others.

With this radical new power of peace, man finds himself back at the start of all political concept once again. However, this time man emerging from the forest of technology, armed with cryptography and the messianic possibility it contains. Man has renewed the opportunity to liberate himself from the camps of modernity; but this time for good. Through bonding ourselves to cryptographic protocols and consummating with the machine directly to create a new form of commonwealth, law, and power; we create the hypermachine of power which opens the next, and final epoch for humanity. Through the personal choice to totally objectify ourselves via code, and giving ourselves to it entirely for the protection that it offers, and the commonwealth it creates, we reopen the *polis* once again.

Through giving ourselves over to the power of cryptography, and the majesty and imperium to which it will always hold, and the liberty and freedom it must always entail; we have the power to open the final hour in which the state can be deactivated. Peace on this earth is not such a radical ideal if we all have the power/knowledge of cryptography at our fingertips, and how to use such a power to protect ourselves, our lives, and wealth.

Through this action alone, any human may become sovereign over their wealth and privacy once again. With the true nature of what the common-wealth of law is rediscovered, *magnus ab integro seclorum nascitur ordo (the great series of ages begins anew.)*.

"One day humanity will play with law just as children play with disused objects, not in order to restore them to their canonical use but to free them from it for good." — Giorgio Agamben

Disclaimer:

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