



WORDS

February 2019

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

Contents

Contents	1
Goals and Scope.....	2
Support WORDS	2
Why Monetary Maximalism could fall short of expectations	4
Demystifying Blockchain Not Bitcoin.....	8
Bitcoin Delta Capitalization	13
Bitcoin is a hedge against the cashless society	18
Rehypothecation: BTC's path to becoming king of collateral.....	21
Security Budget in the Long Run.....	28
Tweetstorm: Power and Money	39
A Primer on Bitcoin Investor Sentiment and Changes in Saving Behavior	41
Bitcoin's Incentive System or When The Stars Align.....	51
Crypto Governance: The Startup vs. Nation-State Approach.....	55
A Human Rights Activist's Response to Bitcoin Critics	61
Cryptosovereignty	68
Disclaimer:	71

Goals and Scope

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. *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 Bitcoin research is in any event too small, as the number of Bitcoin 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 Bitcoin space.

Enter *WORDS*. Published independently, *WORDS* is a journal that welcomes submissions on a range of topics of interest to the Bitcoin 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. *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 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.



Spread the word

Have a website or use social networking sites like Twitter, Facebook, or LinkedIn? Please consider sharing the content found on *WORDS* or linking to <https://bitcoinwords.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:



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.

A dark gray rectangular button with the word "Subscribe" in white text.

Subscribe

Our pledge

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

Why Monetary Maximalism could fall short of expectations

By Su Zhu and Hasu

Posted February 2, 2019

Monetary maximalism is the idea that in a free market for money one big winner will emerge and that the "soundest" money is in the best position to do so.

In a previous post I wrote that "every token competes in one massive power law distribution for the title of dominant non-sovereign monetary store of value. If it does not win this rat race (or comes to a close second or third place), its market share will, effectively, be zero."

The most popular argument for why that should be the case is that it already happened once – with gold.

There are two big assumptions baked into the grand narrative of monetary maximalism today. First, that the world will gravitate towards the soundest monetary-policy coin. And second, that gold-analogies are apt in describing Bitcoin.

We would argue that this is reasoning by analogy, and that the analogy is not self-evident even for many people inside crypto, let alone outside. We should steer clear of suggesting that we can use logic to determine how this will all play out.

Instead, we should realize that for Bitcoin to become what most of the community wishes it to be, there are multiple challenges to overcome that work as counterforces to the consolidation into one money. These counterforces are:

Misalignment of incentives with crypto companies

Crypto companies are funded with the goal to capture value – especially value that can weather both bull and bear markets. The result is a value capture layer on top of Bitcoin with actors that over time evolve their own opinions that ultimately become social attacks on Bitcoin.

Many of these companies would lose if bitcoin was to become a mature store-of-value tomorrow and since they respond to their shareholders and not the Bitcoin community, it's in their best interest to prevent that.

The biggest "attack" on Bitcoin is the existence of altcoins. Investors and VCs are incentivized to push for a multicoin future because they can be paid for finding the next Bitcoin. Monetary maximalism ascending necessarily implies that this paradigm of crypto-as-tech would come to an end.

Exchanges like Coinbase are also incentivized to push for a multicoin future, as they benefit from people trading back and forth between different assets. Consolidation into one money would mean a massive decline in cross-currency trading. As an exchange, they love drama and volatility in the markets to attract traders. Their support for past contentious Bitcoin forks as an attempt to shape the protocol to suit the needs of their business and later pushing for a world where Bitcoin is just one of many assets have been entirely rational.

Miners can also decide to attack Bitcoin, with Bitmain as a prominent example. When they disliked the direction protocol development was going, possibly because they were afraid that a layered scaling approach would hurt their bottom line, they launched a social attack in the form of Bitcoin Cash. Even though the attack ultimately failed, the fork diluted Bitcoin's supply in the eyes of the public as well as its brand value.

If we look at who is actually incentivized to help Bitcoin become a mature SoV, in terms of crypto businesses there are shockingly few. A mature Bitcoin would force many of them out of business. And yet we find that Bitcoiners are constantly surprised by the so-called impure behavior of companies in this space.

Culture clash between different currencies

Because of crypto's unique nature of a social layer and technical implementation reinforcing each other, all networks are highly cultural in nature.

All coins get their properties from the shared beliefs of their holders. A strong culture has to be enforced so they can retain these properties against change.



Image Source: [Unpacking Bitcoin's Social Contract](#)

Arjun Balaji and Yassine Elmandrja have recently [laid out](#) how almost all fundamental disagreements in crypto are not about details of implementation, but about the fundamental values that each project enshrines in their social layer.

The result is competing frameworks like "Vision of the Constrained vs Unconstrained", "Money crypto vs tech crypto" or "Autonomous vs Governed", proving that there is a lot to disagree about when it comes to culture.

Just as the world is unlikely to converge to a single culture, whether we are talking about politics, art, music, language or food, so too can crypto exist for a long time as a pluralistic collection of different cultures.

If we assume there are irreconcilable disagreements on the social layer between projects and that the value of each token is agreed upon at the social layer, then the logical conclusion is that people with different cultures will prefer – and hence monetize – different coins.

We claim Bitcoin is apolitical maximalist money, but in practice the political philosophy views of bitcoiners are homogenous, especially with regards to libertarianism, and distinct from other crypto communities (which your authors have previously argued is a dangerous mismatch).

Bitcoiners tend to be objectivists – they believe there is such a thing as objective moral truths. But let us not mistake strongly held opinions for provable truths. We can neither prove that global money will evolve through soft forks rather than hard forks, nor can we prove that a premine is worse than no premine.

We can only show that the tradeoffs are such that we believe certain approaches are more promising than others. But if people disagree with us and these projects don't actually implode as we predict, then this market can well stay fragmented forever.

Appealing to human biases

Beyond basic preferences that are the result of a different culture, there are some biases inherent to our thinking that can draw people away from Bitcoin's monetary maximalism and towards other forms of money.

The most familiar example is probably the unit bias. When faced with a selection of coins most people intuitively compare the price of one unit, without regard for the number of total units outstanding. As a result, they falsely assume the cheapest unit is underpriced relative to the others and buy it.

Then there are people who have a bias in favor of innovation and tend to promote the new over the old without really looking at its limitations or weaknesses. Pro-innovation bias could play a big role in Bitcoin's future as the incentives of this market (see earlier) are aligned in such a way that crypto companies and investors collectively benefit from a steady flow of new competitors.

The most important bias working against Bitcoin, however, might be the "anti-waste" or "anti-PoW" bias. Already today there are many who categorically refuse to use any currency that uses proof-of-work for security, claiming that it is extremely wasteful and hence dangerous to our environment.

You can expect Bitcoin competitors like Ethereum to lean even more on this bias once they have completed their switch to proof-of-stake.

It's hard to imagine that people with a strong ideological dislike for proof-of-work can be convinced by economic arguments to turn around and embrace it. We find it more likely that this particular bias will continue to appeal to many people in the same way that easy answers to hard questions have always appealed to humans throughout history.

Conclusion

While we don't fundamentally disagree with the idea that a big winner could emerge from the battle of monies in the ultra-long run, there are also significant counterforces at work to prevent Bitcoin from being that winner.

The counterforces presented today all assume that the market structure itself is uncompromised, i.e. a free market for money exists. In practice, this assumption is hopelessly optimistic. Governments will continue to shape our economic realities as people in the Liberal West will not risk their lives to use one money over another for ideological reasons.

Most Bitcoiners are gleefully unaware of how few companies in this space actually have an incentive to help Bitcoin succeed, especially those who own the customer relationship and onboard all the new people into this space.

Bitcoiners should stop expecting companies, miners, etc. to virtue signal to them and instead start taking ownership of the means of production by building their own exchanges, nodes, wallets, custody, and education.

All cryptos are highly cultural. They need to be because they derive their properties from the shared beliefs of all users. This is a major differentiation from gold. The idea of Bitcoin monetary maximalism would require Bitcoin to transcend culture itself if it wants to appeal to people versus other cryptocurrencies.

Many people are questioning the "top-down" analogies used by bitcoiners today. Even many Austrian economists are not buying into Bitcoin as sound money.

So instead of mapping the history of gold over the future of bitcoin, we should look where we are today, where we want to be tomorrow, and how we can get there.

Demystifying Blockchain Not Bitcoin

By David Nage

February 9, 2019



This is a conversation that needs to happen now. As many know, I have been part of the family office community for the last decade and have been working to educate my peers on crypto for the last two years. This article comes on the heels of two private luncheons this week, where we discussed crypto amongst other investment themes. The popular, but incorrect catch phrase, "blockchain, not bitcoin" came up several times and I attempt

to identify several drivers of this narrative.

Some of you will read that catch phrase and be filled with 3 emotions: rage and disgust followed by annoyance. Others will think this is a logical separation, and...more importantly, will be more inclined to put their chips down on the Blockchain island.

Non-crypto focused investors hear about IBM and their work with Hyperledger; they hear about JP Morgan and Quorum. These are brand names no different than Nike, Pepsi and Ford; they've been comfortable with them for a long time—but in essence they don't understand the fundamental differences in what IBM and other corporate entities are building (a permissioned DLT) versus what Bitcoin, Ethereum and other protocols are building.

Why does this divide exist? How did we get here?



Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

As Garrick Hileman writes:

"The 2008 financial crisis reached its nadir with the collapse of Lehman Brothers on September 15, just six weeks before Satoshi Nakamoto published the bitcoin paper"

This is what was given to the world after the financial crisis—a purely peer-to-peer version of electronic cash allowing online payments to be sent directly from one party to another without going through a financial institution.

Innovation and adaptation has occurred during the last decade, as observed with every other technology society has bore witness to. In addition to Bitcoin we've seen other protocols leveraging the proof-of-work consensus algorithms and we've seen other consensus algorithms be created, such as proof-of-stake.

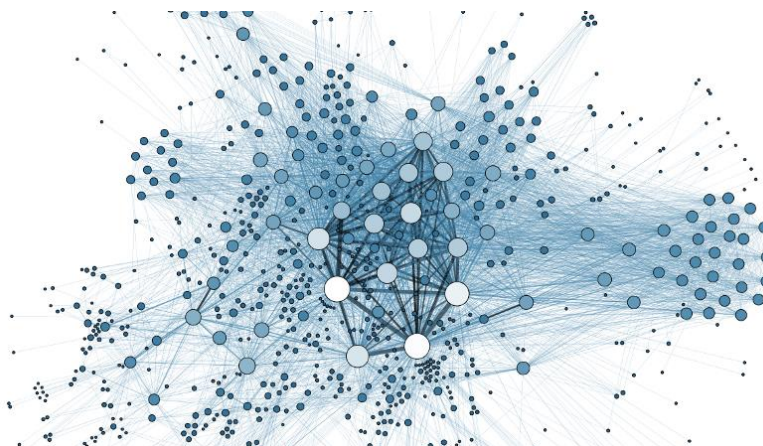
This discussion is NOT going to delve into which is the best and why, etc. However, at the very core, there is a fundamental lack of understanding from the perspective of the Institutional Investor on several main tenets which need to be illuminated:

1. Difference in Distributed, Centralized and Decentralized Systems;
2. Why we (as a society) need them;
3. Contributor (node) and Incentive models and;
4. Why it can't be in the form of fiat/USD.

Distributed Systems

The work done by Stanislav Kozlovski: "[A Thorough Introduction to Distributed Systems](#)" provides color on this; as stated:

A distributed system in its most simplest definition is a group of computers working together as to appear as a single computer to the end-user.



These machines have a shared state, operate concurrently and can fail independently without affecting the whole system's uptime.

Distributed But Centralized

As [Julia Poenitzsch](#) writes:

A distributed, but centralized system may sound contradictory but consider a cloud service provider offering a data storage service. Physically, your data could be shared and replicated on different machines according to resource availability and resiliency (distributed). However, wherever the machines and data storage facilities happen to be, the cloud service provider still controls them all (centralized).

Distributed systems and ledgers can be either decentralized, granting equal rights within the protocol to all participants or centralized, designating certain users particular rights.

Decentralized Systems

Decentralized and distributed systems, such as Bitcoin, cannot be altered by any one entity. It also runs as a *peer-to-peer network* of independent computers spread across the globe.

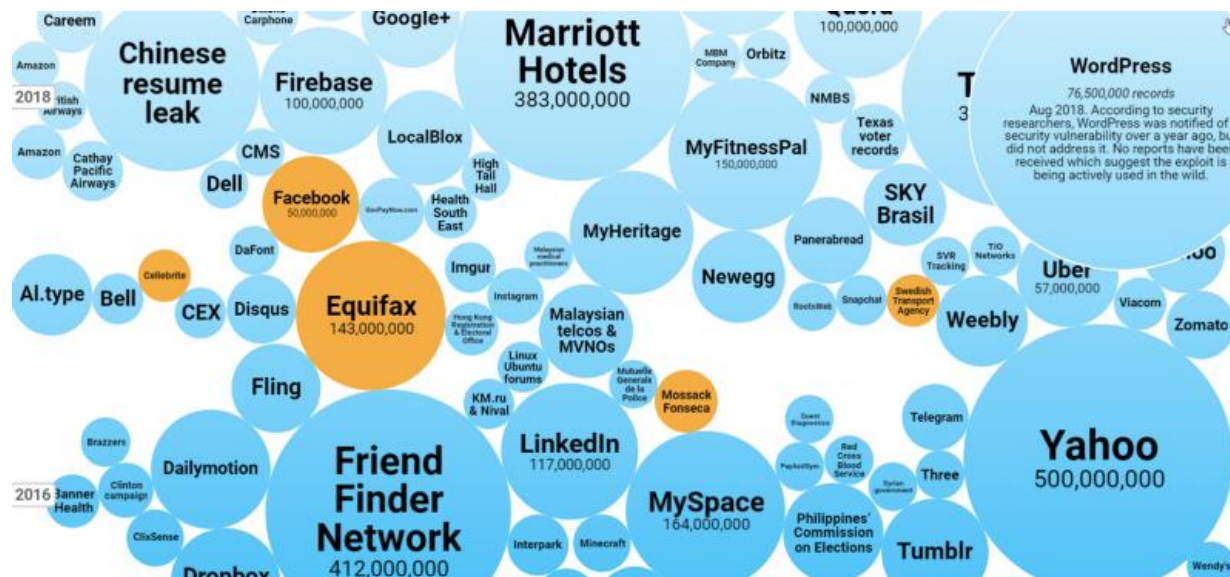
In conversations with Institutional Investors they understand concepts associated with Distributed Systems but this shift from centrally controlled distributed systems to a P2P network of "*independent*" computers/nodes is where the confusion comes in.

Why We Need Them

Decentralized, distributed systems offer advantages to their legacy centralized systems. Two of the more pronounced arguments in favor of these new systems that may resonate with traditional, non-crypto investors are:

Fault Tolerance: Because they rely on many separate components, decentralized systems are less likely to fail accidentally. The recent [Wells Fargo](#) outage serves as evidence of legacy systems failing.

Attack resistance: Due to the presence of a lot of players, decentralized systems lack central points of failure; there's no one point of attack that would disarm the entire system. This makes it more expensive and less viable to destroy these systems. This [infographic](#) is very useful to explain the significant amounts of data hacks we as a society have fallen victim to over the last decade and a half.



Incentive Models

Cathy Barrera discusses how incentive models help crypto: "[Blockchain Incentive Structures: What they are and why they matter](#)"

As Cathy notes:

An incentive is any design element of a system that influences the behavior of system participants by changing the relative costs and benefits of choices those participants may make.

Incentives include pay-for-performance reward systems that compensate individuals with money and they also include systems that incorporate no financial rewards at all.

Economics of Bitcoin

As Bitcoin.org states:

Bitcoins have value because they are useful as a form of money. Bitcoin has the characteristics of money (durability, portability, fungibility, scarcity, divisibility, and recognizability) based on the properties of mathematics rather than relying on physical properties (like gold and silver) or trust in central authorities (like fiat currencies). In short, Bitcoin is backed by mathematics. With these attributes, all that is required for a form of money to hold value is trust and adoption. In the case of Bitcoin, this can be measured by its growing base of users, merchants, and startups. As with all currency, bitcoin's value comes only and directly from people willing to accept them as payment.



This is a fundamentally misunderstood concept; more and more I hear "why can't a bitcoin/blockchain miner be paid in USD/fiat". This sounds ridiculous to people who've been in the ecosystem for years, but this phrase comes from multiple conversations with HNW/Family Office investors. Investors need more education on this topic because it is essential that they understand it.

Conclusion

Bitcoin, blockchain and the phrase "crypto" are part of the conversation among Institutional Investors these days; education from crypto investors, researchers and builders has significantly improved over the last year but there continues to be significant deficits in understanding the fundamental roots of the technology. Conversations with investors should focus on the four areas highlighted in this article; especially during the elongated "crypto winter" so they better understand the massive tectonic shift that is underway.

Bitcoin Delta Capitalization

A New View of BTC Long-Term Valuation

By David Puell

Posted February 14, 2019

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

As a follow-up to Willy Woo's recently-introduced Bitcoin Valuations live chart, this article aims to present delta cap with the goal of answering two of the most pressing questions in speculators' minds at the present moment:

1. Where is the bottom?
2. When is the next bull run coming along?

Something's Amiss

Two sets of items originated the search for what later became delta cap:

1. Awe and Wonder's studies on Bitcoin's logarithmic regression and Plan B's studies on Bitcoin's power regression (R^2 of 0.93 and 0.95 respectively), which seem to suggest that the BTC trend is increasing at a decreasing rate.
2. Murad Mahmudov's exploration of historical moving averages, expressing a dissatisfaction with any particular SMA or EMA as definitive enough to "catch the bottom" in every bear cycle.

This initiated the search for a metric that both adapted to Bitcoin's rapid, high-velocity parabolic moves and accounted for its overall trend decay over time. Two other valuation models seemed to provide a tentative answer: realized cap for the former and average cap for the latter.

Delta Capitalization

Delta cap is, as seen next, a hybrid of sorts—half "fundamental," half "technical." It is calculated through the following formula, measuring the difference between two long-term Bitcoin moving averages:

$$\text{DeltaCap} = \text{RealizedCap} - \text{AverageCap}$$

For the purposes of this piece, let's review these definitions:

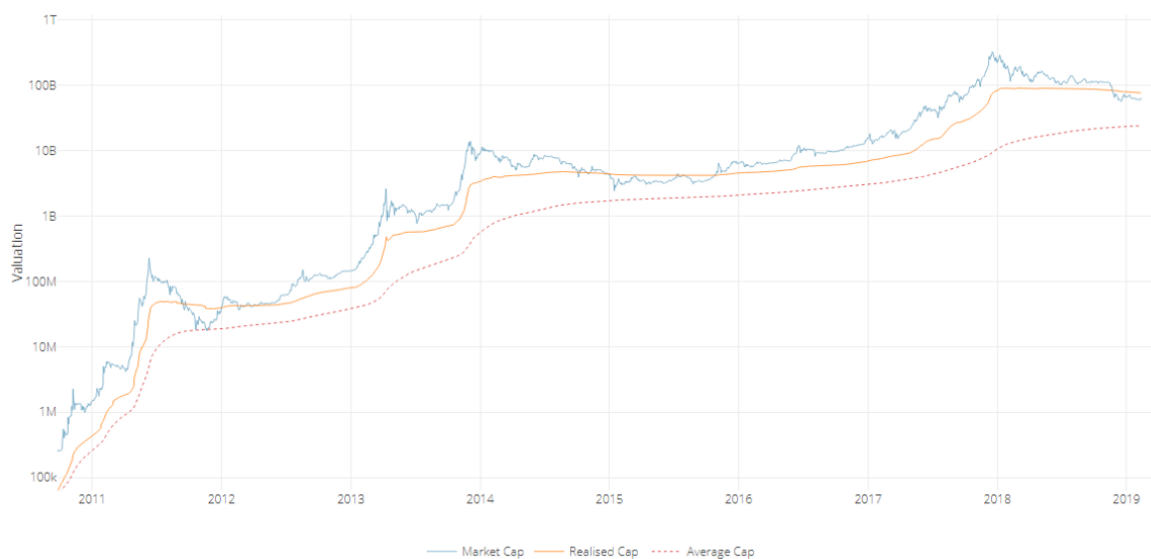
Realized capitalization

Invented and presented by the brilliant team at Coinmetrics, instead of counting all of the mined coins at current price, the coins are counted at the price when they last moved through the blockchain. This approximates the USD value paid for all the bitcoins in circulation. Best put by its co-creator Nic Carter, it can be described as an on-chain volume-weighted average price (VWAP) of BTC.

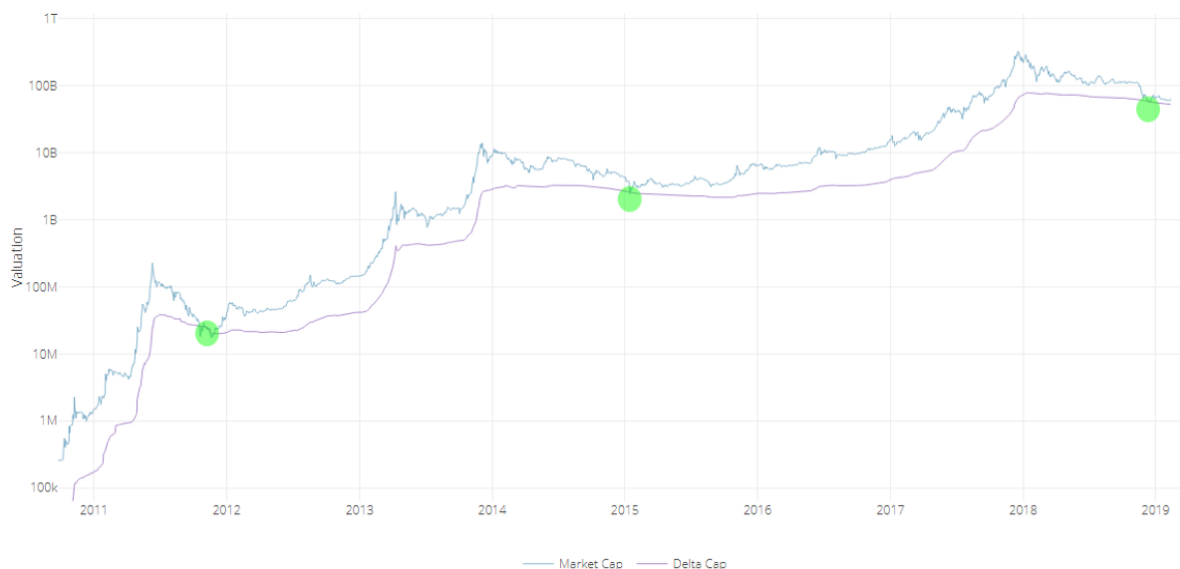
Average capitalization

Instead of setting a fixed period for calculating a moving average (e.g., a 200-day MA), this is a life-to-date, cumulative simple moving average that serves as the true mean of the whole history of market cap. Due to its “laggy” nature, it is the perfect mechanism to help decay the upward speed of delta cap over time. Shoutout to Renato Shirakashi for first pointing out this average.

Below, a view of both lines, courtesy of Willy Woo:



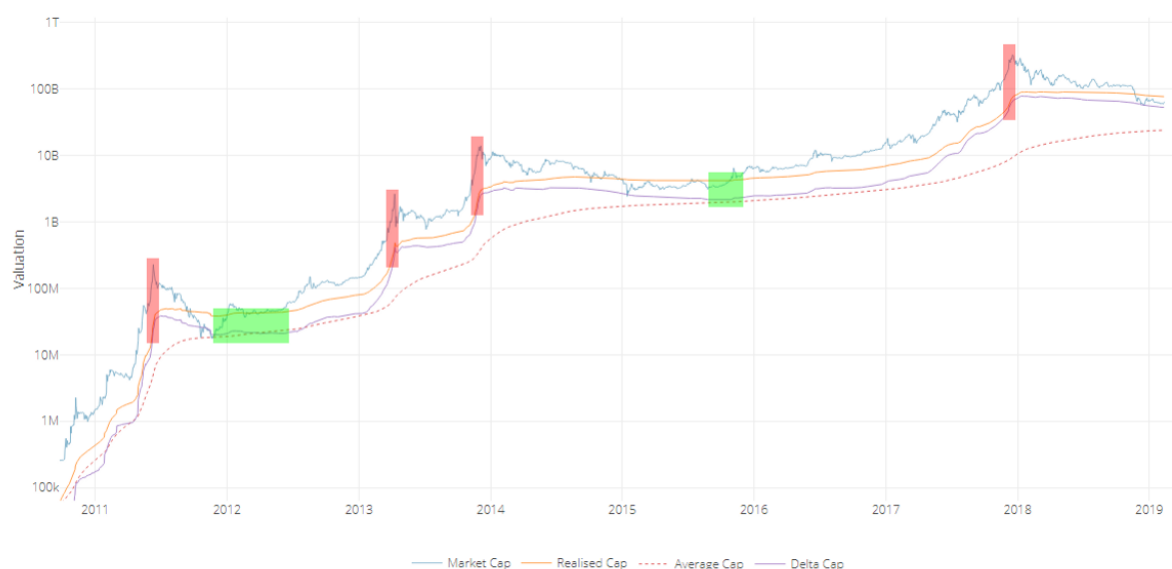
The aforementioned subtraction of the two in turn provides the following delta cap line, both reactive locally and decaying globally:



As seen at first glance, delta cap provides an excellent framework for catching global bottoms—or at the very least bottoms near the floor of the bear cycle. Please see the caveats of this indicator below to have a more nuanced view of the current state of affairs, since *having just touched delta cap does not guarantee that we have bottomed*.

Time Analysis

Another interesting (and still experimental) exploration of delta cap emerges when comparing it to its parent inputs through a logarithmic view, as follows:



We can easily gauge periods where delta approaches realized cap during the bubble tops, and then evermore slowly descends to almost touching the average cap during the phases of breakout price behavior, signaling the inauguration of the new bull run.

The good news? If this pattern continues, people will have lots of time to buy up. The bad news? This bear-to-sideways market may last for an unprecedented while, going as far as projecting a post-accumulation breakout as late as Q2, 2020—the moment when it could be expected for delta cap to get nearest to average cap if the extension of these lines continues as-is. Bear in mind that this is all pending on the overall rate of drop of realized cap and the rate of rise of average cap—local price action, velocity, and dormancy are all in play. Time domain here is still a broad estimate.

It goes without saying that we lack enough bottom samples to claim this as a certainty, but long-term investors must stay mentally prepared for this possible delay. It is further evidence that suggests Bitcoin's cycles are elongating.

Yes, Another Ratio: MVDV

Since most will be curious about how the Market-Value-to-Delta-Value (MVDV) Ratio looks like, here it goes:



A few notes on it:

1. Just as seen on MVRV Ratio and the Mayer Multiple, MVDV seems to indicate that each of Bitcoin's blow-off tops is losing momentum. This is not necessarily bearish, as I believe it merely implies that each bubble is becoming less exuberant and getting closer to the mean.
2. Major bearish divergences seem to announce global tops (red circles) while differentiating them from previous local tops of the same cycle.
3. The bottoms seem to maintain a steadier horizontal longitudinal threshold at 1 (green line). If market cap were to revisit delta cap today at a lower low, the oscillator would present this event as a double bottom.

Caveats

1. _Having touched delta cap recently does not imply a global bottom:_One must remember that delta cap is currently sloping down—and it will continue to do so for several months—so the likelihood of market cap revisiting it is not out of the question. Add to that the fact that the NVT tools are still just slowly trending into normal historical conditions and velocity remains weak. Touching delta cap on a lower low in the following months is still a likely possibility. Every penetration of market cap into delta cap should be best used as one componet of an averaging-in strategy over a prolonged period of time.
2. *Despite timeboxed halving days, the Bitcoin cycle seems to be elongating:* This makes perfect sense, since larger bull runs require larger liquidity. The experiment here is to continue evaluating delta cap as a mean that keeps adjusting to Bitcoin's curved trend. That being said, the time analysis section of this article remains highly speculative, especially for signaling the breakout events, so let's take it one day at a time.
3. _The market currently holds a major dissonance:_That of delta cap providing a good "baseline" for a relatively optimistic market floor, versus the current state of velocity as seen on NVT Ratio,Network Momentum, and NVT Caps— on life support relative to price.
4. *Delta cap remains experimental:* Just as with most technical and on-chain tools, these indicators should be used with prudence and in the company of other trading mechanisms and a sound risk management strategy. Past events don't reflect future outcomes.

Acknowledgements

Many thanks to the following individuals:

1. Willy Woo, for the beautiful charts and valuable feedback.
2. Murad Mahmudov,Phil Bonello,Hans Hauge,PositiveCrypto, and Plan B, whose comments helped perfect this article.

Sources

1. Woobull.com : Charts and early market cap data archeology.
2. Coinmetrics.io : Realized cap data.
3. Blockchain.com : Market cap data.

Bitcoin is a hedge against the cashless society

When cash is gone, where will you turn to transact with a basic level of privacy? What money do you hold when negative interest rates start eating away at your bank account?

By Su Zhu and Hasu

Posted February 12, 2019

The rise of digital payments and the move towards a cashless society are often seen as the same, but there is an important difference between them.

Digital payments like Paypal, Venmo, domestic-, and international bank transfers are convenient for people and businesses to transact with. They represent fintech innovation to consumers by the market. Faster, cheaper, and more efficient forms of digital payments are uncontroversial and largely an engineering and marketing challenge.

They don't, however, remove every need for cash. Cash has unique properties that digital payments have not. As physical coins and notes, it can be exchanged peer-to-peer without a middleman. Its ownership is transferred simply by handing it over. The absence of an intermediary ensures that transfers are permissionless, censorship-resistant and, most importantly, private.

Digital payments solutions do not utilize physical cash but also do not prevent anyone from continuing to use cash if they want. It is an alternative payment method to cash but is not antithetical to it. Indeed, in almost all modern societies, there coexists both a large digital economy and a large cash economy.



We will argue that the elimination of cash, even if most payments are already digital, will make society more vulnerable to surveillance, financial control, and authoritarianism.

Why do countries go cashless?

In a cashless society, the government seeks to discourage or even criminalize the holding and using of cash itself. In Sweden, it happened largely without coercion. In India, the government demonetized the 500 and 1,000 Rupee denominations of notes.

Different countries can have different incentives to push for a cashless society. In China, digital payments are primarily a tool of social control and serve as a backbone for China's social credit system. And they are making progress on it: 96% of cash payments in 2012 have turned into only 15% in 2019.

Over in Europe, central bankers are enthralled by the idea of negative interest rates. A recent IMF report states that:

"Severe recessions have historically required 3–6 percentage points cut in policy rates. If another crisis happens, few countries would have that kind of room for monetary policy to respond."

Negative interest rates were traditionally hard to implement because cash served as a lower bound. In a cashless society, this lower bound would disappear. In a severe recession, the CB could drop the policy rate to, say, -4% to make consumption and investment more attractive relative to saving.

Recently, central banks have started to brush everyone who prefers cash with the label of a criminal. They do that by separating the uses of cash into legitimate and illegitimate. People "abroad" can hold cash "legitimately" to replace an unstable or inflationary currency. Now domestically, the only beneficiaries of an anonymity-providing currency are

"those engaged in tax evasion, money laundering and the financing of terrorism, and those wishing to store the proceeds from crime and the means to commit further crimes."

Indeed, the use of cash in larger denominations has become so stigmatized in the US and Europe that withdrawing or carrying above a certain amount requires explicit government permission.

Problems of the cashless society

A society without cash has no ability to transact value without the omnipresence of government actors. By going cashless, societies double down on the properties of digital payments but lose all access to the unique properties of cash.

If every payment is intermediated, it becomes impossible to pay someone for anything without there being a record somewhere. It eliminates privacy and places the government as the third party in every financial event.

Governments claim that a cashless society enables them to protect citizens from criminals. The specters of terrorism and organized crime are often cited at this point. But this makes the naive assumption that governments itself can never become evil.

Because all transactions require the consent of an intermediary, they can easily be censored and funds confiscated. It might not be happening right now, but a good monetary system should be robust to changes in political moods. A cashless monetary system is less resistant to both the tyranny of the majority and shifts towards authoritarianism.

Cash may not be the right tool for the majority of transactions, but the elimination of it removes an important choice, and safeguard against government abuse, for the people.

Bitcoin as a hedge against the cashless society

When cash is gone, where will you turn to transact with a basic level of privacy? What money do you hold when negative interest rates start eating away at your bank account?

Traditionally, it has been impossible for the private market to come up with solutions for these basic human demands. The state doesn't like competition to their own fiat currency and made sure to quickly shut down all attempts of other monies to enter the market.

Bitcoin could change that. Decentralized and digital in nature, it no longer has the central point of failure that made previous "private monies" vulnerable. And it is modeled to marry the two forms of money — physical cash and digital payments — into an entirely new breed: digital cash. It can be transacted peer-to-peer, is permissionless, does not censor people or transactions, and has a reasonable level of privacy (if one knows how to use it).

We are still early into the Bitcoin-experiment, but with the cashless society looming on the horizon, we more than ever need it to succeed. Its fixed monetary policy already makes it a hedge against high inflation (that is increasingly used in places with collapsing fiat currencies like Venezuela). But, equally importantly, Bitcoin is a hedge against the demonetization of cash and the rise of the cashless society.

Rehypothecation: BTC's path to becoming king of collateral

By Patrick Dugan

Posted February 15, 2019

Quick Take

- Concerns about rehypothecation in layer 2 protocols for Bitcoin are overblown, we just need to accurately price its risk premiums
- In the default model of the Lightning Network, lots of BTC is needed in a fully-collateralized fashion to facilitate payments, earning a low yield from routing fees of generally under 1% per annum
- There's a strong argument to be made that historically, when people were allowed to create currency, e.g. credit instruments, to facilitate trade, prosperity rose
- Power money that is more scarce in supply becomes useful as a market referent and collateral base when it has the lowest perceived counterparty risk on the planet
- The path to BTC becoming king of collateral will require forms of rehypothecation

Concerns about rehypothecation in layer 2 protocols for Bitcoin are overblown. We don't need to fear rehypothecation, we just need to accurately price its risk premiums. There's inflationary and deflationary forms of derivative open interest. The deflationary version comes in the form of fully-backed synthetic cash positions, which fuels Bitcoin Dollarization and gives a sensible valuation-growth model for Bitcoin. To understand these nuances, we have to understand bank credit.

If your collateral is so good, why not use it like any other collateral?

What is fiat? Fiat is a b-side currency note, a form of immediate-term debt, it's an asset, but only because of its legal connection to the amortization of debts. It is an anti-liability, but mathematically, by the transitive property – that's an asset!

To restore some sanity, we call these “financial assets”, derivatives are also financial assets, that's why you can be short them. For every \$1 in someone's pocket, which they are “long”, the Central Bank or Commercial Banks are short \$1.

A real asset would be, for example, some Caterpillar machinery purchased with a secured loan. To buy real assets, people accept shorting units of fiat that they borrow, then spend. You get this phenomenon of “fiat” – let it be – the “creation” of new money in the form of credit. The difference between a licensed bank, and a pool of investors funding loans on LendingClub with full capital paid, or a bond investor, is that the bank has essentially a

portfolio margin license from the government. You don't have to fund loans with cash, you can fund them with credit. Your bank's credit. Also, the checking account deposits everyone depends on to survive are a junior, most-subordinated liability of the bank — thanks for looking out for us.

In essence, a lender is making a hypothesis that the borrower will pay them back. In the hypothetical scenario of a default, XYZ can be triggered (e.g. going and taking assets to settle the loan). So to hypothecate something, you just have to lend it.

To rehypothecate something then, you just... lend it again! Currency units issued by a bank as consideration for a new debt note, which may cycle back to that same bank and generally these days the value stays in the banking system, and around and around it goes. One man's leveraged capex is another man's revenue is another bank account's deposit. You get the money multiplier effect.

People who are Pro-Bitcoin generally hate the Federal Reserve, inflation, and fractional reserve banking. This is because many of us came of age at a time where all of these institutions were called into question, amidst great cataclysm unleashed through corruption of the highest halls of capitalism, and also we saw this movie called *Zeitgeist* and watched Ron Paul run for president. We read Baby Boomers' rants about gold manipulation on ZeroHedge, and then we found BTC. Murray Rothbard, Hayek, and the general school of Austrian economics figured in, but people who consider themselves a priori, categorically, it's gotta be Austrian, Austrians, are not necessarily representative of the majority of Pro-Bitcoin people.

Rehypothecation can fuel Lightning

In the default model of the Lightning Network, lots of BTC is needed in a fully-collateralized fashion to facilitate payments, earning a low yield from routing fees of generally under 1 percent per annum (what Nik Bhatia calls the "Lightning Network Reference Rate"). The presumption here, was that LN is necessarily going to be used in that way, that BTC would necessarily dominate liquidity in an environment of cross-chain asset swaps, and that nobody would use BTC/LN in a way that would contravene these Austrian economics tenants of strictly deflationary currency — which by the way, aren't strictly speaking representative of pre-Bitcoin Austrian economics, perhaps better described as Quebecois Economics, after its two most prolific proponents, Francis Pouliot and Pierre Rochard. Much respect.

However, one of the greatest things about Bitcoin is that nobody can censor usage of it. The only thing you can do to discourage certain kinds of usage is, either get mass consensus for a soft fork, changing around parameters that make it more difficult to relay "spam", or have it be generally uneconomical. But if it's economical, enough clients will relay it, and a single block-winning miner will include it, it can get in. Lightning Network is also a client-agnostic network in the sense that it has no global consensus state or specific blockchain. So it reasons, LN clients that run a bit differently could be pretty

amazing for getting yield on BTC. For those who know what they are doing, there's nothing that can be done to stop that, and it will have some degree of synthetic dilutive effect on BTC in the Lightning Network.

Rehypothecation of BTC across Lightning Nodes, creating some sort of money multiplier, is possible if channels are constructed that operate based on un-collateralized trades. Finance has given us solid math describing the adequate pricing, as least to the extent that major bank trading desks are able to stay in business, for trades both involving collateral and without. For those without, they price a sort of Credit-Default-Swap-like option premium, called a Counterparty Value Adjustment, in order to compensate the optionality of having some time window to deliver on a trade.

In the context of Lightning Network HTLC-like trades with a time-based escrow, someone can underwrite those failures to deliver as an income business, in a manner similar to a bail bondsman; think of it as collating the default risk of all those option-writes into a big secured loan that aggregates however many writes a party wishes to make. Those writes come with risk of default, but if there are recoverability mechanisms with a high efficacy rate, the business can end up looking like covered writes rather than risky, uncovered writes, and the premiums can get pretty cheap. Instead of stacking lots of BTC for a low yield, smaller sums of BTC can underwrite throughput for a higher yield and slightly higher risk, making loose trading more cost effective. Cheaper premiums allow people to trade up a storm, which creates derivatives of open interest (basically rehypothecated BTC). Time horizon is a major limiter to how much this sort of synthetic inflation can actually scale.

Bakkt to the future

With Baakt, they start with a 1 Day contract, the community doesn't cry fowl, they bridge the old money to the new, fees akimbo, great. That open interest is unlikely to become substantially larger than their daily volume, more likely the open interest will be a fraction of daily volume. They then position themselves to the retail public as anti-rehypothecation, but most likely with success on the 1 Day they'll consider quarterlies and monthlies, and we'd quickly see open interest expansion. However, there are many spread positions in derivatives. Calendar spreads are an example, people trying to milk out a living at the edge of market efficiency, that expansion of open interest is inflationary to some extent and is rehypothecation-like, but it's still healthy for market liquidity. What we'd like to see is the equivalent of the CME's Commitment of Traders report for bitcoin derivatives, breaking down hedgers vs. speculators, and ideally, to separate the inflationary OI from the deflationary.

A loan default is deflationary. The money goes out of existence, it's balanced, and it's why the Fed has done okay manipulating interest rates for the last 40 years. Derivatives portfolios are similarly limited. For swaps and futures open interest, scarcity in the cash-collateral is needed to capture the "risk-free" return of swap payments or futures premium; this creates demand in spot markets, soaks up supply, and puts BTC to work as collateral on higher time horizons.

But if Baakt, or even enterprising traders, are willing to adapt the horizon of Wall St. derivatives practice to loosening the margin requirements of Lightning-type DEX environments, we could end up with a situation where 1 BTC in margin can be used to portfolio-margin a lot of spreads in CVA options vs. BTC settled options that reference some price. We could then have those under-writers hedge by using graph default swaps, the equivalent of Credit Default Swaps but for sets of networked counterparties. These GDS price the risk of different sets of channels operating by different margin rules, and perhaps also with detectable capitalization levels that indicate greater risk, it will be possible to trade these GDS instruments effective in dynamic, data-informed strategies.

Imagine a CDS on BitMex's contracts: the CDS pays you whatever percent of open interest is experienced as a shortfall on BitMex due to margin calls that are unfilled by a fast-moving market. BitMex has an insurance fund and a lot of revenue to replenish it, but let's say it didn't, such a CDS might be relevant to some traders, and provide a seemingly "free money" yield to those willing to take the other side. Now imagine the same for a decentralized BitMex based on LN. The nuanced degree of how much a contract shortfall can amount to makes these GDS potentially much more efficient to trade than traditional CDS, which deal in tail risks, usually involving extreme binary events. Sometimes corporates go bankrupt and semi-senior notes recover at some rate, or sovereigns default and try to force a restructure, but the percentages involved are usually greater than 50 percent of face value, rather than the 2-25 percent range that a volatility-stricken decentralized contract might suffer margin short-falls.

There are two strong attractors: the higher time-value based return of deploying BTC in the LN to channels operating along CVA-type margining, and the demand for leverage which keeps those premiums enticing. It's a bilateral way of doing leverage in the Lightning Network between chains, in the form of options, which could complement more "traditional" perpetual swaps (less than three years old, BitMex launched XBTUSD perpetual swap in April 2016) that settle on LN just in BTC or LTC. All these forms of leverage create, temporarily, and against risk, some inflation in the trade-able supply of these coins. That's just a fact of life.

Gold as an analog only goes so far

If we look at what happened to the gold market, prior to China's buy-out plans, the lending of gold allowed banks to lend more gold on-paper than they had sitting in a vault. Gold banking, in other words. Before anyone turned in their tallysticks to buy shares in the Bank of England, gold receipt issuance was a source of fiat inflation. In the London/New York gold market structure, both spot and derivatives markets were saturated with multipliers. These were not transparent systems, LN counterparties are probably much more auditable. It's arguable that 200x open interest to warehouse inventory ratios, or having less detectable dilution of supply through rehypothecation of gold was bad for the gold market, and made some ideological investors pretty upset. But let me ask you: if your collateral is so good, why should it not be utilized like any other collateral? The main issuing is one of auditing transparency so that extreme financial practices don't create moral hazards, systemic risks and information asymmetry. There's a strong argument to be made

that historically, when people were allowed to create currency, e.g. credit instruments, to facilitate trade, prosperity rose. See the late Stephen Belgin and Bernard Lietaer's book *New Money For A New World* for more color on that. It's probably not so simple as, fixed supply good, expanding supply bad. Elastic supply that is intelligently allocated, not by a single intelligent planner but by many people lending, trading, working, building and so forth in the economy, based on value production, not political graft, that is what seems to make a currency most dynamic and valuable. See also Niall Ferguson's chapters in *The Ascent of Money* regarding the fortunes of the gold-hungry Spanish vs. the debt-happy Italians, it's like night and day.

Power money that is more scarce in supply becomes useful as a market referent and collateral base that has the lowest perceived counterparty risk on the planet, which then evolves a complementary market mechanism. As with interest rates, a balance is achieved through price discovery, between inflation and deflation.

Bitcoin is valuable because it serves a purpose in that market mechanism, but with the added hyperfungibility of information; it's globally transversable, melting capital controls like the invisible, imaginary boundaries they are. So it's got an uptrend. It's got time value as collateral. It's got other derivative time-value returns that can be obtained at times, by using it to hedge, shorting those derivatives. These things have so far reinforced each other, with other key metrics like the thickness of Bitcoin's mining moat being positively correlated.

King of collateral

This is how BTC becomes king collateral for the world:

1. Lightning Network Swap Dex's
2. Inter-chain Counterparty Value Adjustment Options Exchanges
3. Reinsurance-like market for Graph Default Swaps that create side-bets, mostly for hedging purposes we assume, on the credit risk of different galaxies of the LN.
4. Now with the ability to have yielding synthetic cash, leveraged bets, options markets, the works, and leading the way in new derivatives frontiers that attract the brightest quantitative traders to seek fortunes in a new wild west of risk hedging, we finally show the legacy financial system what a parallel, independent, systemic risk-quantified financial system can look like.

Whereas banks currently employ quants crunching simulations of graph triangle-counters to try and process nettings of various derivatives counterparties (we're talking about hundreds of thousands of big to medium sized bank counterparties), we can do this on the scale of hundreds of thousands of LN nodes. The utility in UTXO money is increased significantly.

In conclusion, I think the fear of rehypothecation may be overstated, but it's indeed possible, and BTC scalability will depend on the influence of fiat-liquidity into the system, seeking a USD-benchmarked return, which will to some extent dilute supply through leverage. But on the other hand, safe-returns-seeking capital will tend to do the opposite,

put on a 1:1 fully collateralized position, and ride it for the USD interest rate, which is very bullish for the supply and demand dynamics of any commodity money that becomes a popular synthetic-USD base.

I think most likely, the most extreme leverage, with the most survivability, will be with the most professional risk managers who can crunch the math on these derivatives and start making markets. Maybe not the 90 percent quoting-time market makers, but those who take smart views to trade mis-priced hedges, who take a market view, who lean into LN constellations with the best margin rules, or who exploit convexity between different instruments.

And that means most of the leverage dilution in imminent supply will be a boon to liquidity, and the sort of leverage that gets people rekt will remain a modest component of overall supply and demand. This will make Lightning many times more capital efficient, maybe not 10x like the typical fractional reserve banking money multiplier, but enough to create convex liquidity aggregation benefits in the LN in general.

Nik Bhatia's counterparty risk spectrum fits into this. He cited cold storage as near-zero counterparty risk (there's still operational risk of physical attack vectors and the credit risk of the underlying blockchain, small though it may be) and the average optimized return for routing fees a bit further up that scale, because you have to be in a live hot wallet perpetually to operate for that revenue. Then, off-chain lending was this example of a riskier thing yet, which veers into the realm of counterparty risk. But HTLCs used for margining general derivative contracts with BTC also come with counterparty risk that must be priced to make HTLC's incentive-aligned enough that those trading mechanisms actually work. We're probably going to need to evaluate Schnorr-based discrete log contracts or some modification on the HTLC-based cross-chain atomic swap model, such that one party clearly holds the option, and the other party is short it. Having either side be equally able to jerk out of the trade is too problematic to be priced and functional.

It's not just about 2:2 locked channels, hashed timelocks, or 2:3 watchtowers. There's also 2:3 of M multisigs, where M is the number of signers, being used as a state channel for Byzantine Fault Tolerant staked sidechains. These create more decentralized watchtowers, allow for instant-finality of signed transactions, and facilitate state references to co-ordinate LN DEX contract settlements, especially once the migration to stealthy transactions with Schnorr/Taproot/unicast begins.

BFT Sidechains are going to figure into solving some of the technical weak spots in the Lightning Network settlement model. It bears considering, when I use portfolio margin on Deribit, ultimately Deribit is assuming underlying clearing risk for me blowing up my account. Perish the thought, but let's say I was a sloppy options trader and I sold 10x the number of naked calls as my equity, Deribit would end up on the hook after that sudden \$500 snap rally that you know can happen any day. Who takes the role of Deribit to enable more sophisticated margining? It would have to be the sidechain, with collateralized validators checking up on state, taking small fees, another layer of income and risk removed.

Turns out this risk spectrum goes in deep if you zoom in on the middle. It's probably the next big thing in derivatives, fueled perhaps by hyper-bitcoin-dollarization, a process of mainstream finance replacing the Eurodollar model with a bitcoin-backed dollars model. If you look into how much time and money is spent on Wall Street trying to deal with collateralization and counterparty risks, you could see how with just the right amount of momentum, just the right amount of debt supercycle unwinding, macro tail-winds, pricing in every inch of a vast semi-decentralized network of dealers, could become quite interesting for Wall Street. They need this financial system, it will eventually save them so much money vs. the old, not because "blockchain technology reduces overhead on back-office auditing and compliance tasks – for the enterprise." But rather because the collateral discounting rates will precipitously favor it. Time value of money is the crux of the whole banking business and they will follow the value in time.

Thanks to Nik Bhatia for providing good feedback on how to reposition the key themes of the essay front and center. Also to Dan Goldman for technical feedback.

Patrick Dugan is a writer, trader, and designer. He founded TradeLayer, a protocol to introduce a native derivatives layer on top of Bitcoin and Litecoin. In previous adventures, Patrick worked in game design, temporarily administered the Omni Layer foundation and ran a sustainable farming-oriented ecommerce website._

Security Budget in the Long Run

By Paul Sztorc

Posted February 14, 2019

A discussion of Bitcoin's ability to resist 51% attacks (ie, its "security budget"). Competition makes it difficult for one network to collect enough fees – instead, we should try to collect fees from all networks. This post is a somewhat more-empirical sequel to "Two Types of Blockspace Demand". And to my Building-on-Bitcoin talk.

1. The "Security Budget"

Bitcoin's "security budget" is the total amount of money we pay to miners (or, if you prefer, the total amount spent *on* mining – they are the same thing). When this value is low, 51% attacks are cheap. In 2018, BTC's security budget was about \$7 million per day. So, the suppression of BTC (via a never-ending campaign of 51% attacks) would cost –at most– \$2.6 billion per year.

\$2.6 B is pretty low – by comparison, the 2017 annual US Military Budget was \$590 billion, and the FED's annual operating expenses totaled \$5.7 billion.

2. The Block Subsidy

Fortunately, we can expect the *block subsidy* to give us more security in the future. Even though it "halves" once every four years (effectively falling by a factor of 0.84 per year), it hits for full force no matter how high the BTC exchange rate climbs. As long as annual appreciation 19%+, it fully compensates for the PP lost to the halvening. Historically, the rate has been *much* higher than 19% (more like 70%+), and so the security budget has increased substantially over time, and will continue to do so for a while.

Of course, eventually the exchange rate must stop appreciating. Even if Bitcoin is outrageously successful, it will apparently reach a point where it simply cannot grow faster than 1.077 per year⁴, as this is apparently the growth in the nominal value of all the world's money.

Here I show the growth, and ultimate decline of the security budget:

Security Budget over next 40 yrs, if Fees are Zero						
Year	Subsidy	Exchange Rate (theoretical maximum)	Exchange Rate (market-imputed)	BTC Security Budget (billions per year)	USA Defense Spending (billions per year)	Safety Ratio
	from protocol	$x_{2017} = \$11.22M$, growth = 1.077	$x_{2016} = \$700$, growth = 1.6265; blended with maximum	= Subsidy * Exchange Rate (m.i.) * 6 * 24 * 365 * (1/1e9)	$x_{2015} = 637$, growth = 1.047	Security B. / Defense B.
2008	50	\$2,725,960	\$0	\$0.00	\$461.76	0.000
2012	25	\$3,671,828	\$100	\$0.13	\$554.95	0.000
2016	12.5	\$4,945,897	\$700	\$0.46	\$666.96	0.001
2020	6.25	\$6,662,050	\$4,900	\$1.61	\$801.57	0.002
2024	3.125	\$8,973,683	\$75,000	\$12.32	\$963.36	0.013
2028	1.5625	\$12,087,419	\$800,000	\$65.70	\$1,157.79	0.057
2032	0.78125	\$16,281,574	\$15,000,000	\$615.94	\$1,391.47	0.443
2036	3.9E-01	\$21,931,039	\$21,931,039	\$450.27	\$1,672.32	0.269
2040	2.0E-01	\$29,540,785	\$29,540,785	\$303.25	\$2,009.85	0.151
2044	9.8E-02	\$39,790,999	\$39,790,999	\$204.24	\$2,415.50	0.085
2048	4.9E-02	\$53,597,887	\$53,597,887	\$137.55	\$2,903.02	0.047
2052	2.4E-02	\$72,195,560	\$72,195,560	\$92.64	\$3,488.94	0.027
2056	1.2E-02	\$97,246,350	\$97,246,350	\$62.39	\$4,193.13	0.015

Above: Bitcoin's security budget over time.

Each row refers to a different year. Theoretical max exchange rate from the [Game and Watch paper](#). Imputed exchange rate is historical rates and growth factors, with some manual "blending in" so as to more rapidly approach the theoretical maximum. Defense budget extrapolated from [wikipedia data](#). "Safety Ratio" is the percentage of military budget that would be needed to disable Bitcoin. All numbers are in nominal dollars.

The "indifference" epoch is one where Bitcoin is vulnerable, but few adversaries squander their opportunity to attack because they are not paying attention. The "healthy" epoch is one where BTC should be able to deter 51% attacks even from ultra-wealthy motivated adversaries. But the "decline" epoch shows us a bleak future, in which 51% attacks on Bitcoin are easy again.

3. Transaction Fees

i. The Desired "Fee Pressure"

As is commonly known, *transaction fees* are expected to come to the rescue. As [Greg Maxwell](#) remarked:

fee pressure is an intentional part of the system design and to the best of the current understanding essential for the system's long term survival

He [later famously wrote](#):

Personally, I'm pulling out the champaign that market behaviour is indeed producing activity levels that can pay for security without inflation.

This view, (of a needed "fee pressure"), is common. Roger Ver has [compiled similar quotes](#) from other Bitcoin intelligentsia. Roger did this in order to discredit them politically, but the quotes are nonetheless accurate.

ii. The Dual Nature

The dual nature of Bitcoin (as both a money-unit, and a payment-rail) has confused people since Bitcoin was first invented.

In general, monetary theorists and economics ignored the payment-rail (and dismissed Bitcoin as supposedly having “no intrinsic value”). Businessmen and bankers ignored the money-unit (and regarded purchases of *BTC* as hopelessly naive), and instead tried hopelessly to rip-off the “blockchain technology”.

The confusion persists today in the “scaling debate”, in the form of a discussion over whether or not the “medium of exchange” use-cases are more valuable than the “store of value” use-cases.

And I think it persists in long-run security budget analysis, as well. Consider the following table:

Revenue Source	Block Subsidy (12.5 BTC)	Transaction Fees
Market's Units	...of BTC	...of block space
Price Units	... \$ (PPP) per BTC	\$ (PPP) per byte
If BTC price = moon...	...SB Goes Up	...SB <i>Unaffected</i>
Meme	Store of Value	Medium of Exchange
Slogan	“Digital Gold”	“P2P Electronic Cash”

While the two are mixed into the same “security budget”, the block subsidy and txn-fees are utterly and completely different. They are as different from each other, as “VISA's total profits in 2017” are from the “total increase in M2 in 2017”.

VISA's profits are a function of how cost-effectively VISA provides value to its customers, relative to its competitors (MasterCard, ACH, WesternUnion, etc). Changes in M2 are a function of other things entirely, such as: election outcomes, public opinion, business cycles, and FED decisions. There is some sense in which M2 “competes” with the Japanese Yen, but there are really no senses in which it competes with MasterCard.

iii. Are fees truly paid “in BTC”?

Transaction fees are explicitly priced in BTC. But, unlike the block reward, they *do* react to changes in the exchange rate. As the exchange rate rises, a given satoshi/byte fee rate becomes more onerous, and people shy away from paying it.

And so tx-fees are not really “priced in BTC”, despite the protocol's attempt to mislead us into thinking that they are. They are actually priced in purchasing power, which –these days (pre-hyper-bitcoinization)– is best expressed in US Dollars.

So, it is entirely appropriate to say, for example, that "in Dec 2017, BTC had tx-fees as high as *twenty-eight dollars*". And it would be inappropriate to say that the tx-fees were "as high as .0015,0000 BTC". For if the BTC price had been 10x higher², the tx-fees would have only reached .0001,5000 BTC.

iv. Stimulating Production

Whenever prices rise, entrepreneurs are induced to produce. (Owners are also induced to sell, but we are not interested in that right now.)

The supply of BTC is famously capped at 21 million. The *produced* supply (aka the "new" supply) is currently capped at 12.5 BTC per block, until the next halving.

The supply of a completely different good, "btc-block-bytes", is also capped. It was first (in)famously capped at 1 MB per block, and now is capped at something-like 2.3 MB per block.

As was just said: whenever blocks become more valuable, entrepreneurs search for ways to produce more of them.

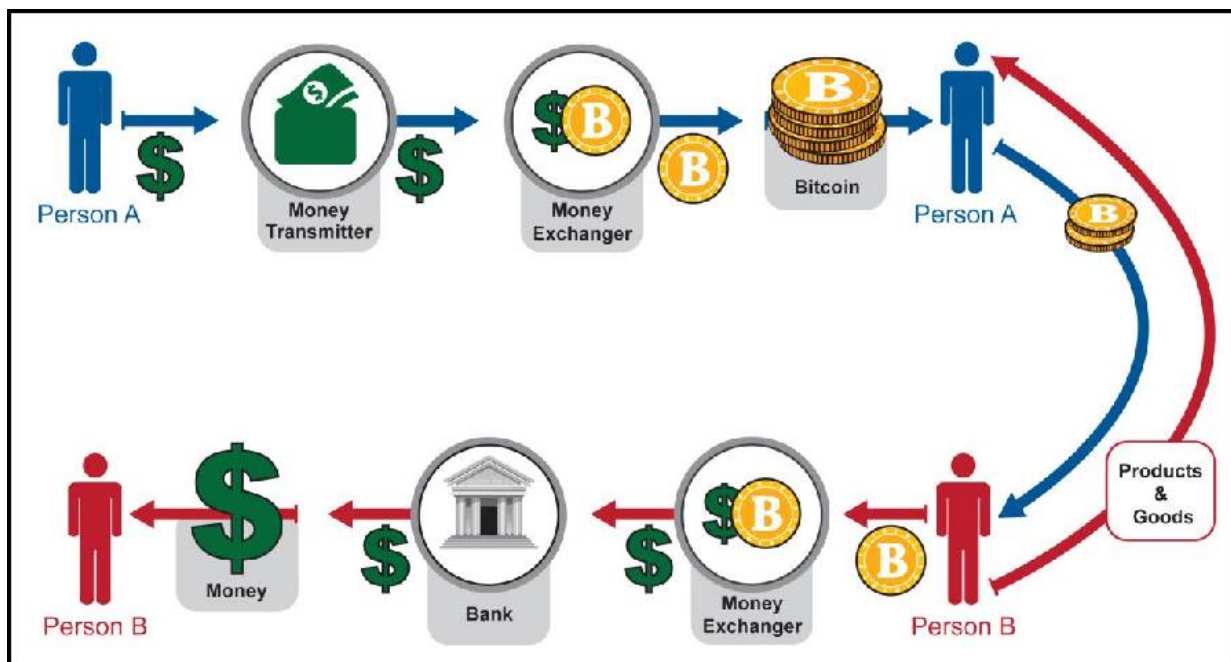
One way is to reactivate older, marginally unprofitable mining hardware. Production then hastens...temporarily. Of course, after the next difficulty adjustment, block-production will return to its equilibrium rate (of 1 block per 10 minutes).

Alternatively, entrepreneurs can create, and mine, Altcoins.

v. Altcoins as Substitute Goods

Alt-"coins" are *very poor* substitutes for Bit-"coins". Each form of money, is necessarily in competition with all other forms: money has strong network effects; the recognizability property has super-linear returns to scale; exchange rates are transaction frictions that are inconvenient; etc. What people wanted was a BTC. They wanted to *get rid of* all their other forms of money!

But it is the reverse when we consider transaction fees and "btc-block-bytes": Altcoin-blockspace is a pretty good substitute for Bitcoin-blockspace. Remember that this type of demand has *nothing to do* with obtaining BTC. Users merely wish to buy something using the Bitcoin payment-rail. This image from 2013 FINCEN Congressional testimony hopefully makes it clear:



insert caption here

Since the amount of coin sent in a blockchain payment is always configurable, it will always be possible to send someone “twenty dollars” worth of LTC; or “one BTC” worth of DOGE; or “one sandwich” worth of EOS. All of this is made much easier by the “exchangers” (ie: Coinbase, ShapeShift, SideShift, BitPay, LocalBitcoins, multi-currency wallets, CC ATMs, etc) which now take numerous forms and are easy to use.

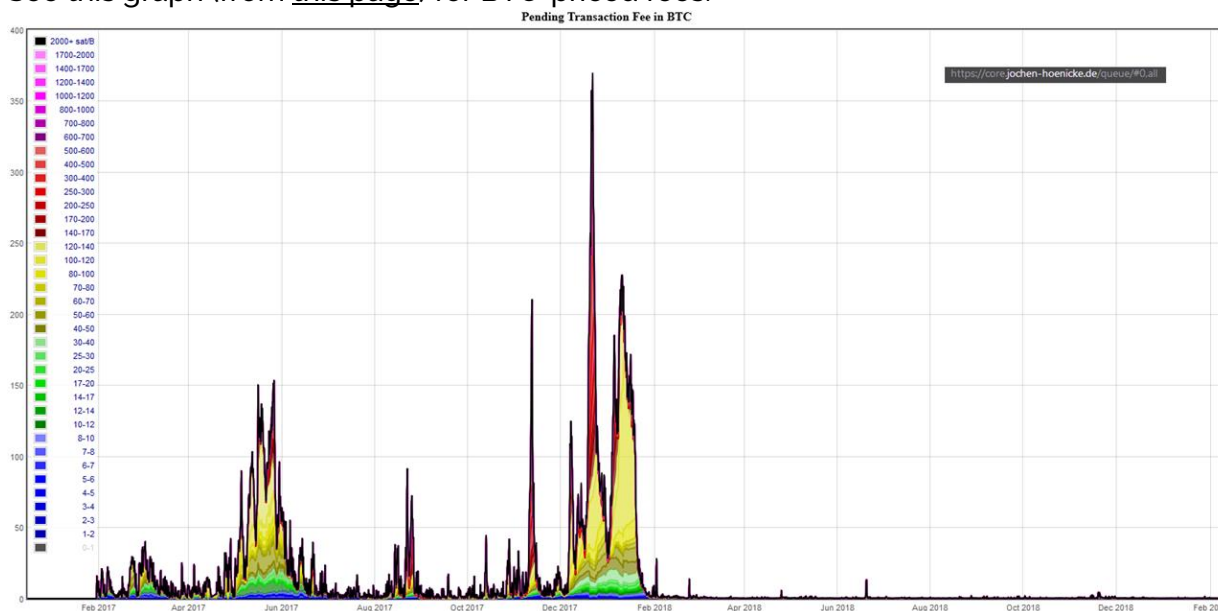
Furthermore, this (true) premise –that Altcoin-payments are indeed substitutes for Bitcoin-payments– is occasionally explicitly admitted³, even by hardcore maximalists. Especially during the last fee run-up in late 2017:

- Samson Mao
- Francis Pouliot
- “The digital currency for payments”

vi. Competitive Demand for the Payment Rail

The supposedly-essential “fee pressure” has, for the moment, deserted us.

See this graph (from [this page](#)) for BTC-priced fees:

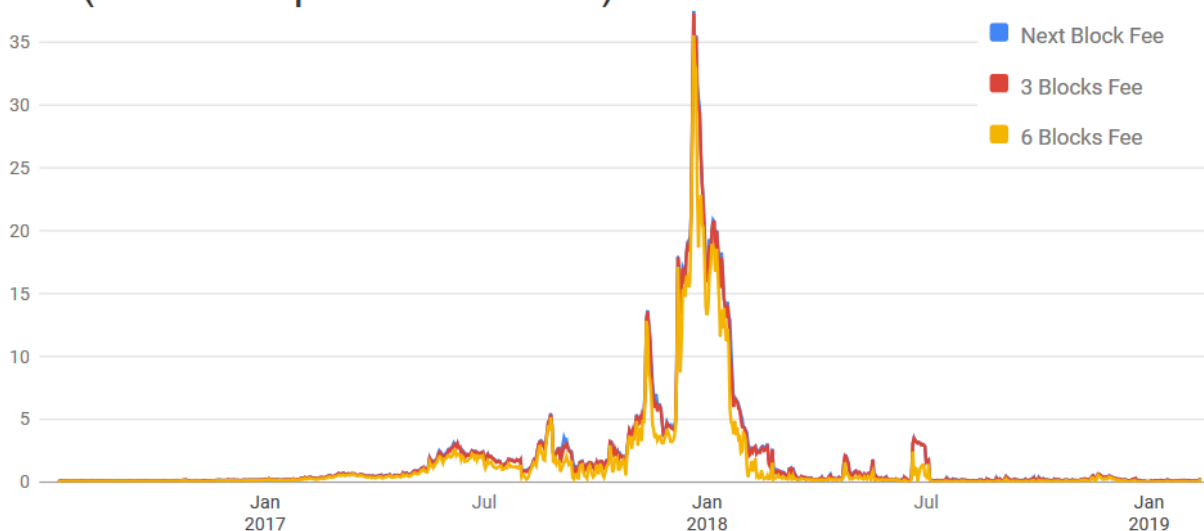


insert caption here

And this graph (from [this page](#)) for USD-priced fees:

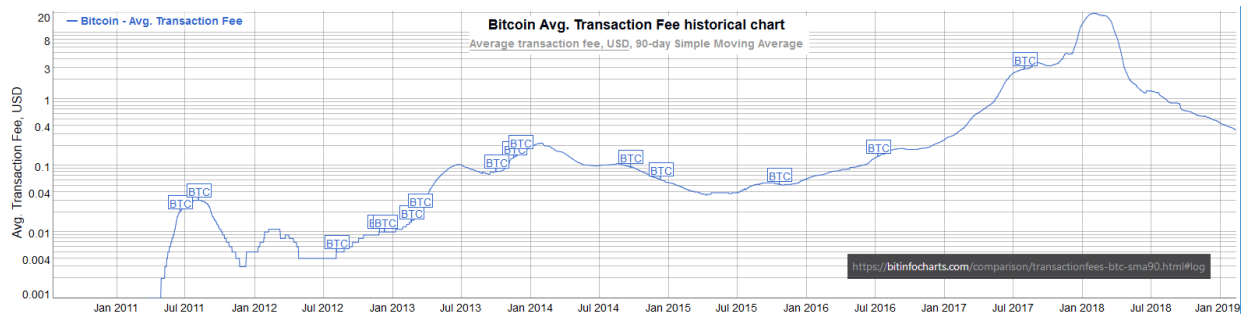
Historic daily average Bitcoin transaction fees

(in dollars per transaction)

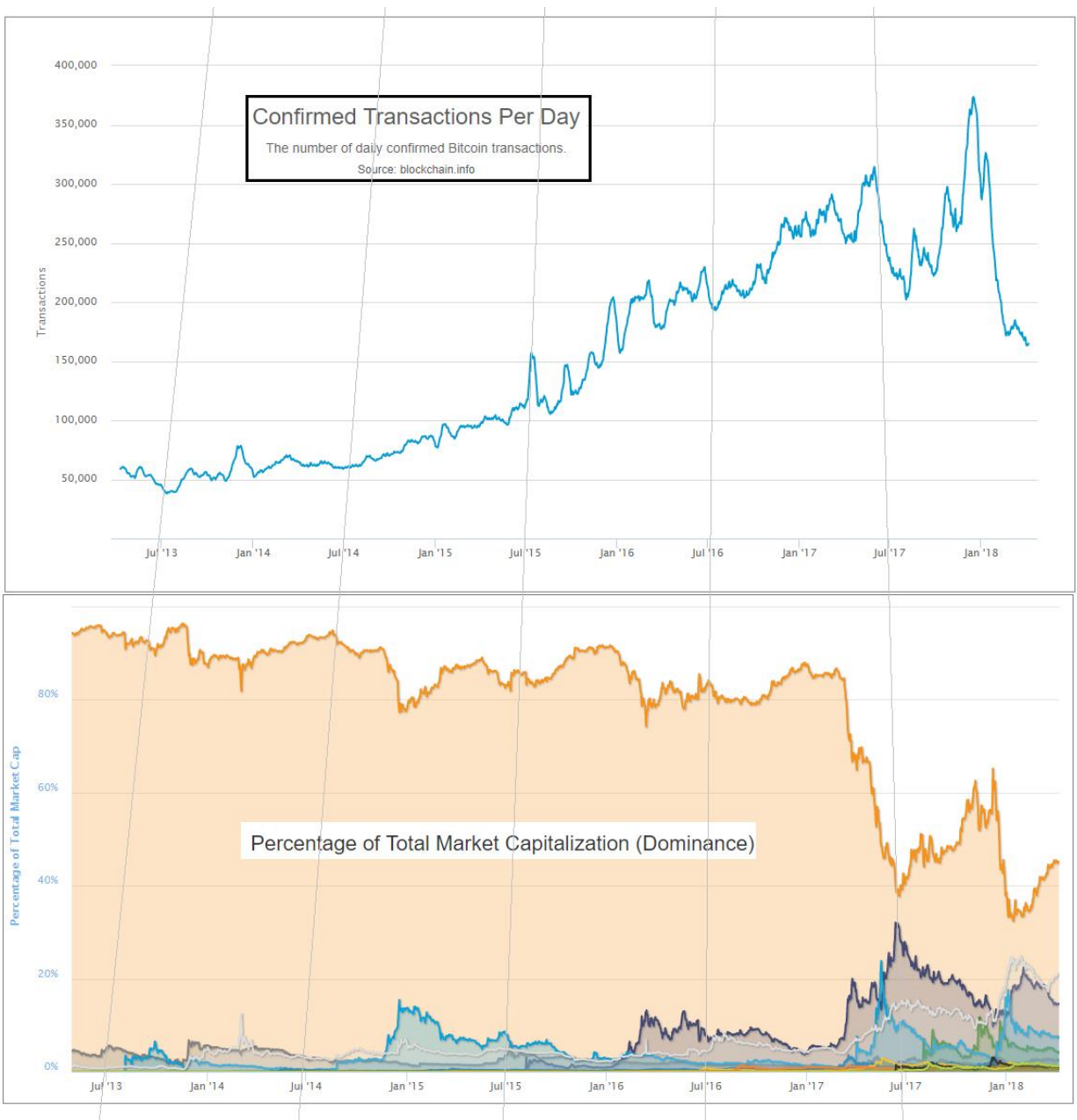


We see that fee pressure has crumbled. Today, a typical transaction will cost 30-40 cents – much cheaper than a VISA txn.

Compare the historical data, given in 90-day moving-average ...



...to the two graphs below:



We see that BTC's crossing of the "1 USD per transaction line", in May of 2017, coincides with the rise of Altcoins. We also see that the "pressure" of late 2017 quickly canceled itself out, and then some. Finally, we see that this release-of-pressure coincided with a sudden (and unprecedented) decline in BTC-transactions.

To me, this data refutes the theory that users will pay high BTC fees willingly. In fact, they seem to have only ever paid high fees *unwillingly*— during a brief "bubble" time (of relative panic and FOMO).

If that theory is indeed false, then total fees will not be any higher—in USD terms— than they are today.

According to blockchain.info, fees in the last 12 months totaled \$70 million. (In the 12 months before *that*, they were \$770 million).

Revisit the [chart above](#), and you will see that this barely registers. After all, when \$70 M is priced in the units of the chart (billions), it is just \$0.07.

If the consumer is cost-conscious, and will only pay the lowest tx-fees, then how can we get those numbers up?

vii. Alternative Fee-Sources

a. Lightning Network

The Lightning Network (if successful) will allow very many "real-life transactions" to be fit into just two on-chain txns.

The immediate effect of this, is to *lower* on-chain transaction fees; but the ultimate effect is increase them. LN boosts on-chain fees by increasing the utility of each on-chain txn (by allowing each to do the work of many txns), and by therefore making high on-chain fees more tolerable to the end user.

Exactly how much will LN boost fees?

At this point – it is anyone's guess. But *my* guess is that they cannot realistically increase by more than two orders of magnitude.

First, on-chain txns are needed to create, and periodically maintain, the LN. So LN-users will still be paying on-chain fees; and will still prefer to minimize these costs. Meanwhile, Altcoins will have their own Lightning Network (they will copy LN, just as they've copied everything else). All of these LNs will compete with each other, the same way that different blockchains compete with each other.

Keep in mind, that the fees paid to LN-hubs⁴ will, by definition, *not* be paid to miners. So, there is no sense in which LN-fees "accumulate" into one big on-chain txn-fee (in contrast to how *the economic effect* of each LN-txn *does* accumulate into a single net on-chain txn).

Second, the LN user-experience will probably always be worse than the on-chain user-experience. LN is *interactive*, meaning that users must be online, and do something [sign a transaction] in order to receive money. It also means that your LN-counterparties can

inconvenience you (for example if they stop replying, or if their computers catch fire) or outright harass you. LN also comes with new risks – the LN-design is very clever at minimizing these risks, but they are still there and will still be annoying to users. Users will prefer not to put up with them. So they will tend to prefer an Altcoin on-chain-txn over a mainchain-LN-txn.

b. Merged Mining Sidechains

Merged-Mined Sidechains do whatever Altcoins can do, but without the need to purchase a new token. So they have infinitely lower exchange rate risk, and are more convenient for users.

On top of that, MM SCs send all txn-fees they collect to Bitcoin miners. Under Blind Merged Mining, they do this without requiring any users or miners to run the sidechain node software.

A set of largeblock sidechains could process very many transactions. In the next section, I will assume that the total Sidechain Network replaces VISA, (and VISA alone), and captures all of its transaction fee revenues. VISA is only a small percentage of the total payments market (which includes checks, WesternUnion, ApplePay, etc), but it is a good first look.

viii. VISA's Transaction Fee Revenues

Contrary to what I believed just moments before looking this up, VISA does not earn any money off of the interest that it charges its customers.

Observe page 40 of their most recent annual report:

Our operating revenues are primarily generated from payments volume on Visa products for purchased goods and services, as well as the number of transactions processed on our network. We do not earn revenues from, or bear credit risk with respect to, interest or fees paid by account holders on Visa products. Instead VISA's revenue comes from transaction fees. This perfectly facilitates our comparison.

Total revenues were 18,538 \$M in 2017, up from 11,778 \$M in 2013. This corresponds to quite an annual growth rate – 12% per year.

If we assume that current trends holds, we get the following:

Security Budget over next 40 yrs (assuming VISA-level fee-revenues)								
Year	Subsidy	Exchange Rate	Exchange Rate (market-imputed)	Block Subsidy (billions per year)	VISA Tx-Fee Revenues (billions per year)	Total Security Budget (billions per year)	USA Defense Spending (billions per year)	Safety Ratio
	from protocol	$x_{2017} = 1.077$	$x_{2016} = \$700$, growth = 1.6265; blended with maximum	$= \text{Subsidy} * \text{Exchange Rate (m.i.)} * 6 * 24 * 365 * (1/1e9)$	$x_{2017} = 18.538$, growth = 1.120	$\text{sum}(\text{block_subsidy} + \text{VISA_fees})$	$x_{2015} = 637$, growth = 1.047	Security B. / Defense B.
2008	50	####	\$0	\$0.00	\$6.68	\$6.68	\$461.76	0.014
2012	25	####	\$100	\$0.13	\$10.52	\$10.65	\$554.95	0.019
2016	12.5	####	\$700	\$0.46	\$16.55	\$17.01	\$666.96	0.026
2020	6.25	####	\$4,900	\$1.61	\$26.05	\$27.66	\$801.57	0.035
2024	3.125	####	\$75,000	\$12.32	\$41.00	\$53.32	\$963.36	0.055
2028	1.5625	####	\$800,000	\$65.70	\$64.53	\$130.23	\$1,157.79	0.112
2032	0.78125	####	\$15,000,000	\$615.94	\$101.57	\$717.51	\$1,391.47	0.516
2036	3.9E-01	####	\$21,931,039	\$450.27	\$159.87	\$610.14	\$1,672.32	0.365
2040	2.0E-01	####	\$29,540,785	\$303.25	\$251.63	\$554.88	\$2,009.85	0.276
2044	9.8E-02	####	\$39,790,999	\$204.24	\$396.05	\$600.29	\$2,415.50	0.249
2048	4.9E-02	####	\$53,597,887	\$137.55	\$623.37	\$760.92	\$2,903.02	0.262
2052	2.4E-02	####	\$72,195,560	\$92.64	\$981.15	\$1,073.80	\$3,488.94	0.308
2056	1.2E-02	####	\$97,246,350	\$62.39	\$1,544.29	\$1,606.68	\$4,193.13	0.383

"Indifference"
Epoch

"Healthy"
Epoch

[Link to Excel sheet](#)

Above: The 'security budget table' from earlier in this post, plus a new column: VISA transaction fees. These fees are added to the base block subsidy amounts, to get a new total security budget.

This security budget *does* seem to be much safer in the long run, and safer in general.

Conclusion


To deter 51% attacks, Bitcoin needs a high "security budget". Today's tx-fee revenues are not high enough; we must ensure that they are "boosted" in the future.

Higher prices (ie, higher satoshi/byte fee-rates) are one way of boosting revenue. Unfortunately, competition from rival chains acts to suppress the market-clearing fee-rate.

A better way, is to attempt to devour the entire payments market, and claim all of its fee revenues. This can be done using Merge Mined Sidechains, without any decentralization loss.

Footnotes

1. The math is that $1.077 = (25.94/5.85)^{(1/20)}$. And note that 1.077 is below the required "stasis rate" of 1.19. [\[D\]](#)
2. I mean that if the USD/BTC price had been 10x higher, throughout the "bubble" of late-2017. In other words, if Bitcoin had started Jan 2017 at around 9,000 USD/BTC and then risen to 190,000 USD/BTC. [\[D\]](#)
3. I do remember there being much more of this, but I could only find a few examples (before giving up). Please message me if you can find/remember any other examples. I guess I will eventually remove this paragraph if I never find any more. [\[D\]](#)

4. By “fees paid to LN-hubs”, I mean the fees that you would pay, (off chain), to any Lightning Node that your LN-payment routes through. 
-

Tweetstorm: Power and Money

By Saifedean Ammous

Posted February 17, 2019

Fiat money allows wars with no real cost to governments, which makes detestable bloodthirsty chickenhawk scum like [@MaxBoot](#) & [@BillKristol](#), who've never faced costs for their warmongering, the perfect "foreign policy experts".

Why Are These Professional War Peddlers Still Around? Pundits like Max Boot and Bill Kristol got everything after 9/11 wrong but are still considered "experts."

<https://www.theamericanconservative.com/articles/why-are-these-professional-war-peddlers-still-around-tucker-carlson-max-boot-bill-kristol/>

In 2003 Wolfowitz told Congress the Iraq war would be practically costless. It turned out to cost more than \$2Trillion. With hard money Wolfowitz would have had to raise the \$2T BEFORE war. With easy money, he can get his carnage on & leave taxpayers footing the bill for decades

Wolfowitz was not alone. Richard Perle, Lawrence Lindsay, Kenneth Pollack, Glenn Hubbard, Ari Fleischer, Donald Rumsfeld, & Mitchell Daniels all lied about the expected cost of war. They all got paid handsomely for it; never had to pay back a dime.

Who Said the War Would Pay for Itself? They Did! Unwise words from the "experts" who promised a cost-free war. <https://www.thenation.com/article/who-said-war-would-pay-itself-they-did/>

Modern "intellectuals", who are government propaganda parrots, think this is just how war works. I urge you to read Hoppe's Democracy The God That Failed for an explanation of how war functioned under governments forced to be responsible by hard money: [riosmauricio.com/wp-content/upl...](https://www.riosmauricio.com/wp-content/upl...)

Under hard money, governments had to finance their operations from their citizens, which made wars possible when necessary but bankrupted governments that engaged in unnecessary war. War was limited & contained to expensive armies kings were careful to not decimate needlessly.

Under hard money, governments fought till they ran out of their own money. Under easy money, governments can fight until they completely consume the value of all the money held by their people. This is why the century of central banking was the century of total war.

Whatever you think of the retarded Keynesian economics used to justify government control of money, you need to come to terms with the fact that the most horrific criminals of history have all operated with easy government-controlled money, as discussed in The Bitcoin Standard:

It is no coincidence that when recounting the most horrific tyrants of history, one finds that every single one of them operated a system of government-issued money which was constantly inflated to finance government operation. There is a very good reason that Vladimir Lenin, Joseph Stalin, Mao Ze Dong, Adolf Hitler, Maximilien Robespierre, Pol Pot, Benito Mussolini, Kim Jong Il, and many other notorious criminals all ruled in periods of unsound government-issued money which they could print at will to finance their genocidal and totalitarian megalomania. It is the same reason that the same societies which birthed these mass murderers did not produce anyone close to their level of criminality when living under sound monetary systems which required governments to tax before they spent. None of these monsters ever repealed sound money in order to fund their mass murder. The destruction of sound money had come before, hailed with wonderful feel-good stories involving children, education, worker liberation, and national pride. But once sound money was destroyed, it became very easy for these criminals to take over power and take command of all of their society's resources by increasing the supply of unsound money.

This is why bitcoin matters, and this is of course the point that critics of bitcoin miss. What better technology do you have for castrating scum like Kristol & Wolfowitz & preventing their sociopathic minds from capturing government money & causing millions of deaths?

Bitcoin's real cost is in hardware & electricity needed to run the network. Fiat's real cost is the hundreds of millions of deaths financed by government made omnipotent by inflation. Which do you find more expensive? Which would you rather pay in the twenty-first century?

Bitcoin might end up consuming half the world's electricity, but if it prevents one war, that would be the best bargain humanity ever got. Bitcoin might be the most important application of electricity. Can you think of a better use for electricity than neutering mass murderers?

A Primer on Bitcoin Investor Sentiment and Changes in Saving Behavior

By Tuur Demeester , Tamás Blummer , and Michiel Lescrauwaet

Posted February 20, 2019

In our conversations with institutional investors, we often get asked the question “What is your model to value Bitcoin?”. Investors want to know what the fundamental drivers are behind BTC price gyrations, and whether at a given time Bitcoin is overvalued, undervalued, or at fair value. The new measures we suggest here are tools to help with that judgement. We build on work that goes back to 2011, and use the Bitcoin blockchain to extract market information not generally available for traditional commodities.

We suggest two new ways to measure changes in Bitcoin saving behavior:

- Relative Unrealized Profit/Loss Ratio(=investor sentiment)
- HODLer Position Change(=insider buying/selling)

Also introduced is the Liveliness measure, which reflects the extent to which a cryptocurrency is meaningfully used by savers.

A History of Bitcoin Valuation Research

Here's an overview of the quantitative approaches we've seen Bitcoin investors take to help them decide what its fair value is at any given time.

- In 2010, Bitcoin users tried calculating the “value” of one Bitcoin by estimating the electricity cost of mining it. However, the usefulness of this was quickly dismissed, as the cost of mining goes up when investors bid up the price of Bitcoin.
- In 2011, early investors came up with the idea of calculating Bitcoin's market cap as a valuation tool, and with the concept of 'Bitcoin Days Destroyed'. The latter was dubbed an “indicator of market health and participation “ and it was the first valuation metric that considered the age of addresses. There was also discussion about a “Price over Difficulty” ratio, to determine whether it was better to mine than to buy BTC, and forum threads emerged about how many lost coins there might be.
- In 2012, Trace Mayer suggested the 200 Daily Moving Average of Bitcoin's market capitalization as a value indicator, because it filters out the long-term secular uptrend .
- In 2013, various authors explored the idea that Bitcoin's price is in a long-term parabolic uptrend, and that deviation from that trend line is indicative of over- and under valuation.
- On January 1st, 2014, user gbianchi proposed “Network Value” as the ratio of Bitcoin's address growth and its market capitalization — similar analyses followed later that year.

- In November 2014, developer Jon Ratcliff published his analysis of the blockchain, showing the distribution of bitcoins based on age of last use, and commented "This graph shows ... how many bitcoins are actively moving at any one time over time."
- In September 2017, Willy Woo and Chris Burniske published research around the NVT ratio, which was called a "PE Ratio for Bitcoin" as it focused on comparing Bitcoin's on-chain volume with its market cap.
- In March 2018, Dmitry Kalichkin suggested a variation on NVT which he dubbed the 90-day NVT ratio. Two months later he introduced the Network Value to Metcalfe ratio (NVM) which was based on Daily Active Addresses.
- In April 2018, Dhruv Bansal updated Ratcliff's work on UTXO age distribution, and suggested the concept of HODL waves. He commented: "It is not possible to make charts such as the one above for traditional asset classes. It's only Bitcoin and other public blockchains that meticulously track these data throughout their whole histories. This enables post-hoc analyses of large-scale market behavior."
- In October 2018, inspired by Pierre Rochard, Nic Carter and Antoine Le Calvez created the Bitcoin "realized cap" which is the aggregate value of the UTXOs priced by their value when they last moved. Soon after, Bitcoin "thermocap" or "accumulated security spend" was suggested, which is the aggregated miner revenues over the entire history of Bitcoin.
- That same month, Murad Mahmudov and David Puell published work on the Bitcoin Market-Value-to-Realized-Value (MVRV).
- In December 2018, Tamás Blummer introduced the concept of Liveliness, which reflects how much a given blockchain is used for meaningful transaction settlement.

Goal: Measure Changes in Saving Behavior

Given that we view Bitcoin's primary use case as censorship resistant store of value (digital gold), and its utility as a payment mechanism as only secondary, our main goal in identifying the components of our valuation toolbox is to find data that specifically reflects changes in *saving* behavior.

Limitations and challenges of existing valuation methodologies

The Bitcoin blockchain records a lot of data, but not all data. It is blind to how many bitcoins are lost. It doesn't know whether a transaction represents a transition from one owner to another (sale), or whether it's simply the same owner moving coins to another address in his control. It also doesn't reflect off-chain transactions—for example it won't show balance transfers from one Bitfinex user to another, or Liquid Sidechain transactions, or Lightning Network transactions.

The limitations of blockchain-recorded information, as well as the commodity nature of cryptocurrencies themselves, have consequences for valuation methodologies:

- With cryptocurrencies, information about real circulating supply is opaque, exchange listing requirements are often extremely loose, and dilution schemes can be stretched to extremes. Assigning a "market cap" to a cryptocurrency (mined

coins \times token price) doesn't at all create an objective comparison tool—a coin's "market cap" doesn't teach us anything about the commitment of coin holders. To illustrate: a centralized coin with a premined supply of 1 billion tokens and a single recorded sale of one token for \$10 would yield a \$10 billion market cap, identical to a decentralized coin with a large community of long-term savers. This "market cap" measure is also blind to lost coins, which stretches the comparison with the securities world where the assets are held by transfer agents, making loss a very rare phenomenon.

- The challenge with using the number of active addresses or transaction volumes (e.g. NVT, NVM) is that these data sources don't allow us to separate behavior that is long-term oriented from behavior that is short term oriented. These measures don't directly differentiate speculators from value investors, and can conceivably be gamed or inflated by moving a large amount of coins back and forth, or by creating a flurry of small on-chain transactions.

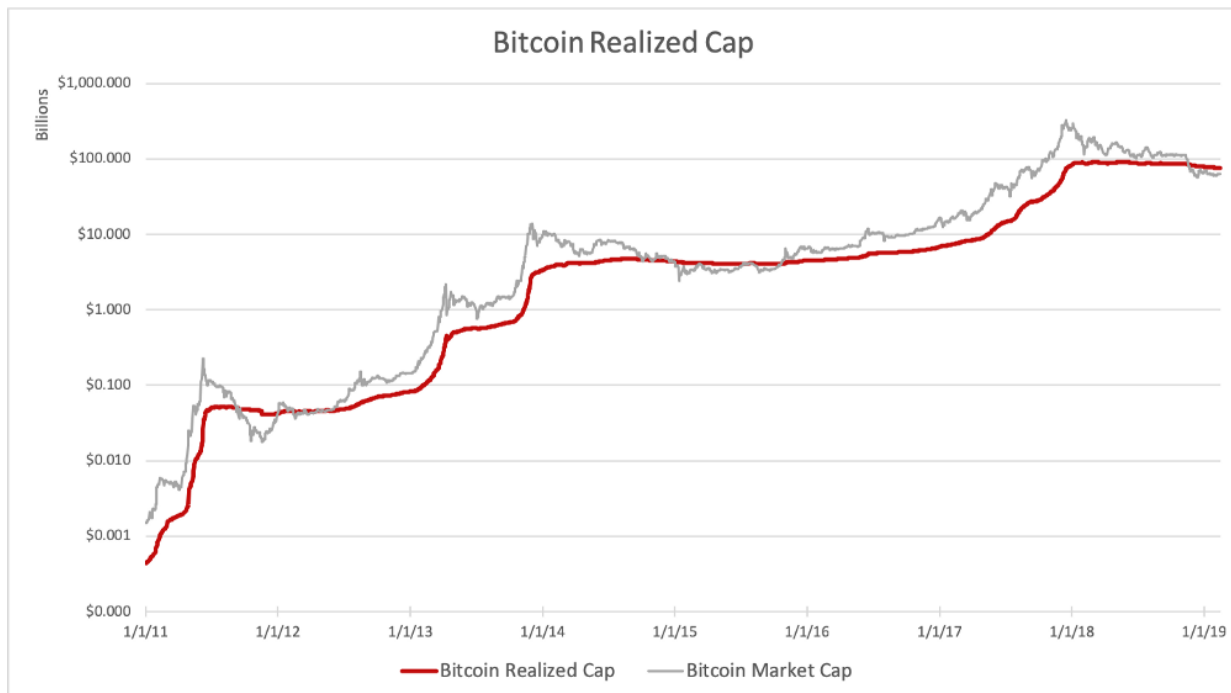
Solution

Our solution is to collect data that places each circulating quantity of Bitcoin *in its historical context*, in the tradition of previous work such as HODL Waves, Realized Cap, and MVRV. We focus on the data provided by *the Bitcoin blockchain*, as this is the ultimate (most secure and final) settlement layer for all its important transactions. By taking the Output Quantities of a block, and combining it with the Recorded Time of that block, we learn more about the behavior of Bitcoin savers.

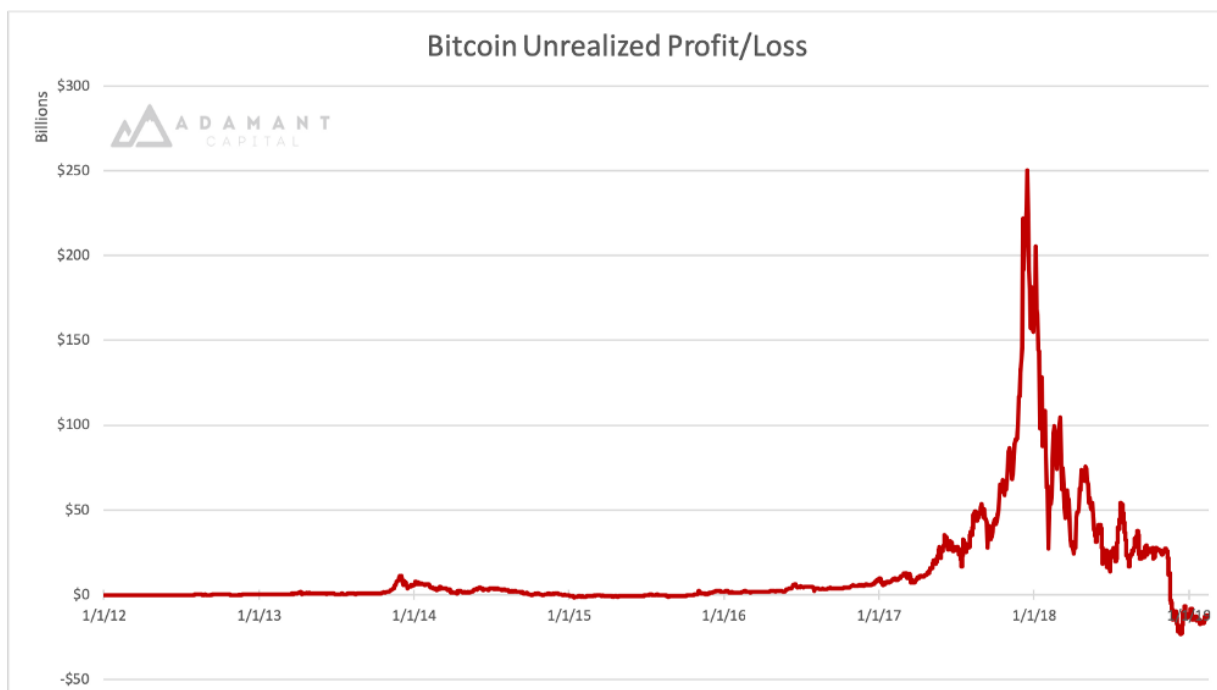
Relative Unrealized P&L (\approx investor sentiment)

Every time a bitcoin moves on the blockchain, its market value is realized. The owner was aware of its value and affirmed his control over it at the point of the move. It doesn't matter if the transaction represents the owner sending the coins to somebody else (a sale or gift), or if it is an act of self-dealing.

If we value every coin at the time it last moved and aggregate these values, we arrive at the "Realized Capitalization."



By subtracting the Realized Cap from the Market Cap, we calculate Unrealized Profit/Loss (P&L):



We see that Bitcoin investors in aggregate currently face a significant unrealized loss, which is quite a change if compared with the 2017 huge unrealized profits.

The measure of Unrealized Profit also contains the unrealizable profit of Lost Coins. Some coins are certainly lost as they were associated with a provably un-spendable output

script, but the majority of lost coins can only be guessed by setting a threshold of inactivity after we consider them Lost.

The measure of Unrealized P&L estimates the total dollar amount of paper profits/losses in Bitcoin, but it does not clearly filter out the relative change that accompanies it. By dividing Unrealized P&L by the Market Cap, we arrive at the Relative Unrealized P&L, which can be interpreted as an indicator of investor sentiment:



When a high percentage of Bitcoin's market cap consists of unrealized profits, it can be interpreted that investors are greedy. The ratio drops as prices decline and investors likely become more fearful. When the unrealized gains turn into unrealized losses, we enter the phase of capitulation and apathy. Here's a suggested illustration:



So why does the percentage of Relative Unrealized P&L go up in a bull market? What this indicates is that on average, investors are realizing profits at a slower rate than the growth in the market cap. For the time being, 20% of the market cap consists of 'underwater' holdings—coins that would generate losses if they were sold today.

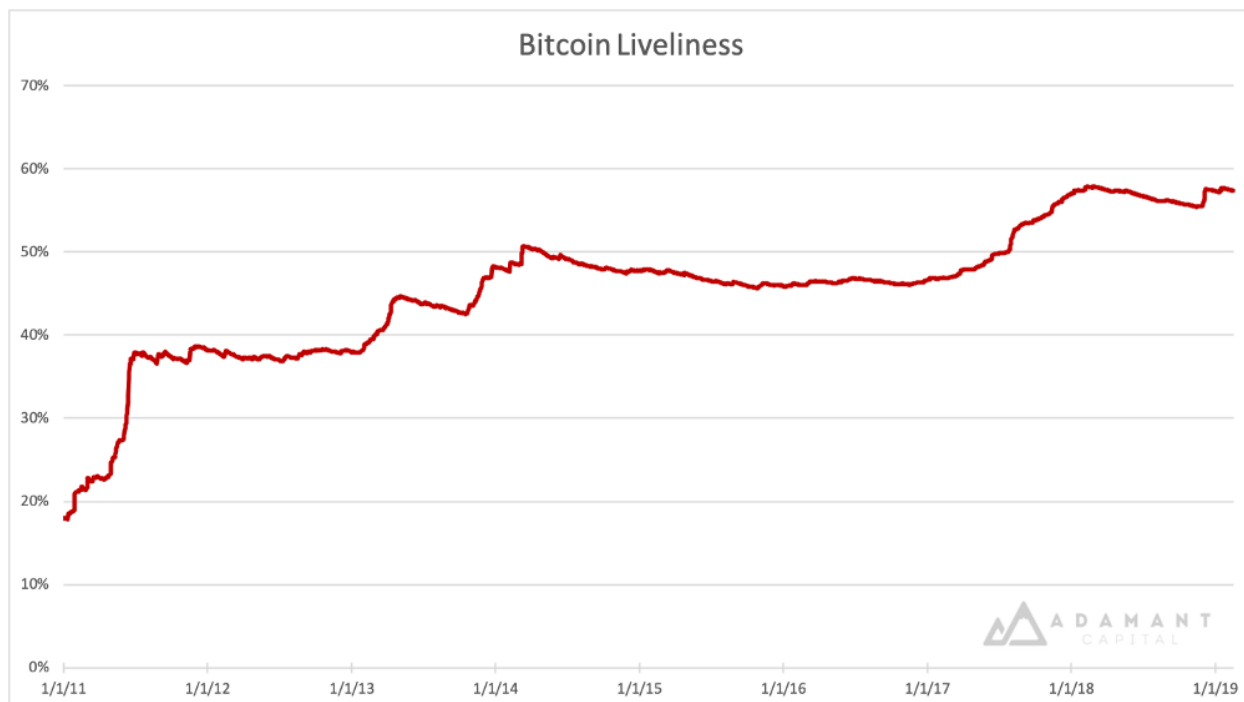
Before we move on to a new suggested valuation tool, HODLer Net Position Change, we first need to explain the measure of Bitcoin Liveliness.

Liveliness

The idea of old coins moving on the blockchain has always spoken to the imagination of Bitcoin enthusiasts and investors: "What are the 'Bitcoin whales' doing?", "What might Satoshi be up to?", etc. The analytical work mentioned in our historic overview provides investors with information on how Bitcoin savers move coins at any given time. However, the challenge with measures such as HODL waves is that they don't provide us with a clear signal or unambiguous utility. We instead propose *a single measure* that focuses on the coins that move relative to how long they were previously dormant.

What is Liveliness?

Liveliness is a new quantitative measure that gives insights to shifts in saving behavior. The higher the amount of meaningful transaction settlement a blockchain accommodates, the higher its Liveliness.



Liveliness can be defined as the ratio of the sum of Bitcoin Days Destroyed and the sum of all Bitcoin Days Ever Created. (See [here](#) for a more detailed breakdown.)

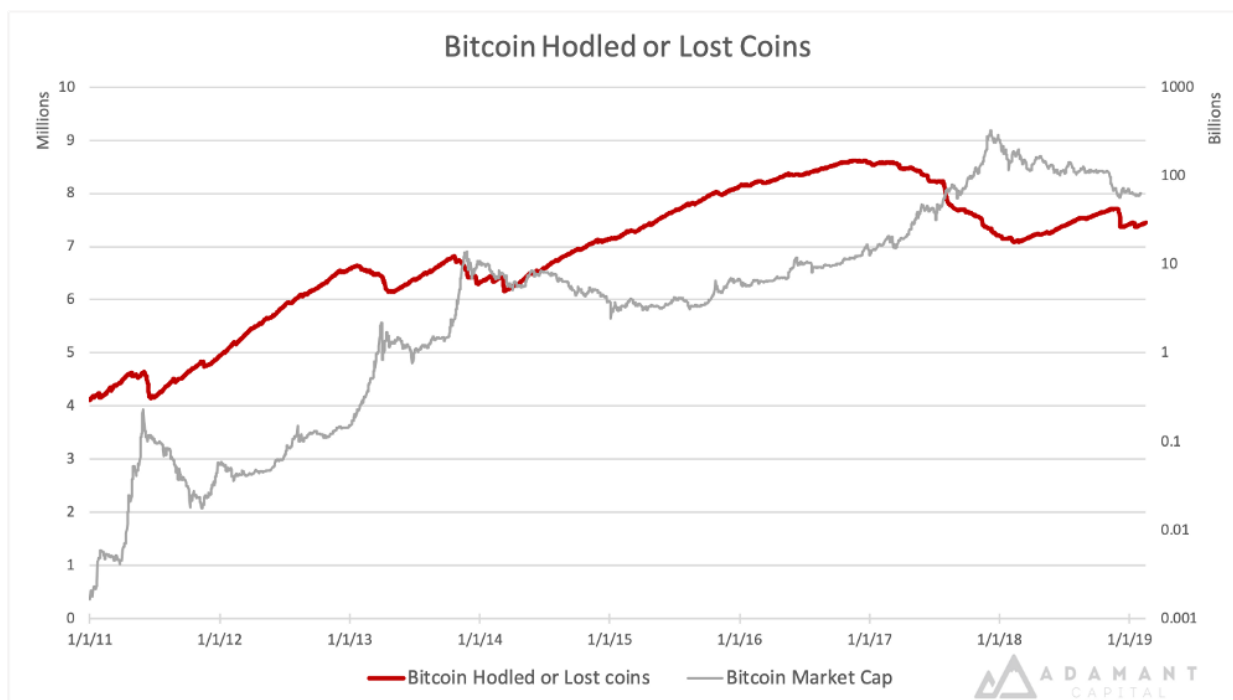
Let's illustrate with a few examples:

- A blockchain that during its lifetime has not yet seen a transaction other than issuance, has a Liveliness of 0%. Likewise, a blockchain where only one recent balance is systematically moved back and forth would produce a very low Liveliness—in other words, this measure is unforgiving for lack of meaningful transactions. Bitcoin has high Liveliness if it facilitates the transfer of large amounts of old coins on a regular basis.
- A blockchain where all the coins move within a single block has at that moment a Liveliness of 100%. A blockchain of two years old with no new block rewards, and where exactly one year ago all coins moved within a single block and no transactions moved since, would have a liveliness of 50%. In other words, the measure fluctuates relative to the total lifespan of the blockchain.
- The total circulating supply also impacts Liveliness: if in the previous example 20% more new coins were created in the year since all the coins were moved, then the Liveliness today would not be 50% but only 40%. So this measure also warns us about blockchains with high inflation/dilution.

Liveliness can be used to weight market cap if comparing cryptocurrencies, as it will be close to zero for currencies that have inflated market cap through pre-mined coins or wash trading of the same few units.

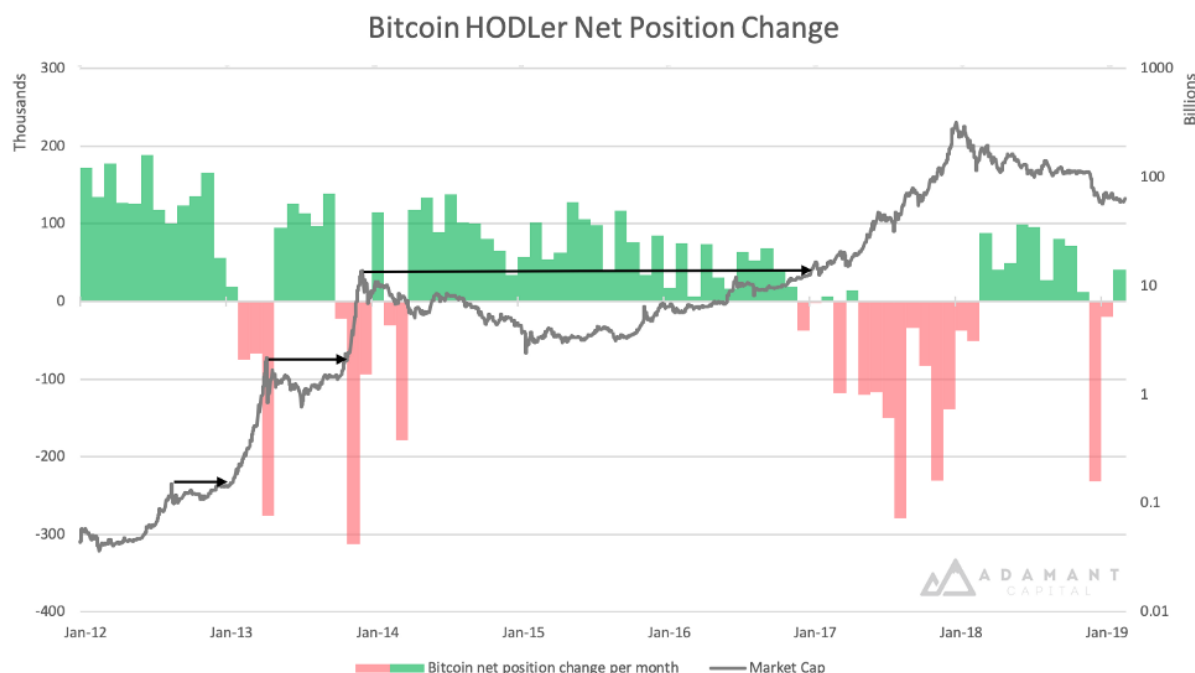
Besides this, Liveliness can also be used as a foundational tool from which to derive other insightful time series. One of these metrics is the aggregation of Lost or HODLed Bitcoins

and alerts us to moves of large and old stashes. For this purpose, subtract Liveliness from 1 and multiply with the circulating supply at the time.



HODLer Position Change (\approx insider buying/selling)

Now that we know the approximate number of coins that are held as a long term investment or are lost, we can approximate the monthly position change among Bitcoin savers. We call this measure HODLer Net Position Change. Because it only measures actual moves of coins, our graph naturally excludes lost coins.



We see that significant quantities were cashed out during bull markets of Bitcoin, and net new positions were accumulated by HODLers in bear phases. Net buying seems to switch into net selling once the previous top is reached (cf. arrows on the graph above).

It's important to note that a significant amount of coins are held on Bitcoin exchanges and that mere administrative decisions on their behalf can have a significant impact on measures like HODLer Net Position Change. However, serious effort has been made to de-anonymize exchange addresses, so future analysis should be able to mitigate for "exchange bias."

For example, one anomaly in the graph is the recent negative position change of meaningful Bitcoin savings (Dec 2018). While at first sight this is worrisome, we found evidence suggesting that a significant part of the move stems from Coinbase reshuffling around 5% of all BTC in circulation.

Another notable negative position change is the 278,000 BTC net move in August 2017. This is likely attributable to the Bitcoin Cash hard fork (BCH) of that same month. Every Bitcoin private key gave access to an equivalent amount of BCH as the BTC in that wallet. And so with BCH rallying strongly—at some point reaching over 20% of a BTC—Bitcoin HODLers were incentivized to split the two via on-chain transactions and either buy more BCH and sell their BTC, or vice versa. Given how strong the (flawed) narrative was at the time of BCH being "the real Bitcoin," it's conceivable that many old bitcoins were actually sold. More analysis is needed in this area.

Conclusion

By creating tools that measure changes in saving behavior on the Bitcoin settlement layer, we believe to have meaningfully contributed to the valuation debate. Relative Unrealized Profit/Loss in Bitcoin tells us about Mr. Market's emotional state, HODLer Net Position Change gives us information about how Bitcoin whales are moving their pieces on the chessboard, and Liveliness gives us a powerful tool to meaningfully compare long-term investor activity, as well as a platform for building new valuation measures in this space.

In a follow-up article we will share our take on what these and other measures tell us about Bitcoin's valuation today. Feel free to [contact us](#) with questions, or [sign up here](#) for future research updates.

Bitcoin's Incentive System or When The Stars Align

By Misir Mahmudov

Posted February 20, 2019



Time and time again, we realize that forcing people to do good or to change their behavior does not lead to meaningful results. Human beings are stubborn and don't want to change for various reasons. Most importantly, humans can be selfish and are not willing to alter themselves in any way unless there is a personal gain to be earned. On the other hand, incentivizing people to behave in a particular way by

rewarding them with something they value consistently produces the intended result.

Alignment of incentives is one of the most important phenomena that make up Bitcoin.

Incentives as a force behind Bitcoin's success

Apart from being a technological breakthrough, Bitcoin is a psychological and social phenomenon. Bitcoin takes human greed and turns it on its head. Bitcoin is fueled by human greed. Bitcoin uses human greed and the natural desire to better one's financial standing to ensure the integrity of the system.

Bitcoin is designed in a way that miners and holders are incentivized to behave in a way that is beneficial to Bitcoin. Any deviation from the optimal behavior on the part of the participants results in a reduction of possible profits. Bitcoin mining and the Proof of Work mechanism is perhaps the best representation of this. Bitcoin miners are incentivized to devote electricity to verify transactions and thus make the network secure and reliable. Their ability to perform this task is rewarded with miner reward (new bitcoins) and transaction fees. If, for example, a miner tried producing invalid blocks (blocks that break the consensus rules), full nodes would reject them and the miners would not be rewarded as a result. The full nodes are run by individuals as well as large processors (e.g. exchanges). These entities are incentivized to act optimally as their objective is a higher price per bitcoin (holders) and a functioning network to earn the fees (exchanges, custodians etc.) Many Bitcoin developers are employed by companies whose business models depend on Bitcoin continuing to grow. It is important to note that many of Bitcoin developers are, to a large extent, ideologically incentivized to contribute to Bitcoin. In his Bitcoin's Incentive Scheme and the Rational Individual, Hugo Nguyen explores the

relevance of philosophical alignment with regards to the cypherpunk ethos as an incentive for developers.

Incentives that propel Bitcoin also exist outside of the Bitcoin community itself. Given the fact that Bitcoin is neutral money (not affiliated to any particular country), it can be argued that countries, institutions and various authorities worldwide are in the long run disincentivized from banning and restricting Bitcoin's use and development. Given that Bitcoin is designed to exist and thrive in an adversarial environment, a particular country, say the United States, stands to lose by banning Bitcoin as developers, users and companies working and using Bitcoin (an industry at the forefront of technological and economic innovation) would relocate to a more accommodating jurisdiction. Given the tense relations and the international rivalry among the world's superpowers (US, China etc.) it is practically impossible to imagine all such countries cooperating together to dismantle Bitcoin (e.g. a multi-nation coordinated attack against Bitcoin mining). The fact that the US dollar has been the world's reserve currency for the last fifty years gives the United States an unfair advantage over other countries that depend on the US monetary policy. Many countries stand to gain from Bitcoin's adoption as it would remove their dependence on the US dollar and provide them with a feasible alternative. It is likely that as some nations start to adopt Bitcoin as their reserve currency, the aforementioned value proposition will become increasingly clear.

Importance of Financial Incentives

As already discussed, making people do good (or anything for that matter) by force does not work. Making people do something by incentivizing them, on the other hand, does usually work.

Thus, alignment of incentives is an integral part of what makes Bitcoin work. Bitcoin is an incentive system that rewards individuals for benefiting the world as a whole. Anyone who spends enough time studying Bitcoin will realize that it will have a considerable net positive effect on our society. Its numerous positive externalities markedly outweigh any associated costs. In fact, it is becoming increasingly evident that most of the criticisms towards Bitcoin ("wasteful" mining, "unfair" distribution etc.) are a result of ignorance rather than any substantive data-backed research.

Although the number of bitcoins is strictly limited, the global prosperity that Bitcoin brings about is the opposite of zero-sum. The average human is going to benefit from the adoption of Bitcoin even if they don't necessarily own any bitcoins throughout the process of monetization and don't directly profit from the increase in bitcoin's price. It is likely that these people will live in a world where they will be paid in bitcoin. This means that their wealth will be unseizable, sound and able to move anywhere in the world in a trustless manner.

Bitcoin as a mechanism for enabling positive change

All of us wish that the world was a better place and that people acted more compassionately. In theory, everyone usually wishes only the very best for the rest of the world, however, in practice, it doesn't always play out this way. Human greed stands in the

way of any decision, desired change or impact. We need to understand that, oftentimes, people forgo or give up on their moral beliefs and social responsibility in the face of personal financial difficulties. Most people are simply trying to get by and provide for their families. In the light of understanding this, it becomes more clear that expecting people to go out of their way to do something good is often counterintuitive and thus doesn't create sustainable results. Humanitarian and philanthropic efforts don't scale. They are often one time acts whose impact does not last. Similarly, redistribution schemes are too vulnerable. There are too many single points of failure which enable human greed to show itself and eventually cause the system to fail.

The biggest impact comes from aligned incentives that reward individuals for creating positive change in the world. Such systems are scalable. They work because they don't depend on finite sources of human compassion in the face of personal and financial difficulties. In fact, such systems work best because they are conducive to self-preservation. Nobody is good or bad, we are all human. We simply prioritize self-preservation over other things.

It is thus not logical to blame someone for having an X amount of bitcoin, or having bought bitcoin at a cheaper price and now becoming wealthy. Anyone who bought bitcoin at a cheaper price was rewarded for the higher relative risk that they took on when Bitcoin was a lot less robust. The economic incentives in Bitcoin were and are necessary to bootstrap a system that can level the financial playing field for the entirety of the world. To enable this, individuals needed to be incentivized.

You cannot expect people to change just by demanding them to be more compassionate. No matter how much you scream at someone telling them to donate their wealth or to give up their power, it won't happen, definitely not on a large scale. The only way to enable change is to create incentives for people. Unfortunately, when people demand corporations to be more humane, pay higher wages, institutions to be more accommodating, you see little change. The PR team launches a campaign and minimum effort is done only to maintain the brand image. Such methods don't create meaningful results as the incentives on an individual level are not aligned. They are one-sided. The individuals on one side stand to benefit while individuals on the other have to give up much of what they are already so used to.

Bitcoin is fundamentally different. Bitcoin has created a unique incentive system which caters to and encourages parties on both sides. Adoption of Bitcoin has the ability to benefit all the people on the individual level, no matter where they are in the socio-economic hierarchy. The very corporations and institutions that stand to lose from the adoption of Bitcoin are made up of individuals who stand to benefit massively from the adoption of Bitcoin.

Understanding that every entity, group or collective is made up of self-motivated individuals is key to understanding why Bitcoin will succeed.

Don't expect people to be good. Expect people to act in their own self-interest. If everybody acts in their self-interest in a system of rules that rewards good behavior, then good behavior emerges naturally.

Acknowledgements

Special thanks to Hugo Nguyen for his feedback.

Crypto Governance: The Startup vs. Nation-State

Approach

Jack Purdy

Posted February 25, 2019

Intro

Humans like to argue. It's in our nature.

Take any facet of human experience and you can find two people who disagree on it.

Nowhere is this more prevalent than in the realm of governance, where we argue who should have power, who gets to make changes to the system, and how decisions are ultimately made. Given the magnitude of the impact governance has, it is easy to see how this became a highly controversial topic.



Now imagine a nascent industry full of highly intelligent people with strong opinions (and egos), where most of the debate occurs on globally accessible platforms. As you can imagine, there is no shortage of debates especially as it pertains to governing this industry. Welcome to crypto.

Crypto governance encapsulates the debates around how we coordinate to make decisions on changing the rules of a protocol. This could include anything from simple upgrades to changing the consensus mechanism to allocating block rewards. It involves many stakeholder groups such as node operators, network providers (miners), core developers, users, speculators, exchanges, and block explorers to name a few. These are diverse groups with varying incentives that frequently conflict with each other. For example, node operators want to keep block size low to reduce the costs of running a full node, while miners have incentives to increase the block size so each block includes more transactions and thus more transaction fees.

It is the interactions between these stakeholder groups that define what a blockchain is, its values and principles and how it evolves over time. This governance process shapes the imagined reality we create surrounding a network, and the value of a cryptoasset lies at this social layer.

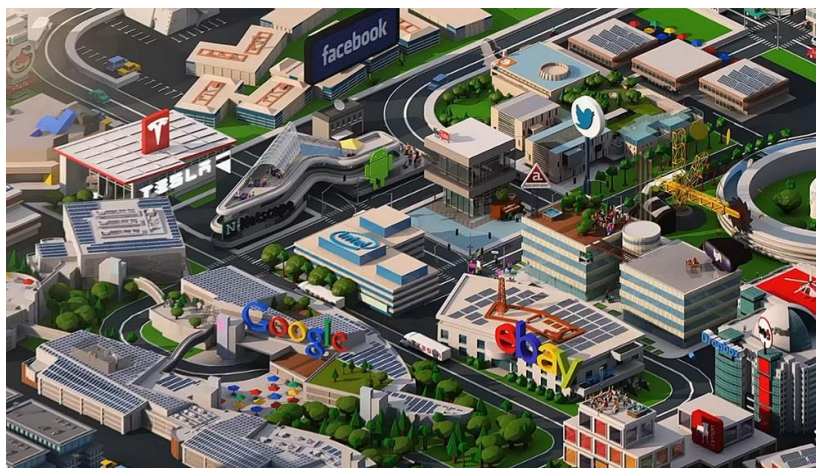
Unsurprisingly, there has been a substantial amount of debate on the right way to govern cryptonetworks, which has created various thought-provoking theories. I believe much of

the debate is misguided since 'crypto' is too general of a term to apply overarching ideas to. Jill Carlson explains it well:

Often investors attempt to apply the same priors and heuristics whether they are talking about bitcoin, petrocoin, or filecoin because they are all "crypto". This would be akin to applying the same fundamental analysis to gold markets, sanctioned Venezuelan debt markets, and the pre-IPO valuation of Dropbox circa 2008.

In the same way we shouldn't apply the same fundamental analysis for these assets, we shouldn't analyze the governance of all cryptoassets in the same manner. We need to more accurately describe what is being governed in order to think about how it should be governed. In this analysis I'm going to delineate between base layer protocols from those further up the tech stack. The former should be governed like an established nation, while the latter an early stage startup.

The Startup Approach



"Moving fast enables us to build more things and learn faster. However, as most companies grow, they slow down too much because they're more afraid of making mistakes than they are of losing opportunities by moving too slowly. We have a saying: 'Move fast and break things.' The idea is that if you never break anything, you're probably not moving

fast enough" — Mark Zuckerberg, IPO Prospectus 2012

Zuck encapsulates this governance theory in the now famous mantra of "move fast and break things". When you are looking at early-stage, user facing applications, you need to be responsive to customer needs. This requires the ability to rapidly iterate in order to meet these changing needs. If you move too fast and there is a bug, it is not the end of the world since there is not a tremendous amount of value in the network. You fix it and move on. The key is that the stakes are low so there aren't grave consequences if something goes wrong. Failure will not result in large personal losses or a complete loss in faith in the idea ever working again.

Now what will this governance look like in crypto? It will likely operate like a well-oiled autonomous organization. A good example of a cryptonetwork that caters to this style of governance is Decred. (Note: Given Decred is aiming to be used as money, I am somewhat skeptical if this model makes sense for them, but regardless it is a general model I believe can be effective for more rapid improvements). Decred utilizes on-chain voting to allow DCR holders to participate in the governance process by staking tokens in order to obtain

tickets. This lets stakeholders vote on matters such as how the treasury funds are spent to support development or whether consensus changes should be implemented via a hard fork. Placeholder summarized it best— "Decred's killer feature is good governance, and with good governance you can have any feature you want." This thinking enables the necessary innovation needed to keep up with consumer needs and avoid a slow descent into irrelevance.

"Move fast and break things" succeeded in turning Facebook from a scrappy startup to a unicorn, but once they reached scale and had data on 2 billion people, that mantra was no longer appropriate. With that many people at risk, breaking things is no longer the goal or even acceptable for that matter. Rather the goal should be keeping the system secure, and unfortunately Facebook failed at this exposing the data of millions.

This brings us to our next approach that starkly contrasts with that of the early startup.

The Nation-State Approach

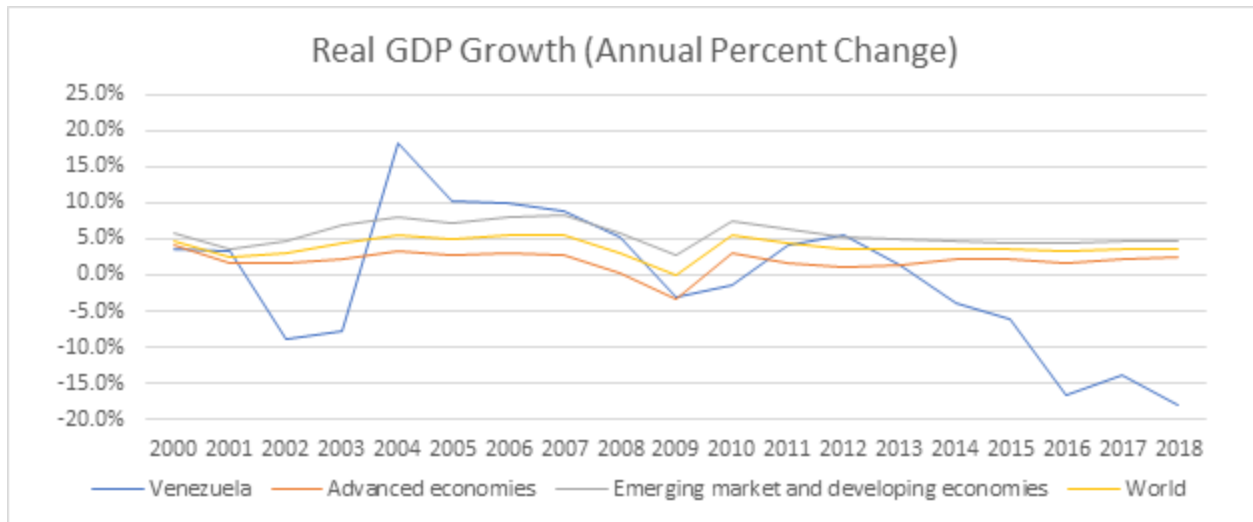
"We have to reinvent socialism. It can't be the kind of socialism that we saw in the Soviet Union, but it will emerge as we develop new systems that are built on cooperation, not competition." — Hugo Chavez to World Social Forum 2005

In January 2005, Hugo Chavez was embarking on a mission to re-shape Venezuela. That month he passed land reform allowing the



government to seize over 6 million acres of private property. Two years later the government took over the last privately run oil field, with the banks following shortly after. The drastic measures taken by no means stop there, and they continue to this day.

This example is not meant to make a political statement, but simply to demonstrate what can happen when a government attempts to make rapid changes that are unproven and largely experimental. This is a highly simplified illustration and there are a multitude of factors at play but that shouldn't distract from showing the risks of this type of governance. The results of these actions are widely known and evidenced by the graph below.



Source: IMF

When there are high stakes on the line to the underlying people, corporation, protocol etc. being governed, then the manner in which decisions and changes are made needs to optimize for the safety and security of those governed. No longer is the motive to innovate in order to outpace competitors because survival is the only way to win out.

Applying this to crypto, base layer protocols such as Bitcoin cannot afford to move fast at the detriment to security. When I refer to security here, I am talking about maintaining the well-being of bitcoin holders. This means not only ensuring the protocol doesn't break, but upholding the censorship resistance, trust-minimized features that keep these holders secure. A 10x improvement in transaction speed or fees is not worth a 1% decline in security. If a critical bug is exploited or a users funds confiscated, it will be incredibly difficult to regain people's trust in not just Bitcoin but the entire story they tell themselves surrounding a decentralized money. This is because technology such as Bitcoin is prone to the Lindy Effect, where the future life expectancy is proportional to its current age. Therefore, the longer it survives, the longer it is predicted to survive. If it fails, it not only starts from where it began but behind since its competitors (namely fiat) are now even more Lindy.

While it can be easy to get frustrated with the slow process to upgrade Bitcoin, it should be noted that extreme caution needs to be taken in changing base layer protocols where significant value rests on top. Valuable networks like Bitcoin need to be governed like national governments, where it is more important to reject unjust laws than to pass just laws. The more active governance is in a cryptonetwork, the more one requires trust to interact with it and the whole raison d'être of a decentralized currency is to minimize trust in others. Bitcoin developer Matt Corallo states:

Of Bitcoin's many properties, trustlessness, or the ability to use Bitcoin without trusting anything but the open-source software you run, is, by far, king. More specifically, interest in Bitcoin appears to almost exclusively derive from a desire to avoid needing to trust some third party or combination of third parties.

This applies to other base layer protocols where there are expected to be valuable dapps built on top of it. In the same way one would be hesitant to incorporate in a country where the laws governing its business are prone to change at anytime, one should be wary to build dapps on top of a protocol that requires trust that the rules won't change in a detrimental fashion. While this is not an apples to apples comparison, I believe it is useful in highlighting the fact that high stakes situations where there is considerable value on the line necessitate a more ossified governance structure to mitigate risk for the governed.

Conclusion

Often times in crypto, we like to believe we're reinventing the wheel. Accordingly we come up with unique heuristics and terminology to describe things. While in some cases this is true, often times we're simply repurposing age old ideas to fit this new paradigm. I believe governance is one of these areas where we can learn from a lot from the past. For thousands of years humans have been organizing themselves in different groups to coordinate around shared goals in the form of nation-states, corporations and others social groups. Over time we have improved our standard of living as a result of organizing ourselves into these groups and evolving new ways to govern them. However, innovation in this front has been slow due to the difficulty in testing out alternate approaches (rightfully so) because of the high stakes on the line.

This is a big part of why I am so fascinated with cryptonetworks. They provide us a sandbox to try inventive new ways to organize human behavior by shifting how we incentivize participants. By carefully studying the failures and successes of different crypto projects I believe we can learn more about governance and at a faster pace than has ever been possible. A great analogy is comparing them to petri dishes, where we can test out different ideas on smaller chains and based on the results begin to implement bits and pieces into more established chains.

This shouldn't be a black and white approach, but more of a spectrum based on the amount of value in the network and trust minimization required. On one end you have Bitcoin that needs to iterate slowly, preserving security at all costs and at the other you have experimental petri dishes that can test the efficacy of new models and look to incorporate them gradually down the tech stack as they grow stronger via the Lindy Effect.

To conclude, I believe instead of making overarching "laws" about crypto governance like Szabo's Law, we need to take a more nuanced approach. My hope here was to start separating the governance of mission critical base layer from protocols from more application specific crypto projects. I look forward to expanding my thoughts on the subject in order to further delineate the ways in which cryptonetworks should be governed.

Much of my thinking was influenced by prior work that includes:

- Bitcoin Governance
- The Crypto Governance Manifesto
- Blockchain Governance 101

- [Blockchain Communities and their Emergent Governance](#)
- [Blockchain Governance: Programming Our Future](#)
- [On Governance: Coordination, Layers, and Structural Integrity](#)
- [Cryptonetworks and Cities: Analogies](#)

Other works linked previously in the article

A Human Rights Activist's Response to Bitcoin Critics

By Alex Gladstein

Posted February 19, 2019



Bitcoin: a tool of freedom and human rights.

Foreign Policy recently published the latest mainstream media attack on Bitcoin from the London-based author and journalist David Gerard. Gerard's "Forget Bitcoin, Try your Mattress" is the newest in a long line of Bitcoin criticism published everywhere from the Financial Times to The Washington Post. This time, Bitcoin is part of a system "plagued by hacks, fraud, and social engineering." Doesn't sound very appealing, does it? Why, might you ask, would a human rights activist like me be interested in something so universally derided by experts and the world establishment?

This response is my answer. If you read along, we'll cover where the critics are right; why Bitcoin is secure and safe; how it does things that we can't do with our existing financial system; how it will scale and improve; why its monetary system is an improvement for many; why it's not a waste of energy; why progressives and libertarians should both be

fans; why it matters for human rights; how we are at just the beginning of the Bitcoin journey; and why now is the best time to learn more and get involved.

This essay is written from the point of view of someone who believes that mainstream Bitcoin critics don't actually understand how it works (meaning: haven't done their homework and couldn't pass a basic quiz on topics like mining, wallets, or nodes) and are fulfilling the historical role of skeptics of a new technology early in its life cycle. There are two main varieties of Bitcoin critics: establishmentarians like Martin Wolf who write from a place of fear, who don't want to see the existing financial system disrupted; and progressives like Gerard who write from a place of disbelief, who don't believe decentralized money (Bitcoin) could actually improve the world just like decentralized government (democracy) and decentralized knowledge (the Internet).

Bitcoin critics do get many things right, as Gerard does in his Foreign Policy article. Too many actors in the cryptocurrency and blockchain space are actually charlatans or thieves; there is a huge amount of snake oil and hype; and many crypto exchanges are unsafe and wind up being hacked. The sad reality is that with the exception of a few valuable efforts like Monero, ZCash, and MakerDAO (whose teams and core values and driving missions of private money and censorship-resistant stable assets are critical even if they fail), most crypto projects are either intentional scams, unexciting modifications to existing technology, or wolves in sheep's clothing — centralized systems which pretend to be decentralized but still have backdoors. The big mistake of the critics, however, is to conflate this entire mess of an industry with Bitcoin, which, despite what Gerard and friends would have you believe, is the most secure form of money on the planet and our first line of defense against the looming threat of mass social engineering and digital authoritarianism.

Gerard's core Bitcoin critique centers on the Quadriga crisis, where \$135 million of cryptocurrency was recently lost when the owner of an exchange died. While right to be alarmed about individuals losing huge sums of money, here is where Gerard makes a puzzling conflation. Losing your bitcoin when it is controlled by someone else (in the Quadriga case, a sketchy company run entirely by one person) is like losing your money when thieves hack your bank account, or losing your jewelry if someone breaks into your security deposit box. In these cases, the security model of your bank is the problem, not the type of assets you own. And Bitcoin is no more responsible for the failure of a crypto exchange than the Internet is responsible for the failure of the latest web startup— and yet this line of attack is one that so many critics take when they try to blame scandals like Quadriga on Bitcoin and fool you into thinking that the project is one big scam.

The community mantra “not your keys, not your Bitcoin” is a constant reminder that you shouldn't allow someone else to control your bitcoin. And Gerard even shares this phrase with his readers, but doesn't seem to appreciate the meaning. Users can have complete financial sovereignty over their bitcoin, which is secured by public key cryptography. Simply put, if you don't have my private key (think: password), you can't steal or spend my bitcoin. This goes for thieves as well as giant companies or even world powers like the Chinese or American governments. No other form of money can boast this kind of security. In the title of his article, Gerard suggests that hiding money in your mattress

would be safer. This is a bizarre argument to make when today you could instead store any amount of Bitcoin on a tiny USB stick or even a brain wallet, where you can memorize a back-up phrase to your assets and cross borders with a billion dollars in your head.

Gerard asks, what use is there for a money where you have to control your own password? Think about that for a second. He's telling you that the only form of digital money that could possibly be useful is one where you have to rely on a third party. Human rights advocates should be wary of this kind of corporate mindset. Consider what is happening right now in China where the Communist Party has loaded nearly the entire population onto systems like WeChat or Alipay where they not only exert easy surveillance and control over your money and payments, but also steer you with powerful incentives and disincentives as part of the largest social engineering project in human history. Control over our data and money will be an increasingly important part of keeping the Internet and our societies free and open as we enter the age of mass surveillance and the cashless world.

While it's true that you probably need to spend days or even weeks (think: a bootcamp or crash course) learning how to use Bitcoin before you can use it safely and properly, the fact is that this knowledge is available to anyone in the world, online, for free. If you would like to sacrifice the opportunity to personally control your bitcoin for convenience, and you opt to use a third party to store your bitcoin, then you can make that decision. But anyone now can choose to be their own bank: a game-changer for the billions of people who don't control their own money. This is especially relevant outside of the advanced economies where nearly all professional Bitcoin critics live.

Gerard claims that Bitcoin takes us to the past, where you could "lose your savings if your banker ran off with your money." The sad part is, this is not the past but the dire present for people living in countries ranging from Iran to Zimbabwe to Venezuela, where governments recklessly print fiat currency, stealing from the hard-earned savings of the average person. In other places, including China, Saudi Arabia, and Russia, the government exerts total dictatorial control over the banking system. Meaning: your banker can and often does run off with your money, whenever he wants. This is even true to an extent in advanced economies, where the value of the dollar (inflated to pay for, among other things, global wars) has plummeted over the last few decades against other assets like oil and gold. Bitcoin doesn't take us backwards, but instead into the future into a world where it will be much more difficult for governments and companies to control us.

As far as Bitcoin's value proposition, one can certainly say that after its first decade, it's still a nascent technology, with a long way to go. It is not as private, fast, accessible, or approachable as it could and will be. But it's a considerable improvement already on at least one key function of our society — the wire or ACH. Bitcoin is a big upgrade here, where, for the first time, one can send money to someone else across the globe within minutes and without worry. Compare this to the existing model, where after sending a wire, we sometimes have to wait days, pay big fees to third parties, and even wonder if the transaction will go through.

Contrary to what the critics would have you believe with all of their scary language about fraud and risk, when I send an on-chain Bitcoin transaction to you, it will get to you, no matter what. There is no point of censorship, seizure, or control. Critics like to paint Bitcoin as a broken system, but actually, unlike Visa or MasterCard, which do “break” and go down from time to time, your access to Bitcoin can't be broken or censored, even if your government shuts down the internet. One of the most exciting developments in Bitcoin recently is the rise of satellite, mesh networking, and even radio infrastructure. Whether with a small satellite device, or even over radio waves, you can send and receive bitcoin from anywhere on earth, and beyond. And people are catching on. Already today, it is estimated that at least \$6 trillion dollars moved across the Bitcoin network in 2018 — \$3.2 trillion over exchanges, and two to three times that amount via OTC transfers. Compare that to \$62 billion for Venmo, or \$8 trillion for Visa.*

Gerard says that the Bitcoin protocol is “incredibly slow, anti-efficient, and hard to scale up.” What he may not realize is that these are features, not bugs. Bitcoin's architects and ongoing community made an engineering trade off at the base layer, choosing security and censorship-resistance over speed. The good news is that there are second layer technologies that people are building today that will allow large numbers of bitcoin transactions to be batched together, potentially allowing bitcoin to surpass our current financial system by orders of magnitude when it comes to speed and scaling.

Gerard actually mentions one of these technologies — the Lightning Network — but calls it a “toy” that is “already centralized.” I would offer an alternative definition. Simply put, Lightning will allow hundreds, thousands, or, one day, millions of payments to get batched together into one transaction on the underlying blockchain. Lightning payments are globally instantaneous (watch this demonstration done by CoinCenter in U.S. Congress) and, in good news for privacy advocates, protected by onion routing, a robust encryption technology. So while today, with enough resources, a government can surveil bitcoin transactions by analyzing the blockchain, and potentially hunt down dissidents, doing so on Lightning will be much more difficult, as payments will occur off-chain, routed in a way where the owners of the network's payment hubs don't know the origin or final destination of the payments which pass through them. As for whether or not Lightning is centralized, the answer is easy. It's not. There is no single point of failure. You may have heard about Lightning in the news lately as Twitter and Square CEO Jack Dorsey has said it is a matter of when, not if, Square will implement the network into its popular Cash App. This is an exciting step in the right direction for advocates of privacy and human rights.

Gerard also attacks Bitcoin for having a limited supply cap. Meaning: there won't be more than 21 million Bitcoin, ever, and more than 17 million are already in circulation, with the rest to be slowly released as rewards for those who provide network security over the next 120 years. This means Bitcoin is a deflationary system, with a transparent and known monetary policy, where no dictator or CEO can decide to print more and devalue everyone else's money. Bitcoin's anonymous creator, Satoshi Nakamoto, was quite clear that Bitcoin was supposed to be an alternative to central banking and absolute government control of money, even inserting a critique of quantitative easing into the first “genesis” block of the Bitcoin blockchain to prove the point. And what's wrong with that? Monopolized control of money may seem “normal” to you today, but in reality, the practice causes misery for

billions of people around the world who are caught under hyperinflation, currency crises, financial surveillance, sanctions, and capital controls. It also makes it easy for governments to print money to go to war and commit violence. We can do better.

Not wanting to miss the most common line of attack against Bitcoin, Gerard mentions that it's a waste of energy. But here he, and all the rest of the critics who blindly repeat an argument sourced mainly from [a non-expert's blog](#), are missing the big picture. Today, more than 75% of Bitcoin's energy usage is estimated to come from renewable resources, a number projected to only increase into the future. Nearly half of all mining is done in a part of China where power is almost exclusively hydroelectric. So while yes, Bitcoin does use a lot of energy — in the same way, as Saifedean Ammous has pointed out, that the car uses more energy than the horse carriage, and the refrigerator more than an ice bucket, and a washing machine more than arduous hand labor, and a modern hospital more than a medieval field tent — it is already unlocking new sources of hydro, geothermal, solar, and wind power that go otherwise unused or unreachable, hopefully helping us toward the end of the hydrocarbon age.

Gerard characterizes Bitcoin as a project promoting "libertarianism." While it's certainly true that you can have a libertarian appreciation for Bitcoin, given that it gives one financial sovereignty and liberates you from government control, one can also have a progressive appreciation. In my view, Bitcoin is a similar phenomenon to democracy and the Internet, technologies which respectively smashed the tyranny of political power and corporate control of knowledge. Through democracy, citizens are able to check the power of kings and dictators, and through the internet, citizens outside of the government and the richest classes are now able to have a strong public voice and have unfettered access to all of the world's knowledge. In the same way, Bitcoin will break the government and corporate monopoly on money. In 100 years, humans will likely look back at today and see a time when a small handful of elites controlled money as a backwards idea, just like the idea of political tyranny or state-controlled news.

Gerard saves his favorite argument for last, that bitcoin is a shadowy network that will surely be used by criminals and drug dealers. But remember, the same types of fear-based arguments were made by kings and elites and dictators when the people demanded that they step down and share power, or by big telephone companies and news organizations and propaganda regimes at the dawn of the internet. But instead of bringing instability and terror and crime to our societies, democracy has empowered half our world and sparked historic advances in innovation, prosperity, peace, and social welfare. And instead of becoming a criminal domain, the Internet has put the sum of human knowledge into anyone's hand, giving a global megaphone to investigative journalists and a world encyclopedia to aspiring students. And while Gerard tries to tie Bitcoin to evil doers, he fails to mention that virtually all financial crime and drug trafficking is committed inside the existing "official" financial system, where trillions of dollars of corruption occur, aided and abetted by banks like HSBC and Wells Fargo. Watch ["Escaping the Global Banking Cartel,"](#) a stand-out talk by Andreas Antonopoulos, and you'll learn more about why Bitcoin is a way out of our current system, which is exclusionary and unjust, and tends to prey on the weak and disenfranchised while letting the corrupt Davos crowd walk free.

In fact, for all of his do-gooder, consumer protection positioning, Gerard misses the key human rights aspects of bitcoin completely. Whether you are trapped under centralized payment schemes like WeChat used to microtrack your lives, or whether your newspaper's bank account has been frozen by a dictator, or whether the US government has unfairly put broad sanctions on your country, punishing you for crimes your rulers committed — Bitcoin is a way out. The greatest potential that Bitcoin has is to help the most vulnerable on this planet, those without bank accounts, identities, or access to the financial system. Now, with just a phone and an internet connection, anyone can receive bitcoin from anyone else in the world, in minutes, for a small fee, with no possibility of censorship or seizure, without needing to ask permission from anyone, and without needing to prove an identity.

In the coming years, as infrastructure and local liquidity and exchange points grow, Bitcoin will have a major impact on foreign and humanitarian aid. Individuals, charities, and democratic governments will no longer need to comply or even deal with the dictators who rule over most of the world's poorest people. As Coinbase realizes with its GiveCrypto program, we'll be able to side-step this old infrastructure completely and transact with aid recipients directly. We can already analyze local exchange data to see that despite Bitcoin's declining price in the past year, usage has increased in authoritarian societies like Belarus, Venezuela, Kazakhstan, and Egypt.

Perhaps the most shocking thing about Bitcoin is that so few know about it. 10 years since the project began, it is estimated that less than 1% of the global population has ever interacted with Bitcoin. Unlike the modern financial system, which is run by a kind of aristocracy, and only permits selective access, Bitcoin is completely open to everyone. It cannot discriminate. Literally anyone can use free online tools to learn how Bitcoin works, send and receive bitcoin, and even learn to code and contribute to the Bitcoin software itself, helping to steer the direction of the future economy. Here's the best part: you don't need to go to Harvard or be a VC in Silicon Valley or have a thirty-year career in economics or central banking to help lead the next financial revolution.

Most world-changing technologies are dismissed by the crowd at first. Consider the telephone, which no one wanted to buy; the car, which surely couldn't work on our horse roads; the plane, which couldn't possibly be safe; or the internet, which was destined to fail. Remember the words of Paul Krugman who said that "by 2005, it will become clear that the Internet's impact on the economy has been no greater than the fax machine." Any fundamental technology, from the fridge to the credit card, follows an adoption S-curve, and at the beginning of the S, there are always plenty of luddites and skeptics. Eventually, the curve goes exponential and the technology spreads throughout humanity. It's hard to imagine a more fair or democratic idea than the fact that anyone today — regardless of their location, gender, language, age, level of education, or wealth — can get meaningfully involved at the ground level of Bitcoin, an exponential technology that is still at the bottom of its adoption S-curve. The only thing stopping you, is you.

Perhaps it's too much for Gerard to grasp this, as he writes from the cozy confines of London. But whether it's in the Philippines, Nigeria, Turkey, Venezuela, or Palestine, there

are people who don't have his rights, freedoms, and trust in their financial system. And they are increasingly using Bitcoin, the most secure and sovereign form of money on earth.

Thanks to Dan Held and Misir Mahmudov for their feedback.

**Coinmetrics has more conservative data, stating that \$2.16 trillion was moved across the network in 2018, with \$601 billion in "meaningful volume."*

Cryptosovereignty

By Erik Cason

Posted February 3, 2019



The sovereign power of cryptography in the digital age

"[We will not find a solution to political problems in cryptography] Yes, but we can win a major battle in the arms race and *gain a new territory of freedom for several years*. Governments are good at cutting off the heads of a centrally controlled networks like Napster, but pure P2P networks like Gnutella and Tor seem to be holding their own." – Satoshi Nakamoto

This is one of the few political comments that we are offered from Satoshi Nakamoto, the unknown developer of Bitcoin. This quote of Satoshi's seems to be referencing a famous political quote from Michel Foucault on the nature of sovereign power, and how it functions. Here is the full quote:

Sovereign, law and prohibition formed a system of representation of power which was extended during the subsequent era by the theories of right: political theory has never ceased to be obsessed with the person of the sovereign. Such theories still continue today to busy themselves with the problem of sovereignty. 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. –Michel Foucault

Satoshi saw that cypherpunks had a political philosophy that was rooted in anarchism and did not rely on traditional sovereignty, law, or prohibition to create systems of power. Instead, cypherpunks wrote code, used cryptography, and built systems that did not need the same physical force or permissions that all contemporary law needs in order to consummate the power of their legal systems. Through expropriating cryptographic tools from being highly coveted military secrets, and tools of war, and hacking them into tools of personal freedom and economic liberty that anyone can use; the cypherpunks introduced a new form of sovereignty into the world: Cryptosovereignty.

Cryptosovereignty is the fulfillment of what was wrote in the Declaration of Independence of Cyberspace more than twenty years ago:

"You [governments] have no sovereignty where we gather. We have no elected government, nor are we likely to have one... I declare the global social space we are building to be naturally independent of the tyrannies you seek to impose on us. You have no moral right to rule us nor do you possess any methods of enforcement we have true reason to fear." — John Perry Barlow, *A Declaration of Independence of Cyberspace*

Cryptosovereignty is the personal power, economic liberty, and political praxis that exist in bitcoin directly, crypto assets generally, and the internet widely. It is the power of any single human—no matter their station of birth, class of wealth, or creed of faith—to choose to put their economic, social, and political rights into a new digital commonwealth that is inviolable and beyond the power of any and all governments to violate. The code alone is sovereign. There is no exception.

"If revolutions and insurrections correspond to constituent power, that is, a violence that establishes and constitutes the new law, in order to think a destituent power *we have to imagine completely other strategies, whose definition is the task of the coming politics*. A power that was only just overthrown by violence will rise again in another form, in the incessant, inevitable dialectic between constituent power and constituted power, violence which makes the law and violence that preserves it." — *Giorgio Agamben*

By engaging in a totally different strategy of 'law' which completely abandons authority, prohibition, and most importantly, violence; crypto creates a totally new form of social contract through cryptosovereignty. Crypto inverts the dictum of sovereign power as surmised in Hobbes' De Cive is "Auctoritas, non veritas facit legem [authority, not truth makes legitimacy]" _into "Veritas, non auctoritas facit legem [Truth, not authority makes legitimacy]." _By refusing the power of authority, in exchange for having truth bear legitimacy through cryptography; a new system of power is born.

"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*

We people of the world and first citizens of the internet recognize our position in the struggle against global fascism and the perpetual emergency that we live in. We understand the history of those who have touched bottom and the "emergency" that always justifies the Other's economic expropriation, social marginalization, and ultimately biological liquidation.

We understand that in a world lost to the corruption and avarice of politicians and profitters alike; the most powerful tool at our disposal is our economic power. The ability to choose to allocate our wealth in the commons of crypto is the real state of emergency—it alone can break the whole perverse system of corrupted power that we call law. Only in a system of totalitarian economic and social control would taking back control of one's wealth and privacy become a revolutionary act.

We understand that through depriving the state and its banking allies of their life-blood — the control of money and power of the gaze — we are introducing the real state of emergency; the general strike on their blood money called fiat. This is a concept of history that understands the greatest robberies ever preformed were done under the watchful eyes of the state and the bludgeons of their minions. By refusing to participate in the disgusting corrupt system of fiat money, broken justice, and social monitoring; and choosing to put our wealth into cryptosystems beyond their power; we have learned that our most potent form of political power is economic power.

The goal of crypto is not to create a new form of sovereignty, law, and prohibition only for us to go through another oscillation of law-destroying, and law-creating violence. The goal is to fundamentally disengage traditional forms of sovereign power, law, and the violence they must always contain, in order to create something better and more fitting for our times. With crypto the sovereign decision becomes the individuals choice alone. The code guarantees and assures itself through cryptographic proofs, which alone makes it sovereign. There are no exceptions.

"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*

Through banishing the power of physical force from having anything to do with contractual enforcement of 'law' within blockchain systems, crypto totally disengages from traditional forms of sovereignty, law, and prohibition. Crypto creates a novel, new form of sovereignty through cryptographic systems which do not need any form of physical force to support them — just the code alone. This causes for traditional systems of sovereign power to unravel against crypto, as they cannot find a foothold from which they can execute their physical power. Cryptosovereignty is the newfound ability for any single human to choose to put their economic, social, and political power into a new crypto-commonwealth where the rules of the system can never be broken or violated; unlike all forms of contemporary sovereign law. Cryptosovereignty is the newly formed political power that each and every human has to refuse the transgressions and violations of state powers, and to choose to abandon these antiquated systems to create something better together using crypto.

"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, *State of Exception*

Disclaimer:

WORDS

Please note that this Journal is provided on the basis that the person who is reading it accepts the following conditions relating to the provision of the same (including on behalf of their respective organization). This Journal does not contain or purport to be, financial promotion(s) of any kind.

This Journal does not contain reference to any of the investment products or services currently offered by the operator of the journal, that means any business I am associated with. Bitcoin, shitcoins, and related technologies can be volatile. Don't buy what you can't afford to lose and please do your own research.

Bitcoin has paved the way for some VERY radical technology AND it's very confusing. Read more. Ask questions. The purpose of this Journal is to provide archive and curate the best commentary and culture in the bitcoin space.

Nothing within this Journal constitutes investment, legal, tax or other advice. This Journal should not be used as the basis for any investment decisions which a reader may be considering. Any potential investor in bitcoin or shitcoins, even if experienced and affluent, is strongly recommended to seek independent financial advice upon the merits of the same in the context of their own unique circumstances.

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

DYOR | BTFD | HODL



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

- @_joerodgers