The Complete Carter

A collection of Bitcoin writings from Nic Carter.

Contents

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 related to Bitcoin. 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 related to Bitcoin. 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.

Support WORDS

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 typically link to content and other things regarding development of this site.

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

Twitter

Subscribe to the newsletter

The journal is published monthly and is distributed via Twitter and 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.

Subscribe

Our pledge

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

Foreword

This is a collection of writings by Nic Carter as of June 4, 2020. Nic has contributed an invaluable collection of writings to Bitcoin. His writings are often referenced by Bitcoiners and are helping to shape narrative around this revolutionary social phenomenon.

Future versions and changelog will be listed below.

Visions of Bitcoin

How major Bitcoin narratives changed over time

By Nic Carter & Hasu

Posted July 29, 2018

Do I contradict myself? Very well then, I contradict myself I am large, I contain multitudes.

- Walt Whitman, *Song of Myself*

Perhaps the most enduring source of conflict within the Bitcoin community derives from incompatible visions of what Bitcoin is and should become. Businesses building on Bitcoin, believing it a cheap global payments network, eventually became nonviable when blocks filled up in 2017. They weren't necessarily *wrong*, they just had a vision of the world that ended up being a minority view within the Bitcoin community, and was ultimately not expressed by the protocol on their desired timeline.

In the absence of a recognized sole leader, Bitcoiners refer to founding documents and early forum posts to attempt to decipher what Satoshi truly wanted for the currency. This is not unlike US Supreme Court justices poring over the Constitution and applying its ancient wisdom to contemporary cases. Others reject textual exegesis and focus instead on a pragmatic analysis in context.

Conflicts within Bitcoin thus arise from entities who hold visions of the protocol that are mutually exclusive—and this leads to friction when these visions cannot be reconciled. Visions of Bitcoin are not static. Technological developments, practical realities and real-world events have shaped collective views. This post is an attempt to aggregate the various dominant narratives that have characterized Bitcoin throughout its 9-year history. This post builds on excellent prior work by Murad Mahmudov and Adam Taché, and we suggest you add that to your reading list.

Changing narratives

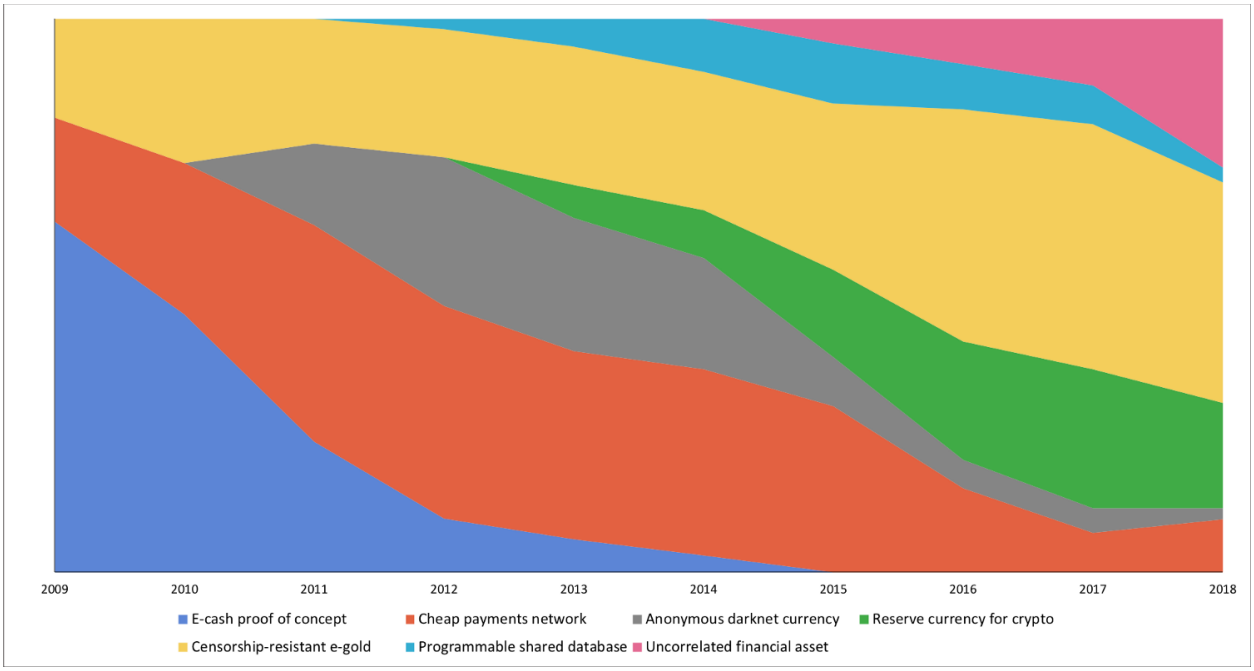
Here, we want to more granularly explore the prevalence of key narratives. We identify seven distinct major themes that have held positions of prominence among Bitcoiners throughout its history. Note that these do not necessarily have to be the *most* influential narratives—we are instead focusing on *major strains of thought* that have characterized Bitcoin users.

In rough order of appearance, these are:

1. **E-cash proof of concept**: the first major narrative, this was the general view of Bitcoin in its earliest days. Back then, cypherpunks and cryptographers were still appraising the nascent project and determining whether it worked, if at all. Since all prior e-cash schemes had failed, it took a while for people to be convinced of its technical and economic viability and move on to more expansive conceptions of the protocol.

2. **Cheap p2p payments network**: an extremely popular and pervasive narrative. Some believe this is what Satoshi had in mind — a straightforward currency for peer to peer internet transactions. A decentralized Paypal or Venmo, if you will. Since microtransactions are a key component of internet commerce, proponents of this view generally believe that low fees and convenience are an essential characteristic of such a currency.
3. **Censorship-resistant digital gold**: the counterpoint to the p2p payments narrative, this is the view that Bitcoin primarily represents an untamperable, uninflatable, largely unseizable, intergenerational wealth store which cannot be interfered with by banks or the State. Proponents of this view de-emphasize Bitcoin's use for everyday transactions, arguing that security, predictability, and conservatism in development are more important. We're callously lumping in sound money believers into this camp.
4. **Private and anonymous darknet currency**: the view that Bitcoin is useful for anonymous online transactions, in particular to facilitate black market online commerce. This is not necessarily mutually exclusive with the e-gold position, as many proponents of the digital gold view believe that fungibility and privacy are important attributes. This was a popular narrative before the chain analysis companies had success de-anonymizing Bitcoin users.
5. **Reserve currency for the cryptocurrency industry**: this is the view that Bitcoin serves an essential purpose as the native currency for the cryptocurrency/cryptoasset industry more generally. This is a view espoused by traders for whom BTC is the numeraire — the currency in which the prices of other assets are quoted. Additionally, traders, businesses, and distributed networks that hold reserves in BTC de-facto endorse this view.
6. **Programmable shared database**: this is a slightly more niche view, and generally involves the understanding that Bitcoin can embed arbitrary data, not just currency transactions. Individuals holding this view tend to see Bitcoin as a programmable, expressive protocol, which can facilitate broader use-cases. In 2015–16, it was popular to express the notion that Bitcoin would eventually absorb a diverse set of functionalities through sidechains. Projects like Namecoin, Blockstack, DeOS, Rootstock, and some of the timestamping services rely on this view of the protocol.
7. **Uncorrelated financial asset**: this is a view of Bitcoin that treats it strictly like a financial asset and finds its most important feature to be its return distribution. In particular, its tendency to have a low or nonexistent correlation to all manner of indexes, currencies, or commodities makes it an attractive portfolio diversifier. Proponents of the view are generally not too concerned about owning spot Bitcoin; they are interested in exposure to the asset. Put another way, they want to buy Bitcoin-flavored risk, not necessarily Bitcoin itself. As Bitcoin has become more financialized, this conception has gained steam.

In the chart below, we've weighted these various narratives according to their popularity at the time.



This isn't modern art — it's our representation of Bitcoin's changing tides

(High-quality version here)

In this chart, we lay out the relative influence of the seven narratives we identified above. As you can see, the e-cash proof of concept was the dominant view at the start, although the p2p payments network and digital gold views were also espoused at the time. Later, Bitcoin as an anonymous darknet currency gained steam with the Silk Road. The idea never really died off, and Bitcoin is still used on the darknet today, even though other privacy-oriented alternatives exist.

As ICOs were invented and a broader market of altcoins began to proliferate, BTC became the reserve asset for that larger economy. This grew to become a significant feature of Bitcoin, especially in the bull markets of 2014 and 2017. We note that the p2p payments contingent remained influential until mid 2017, when they largely migrated to Bitcoin Cash (some had already left for Litecoin and Dash). However, with the emergence of Lightning in 2018, there has been an upswing of enthusiasm for online microtransactions and fee-less internet payments.

In 2015 and 2016, sidechains became a popular talking point, and it was assumed that Bitcoin would soon boast a much-expanded functionality, obsoleting most altcoins. Related functionality-extending projects like Mastercoin (now Omni), colored coins, Namecoin, Rootstock, Blockstack, and Open Timestamps, contributed to this general view. However, as sidechains proved complicated to implement, non-money uses of Bitcoin fell out of favor.

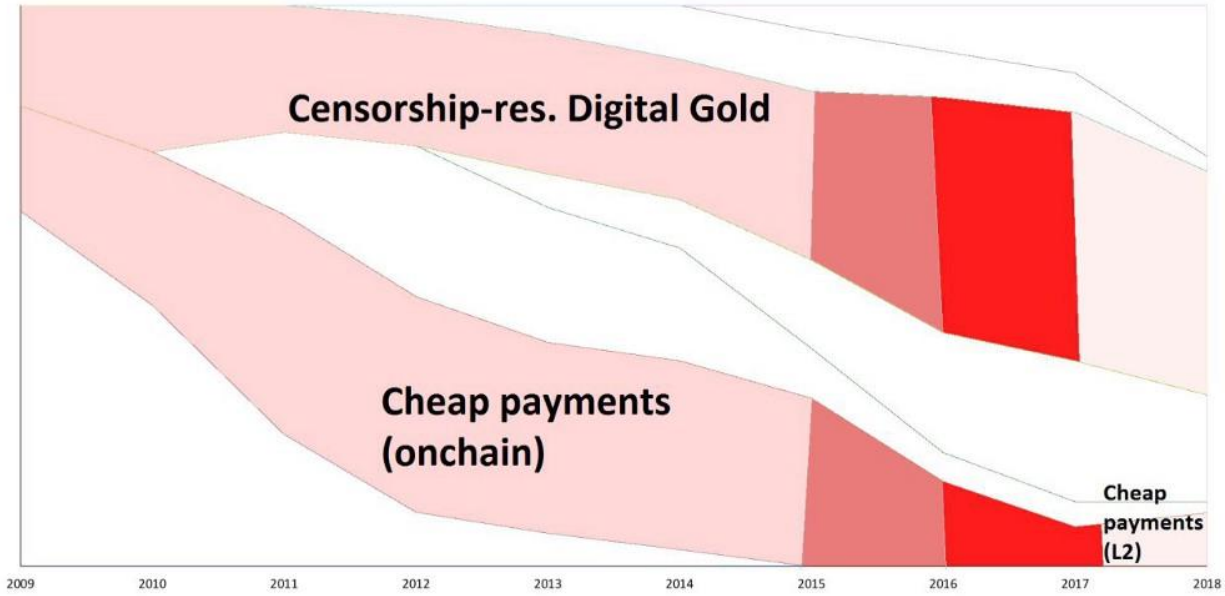
As Bitcoin emerged from the 2014–15 bear market, analysts began to contemplate its status as a differentiated commodity-money. In November 2015, Tuur Demeester published an investment note entitled "How to Position for the Rally in Bitcoin," arguing that it had unique characteristics as a portfolio asset. In mid-2016, Burniske and White influentially argued that Bitcoin represented an entirely new asset class. These analysts noticed Bitcoin's stubbornly low correlations with traditional assets, and as this

persisted, Bitcoin as a portfolio diversifier gained steam among certain forward-looking corners of the asset management industry. Today this is a popular view, driving much of the demand for financial products which would give traditional investors exposure to Bitcoin.

Throughout all these regimes, the digital gold conception has remained influential, and now is the consensus view, predominating over the p2p petty cash faction, which largely departed with Bitcoin Cash. Today, after years of strife and infighting, this is the majority view. However, not all Bitcoin users are ideological bitcoiners, and wanted to reflect this in the chart. Many Bitcoin holders hold it as a portfolio diversifier, some still use it for anonymous darknet transactions, and the p2p cash contingent has re-emerged alongside Lightning.

Tension and release

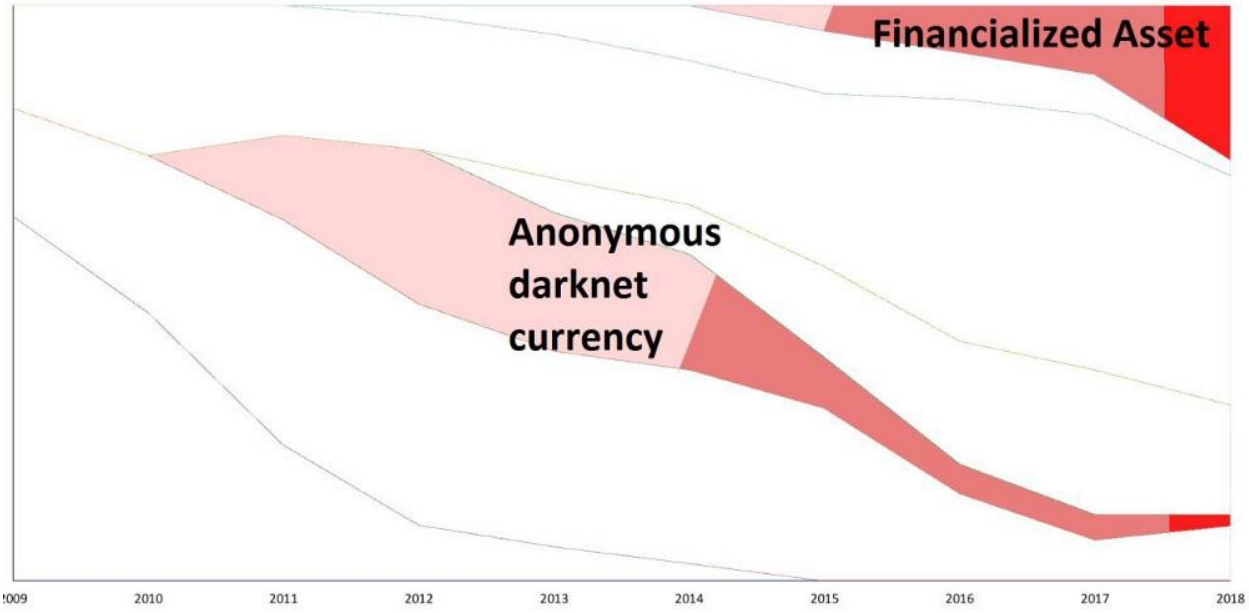
If you scrutinize the above chart, you'll notice that some of the visions of Bitcoin are entirely incompatible. For instance, a move to a global on-chain payments network conflicts with the digital gold view, as emphasized by Spencer Bogart. We've depicted the conflict between these views of the world by isolating them on this chart.



The conflict really began to be fought seriously with the release of BitcoinXT in 2015, although rancorous discussions had long preceded that. Further provocations including Bitcoin Classic, Unlimited intensified the conflict. It reached its peak in mid 2017 when Bitcoin Cash finally forked. During the bull run of late 2017, Bitcoin fees reached extreme levels, leading to defections to the Bitcoin Cash camp. However, since then, fees have settled down and the need for big blocks appears less urgent.

Additionally, in early 2018, Lightning implementations became viable, and micropayments with Bitcoin emerged. Thus, the tension dissipated, as both camps were able to pursue their own objectives. We noted an uptick in the cheap payments school of thought from within the Bitcoin crowd in 2018, as there has been a resurgence of optimism for payments through second-layer solutions.

An interesting conclusion that we think can be drawn from the analysis is that Bitcoin is currently benefiting from a rare period of relative harmony. While there is no single view that entirely dominates, the digital gold narrative is certainly most prevalent right now. The civil wars of 2015–17 ended with the Bitcoin Cash fork, and migrations to other p2p payment factions like Litecoin, Dash, and Nano. For now, the tension seems to be largely resolved, and we find ourselves in an unusually placid era in Bitcoin's history. Subjectively, it appears that under this comparatively peaceful regime, development seems to be progressing more rapidly. Endless social media battles, conference-driven agreements, and positioning for contention forks certainly created a drag on developer efforts. There is another battle looming, however.



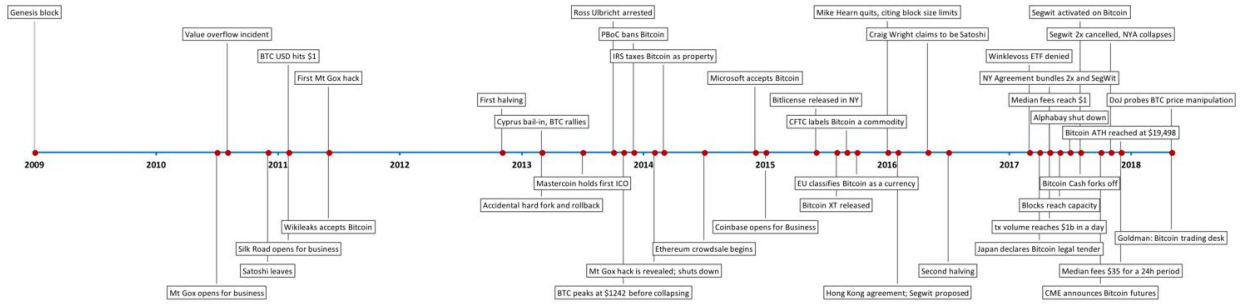
As depicted in this chart, the anonymous and fungible vision of Bitcoin (generally preferred by the digital gold camp) is somewhat at odds with the financialised, transparent version which is growing in popularity. Individuals that want exposure to Bitcoin the financial asset tend to prefer a Bitcoin which is compatible with AML/KYC and tend to put a lesser emphasis on privacy or fungibility. Many pundits believe this will be the next bitter fight for the soul of Bitcoin.

Ultimately, both the conflict and the peacetime phases are important. Conflicts reveal where power structures reside, and tend to yield informative signals about how key stakeholders truly feel. Under duress, business, individuals, and developers are forced to take sides, revealing their genuine preferences for the development of the protocol.

Timeline of events

We are aware that much of our analysis relies on our subjective interpretation of old BitcoinTalk posts. If you disagree, we welcome you to suggest an alternative. To make subsequent analyses easier, we've put together a timeline of key Bitcoin events, tracking its entire history. (We drew heavily on the 99bitcoins annotated price chart to make this.) We recommend considering our colorful 'changing tides' chart

alongside the below timeline. The juxtaposition should help elucidate why exactly we made the decisions that we did.



(High quality version here)

Conclusion

We put together the changing narratives chart through an analysis of BitcoinTalk posts, a set of discussions with Bitcoiners who had been there from the very start, a healthy respect for Bitcoin history, and a recollection of major attitudes over the years. Anyone who has been around Bitcoin long enough should be able to perform a similar analysis.

We're not positing our analysis as the absolute truth. Instead, we want to nudge Bitcoiners away from absolutism and acknowledge that major narratives within the Bitcoin community have changed over time. And that's ok—it's appropriate to change your mind in response to new data. Purity tests are generally weak, since they tend to require that individuals do not evolve. But if most Bitcoiners went back and contemplated their own past histories, they would probably find that they evolved over time, too. Both of the authors have certainly been through the cycle.

In the end, a healthy respect for Bitcoin history is a necessary starting point of any attempt to define it. It is not unitary, and Bitcoiners are not ideologically homogenous. Bitcoin contains multitudes, and it's important to remind ourselves of that.

Thanks to Dan McArdle and Murad Mahmudov for the input.

Media Coverage of Bitcoin Is Still a Total Disaster

A recent Washington Post article shows how journalists get cryptocurrency wrong

Nic Carter

August 11, 2018

I 'm fed up with journalists who are either ignorant or unwilling to learn about cryptocurrency holding forth on its perceived weaknesses. Recently, the *Washington Post* published a piece entitled "Bitcoin is still a disaster" by economic affairs reporter Matt O'Brien, which I feel relies on mistaken assumptions to paint a misleading picture of the world. Today, I'd like to engage with some of the claims made in the piece, and show how O'Brien — among many others — get it wrong.

Claim: Currencies are meant to be stable

"*There's one thing a currency is supposed to do that bitcoin never has. That's maintain a stable value.*"

This assumes that bitcoin is a currency, and that the definition of currency is normative ("x should do y") as opposed to descriptive ("things of type x have the qualities y and z"). I'd classify Bitcoin the protocol as a complete monetary system, and bitcoin the unit of value as a commodity money, which has the potential to become a gold-like reserve currency. Commodities fluctuate — that's what they do.

Additionally, currency isn't meant to maintain a stable value. Monetary policy is used for a variety of macroeconomic objectives, including targeting GDP growth, unemployment rates, inflation, trade balances, and more. If stability was the objective, the Federal Reserve Board would target zero percent inflation rather than the two percent that it currently does. Am I moving the goalposts? It's matter of figuring out how bitcoin is used, and what it was intended for. I'm not sure [bitcoin creator] Satoshi Nakamoto ever defined bitcoin as a currency. He defines it as a system for electronic transactions, a peer-to-peer version of electronic cash, and an electronic payment system. He envisions bitcoin as a protocol and a bearer digital unit of value.

The interpretation of bitcoin as a currency is mostly inferred by outsiders imposing a particular view upon the protocol. Unburdened by priors, a neutral analyst would probably describe it as something similar to gold. In fact, Satoshi described PoW (proof-of-work) with a reference to gold mining, and later discussed bitcoin as analogous to a scarce, inert, infinitely portable metal which might develop a monetary premium. He clearly saw it as a gold-like commodity which would recapture those same properties in the digital realm, and I think this the most fitting interpretation of the system.

Claim: Bitcoin was designed with volatility in mind

"*Why has bitcoin's price been so up-and-down? Well, part of it is that it was designed that way.*"

This is an odd rewrite of history, or more charitably, a very strange interpretation of bitcoin's purpose. The impossible trinity tells that it's impossible to have free capital flow, sovereign monetary policy, and a fixed exchange rate all at the same time. Bitcoin was designed with sovereign monetary policy and a free flow of capital. No one underwrites or backs bitcoin, so it cannot be pegged to a real-world basket of goods. That's the same with gold. Both have emergent monetary premia. This can't be planned for — it just so happened that way. Needless to say, Satoshi didn't design bitcoin to be unstable, he wanted to solve the problem of double spends with digital cash such that it didn't rely on a single validator. Its volatility is an emergent property, not a design objective.

Claim: Validating transactions is the source of its computational overhead

"*[…] the problem [with a decentralized network] was that the only way to do that would be for every member of that network to keep a record of every bitcoin transaction there had ever been — that way they knew who had bitcoin to spend — which would require_a lot _of computing power.*"

This is a common misconception. PoW and mining ensures that the network deterministically converges to a shared history, without any subjectivity or off-chain coordination. The fact that the minted units have value means that miners are incentivized to behave appropriately in the short and medium term. And the fact that those units are worth $x means that miners will pay anything up to $x to obtain them. This is the source of the large quantities of computing power allocated to the network — the combination of efficient mining hardware and large amounts of value at stake.

The validation and record-keeping is behavior conducted by full nodes, not miners. The cost of maintaining the bitcoin data store is an externality pushed onto full nodes through bandwidth and storage costs. This is NOT the job of miners. This is a basic distinction lost on many.

Claim: Bitcoin's volatility is unnatural

"*But even this inbuilt volatility doesn't fully explain why bitcoin has been on such a roller-coaster ride. Something else must be going on, and that something is plain-old manipulation.*"

Volatility isn't inbuilt, it's a feature of every non-pegged economic asset. The *Post* should keep its fragilista-thinking to itself.

Does the Post have any proof that markets are not long-term efficient? If so, they have a Nobel prize in economics to collect.

Plain old manipulation? You really mean to tell me you think a $100 billion network was manipulated into existence? Is it so difficult to accept that bitcoin provides a differentiated, useful service to millions of people worldwide, and that's why it has value? Does the *Post* have any proof that markets are not long-term efficient? If so, they have a Nobel prize in economics to collect.

"*[…] what seems to still be happening in 2018 with various pump-and-dump schemes.*"

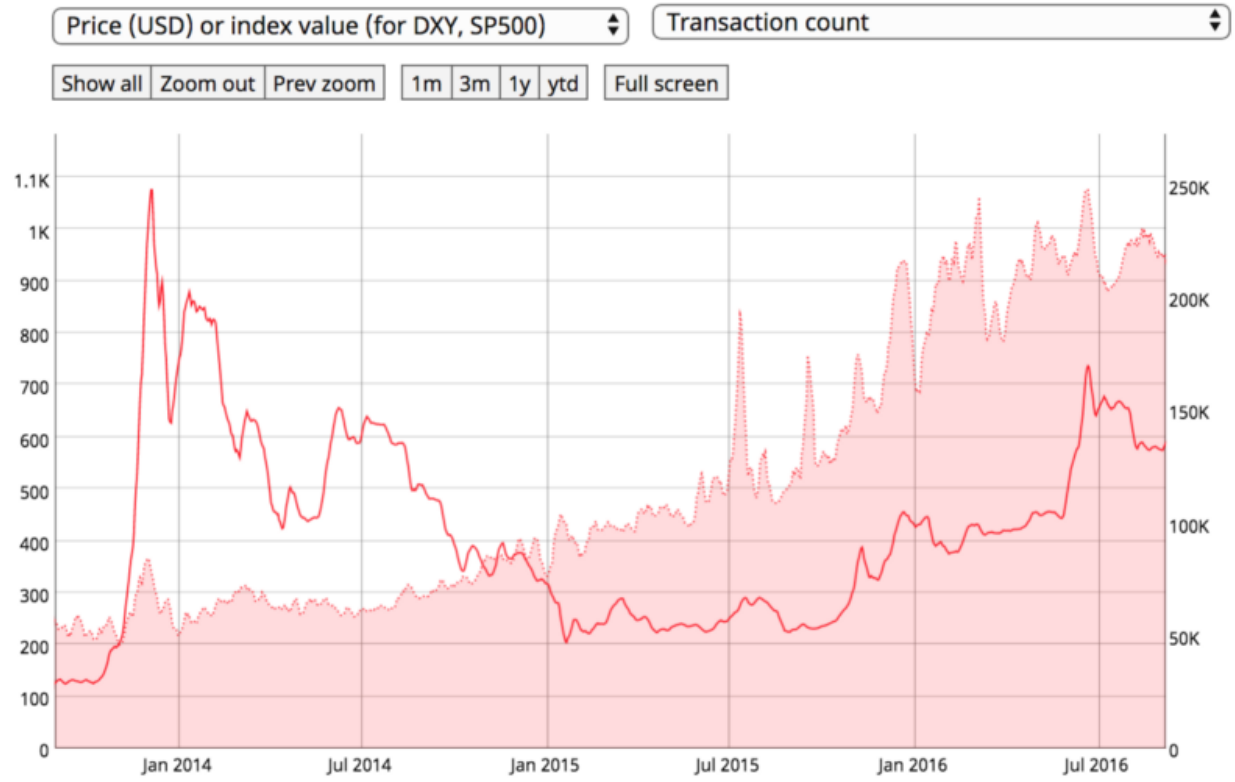
Don't conflate bitcoin with random worthless altcoins. There is a lot of PND [pump-and-dump] in this industry, but it is infeasible in the extreme to PND bitcoin. If you're part of a PND group, you target alts in the $50–$300 million range, not bitcoin.

Claim: Bitcoin is only used as a currency due to the wealth effect

"The first is that what makes bitcoin work as a way to transfer things—the expectation that its price will keep rising."

That's not what makes it work. It works as a way to transfer things because it's a pretty good distributed clearinghouse for value. If bitcoin were stagnant at $1000 for the next ten years, it would remain a good way to transfer things.

During the 18-month bear market that began in January 2014, people still used bitcoin. In fact, usage grew consistently the entire time.



Price (solid red line) and transaction count (shaded red area) during the 2014–16 bear market. Image: Coin Metrics

Bitcoin offers transactors a rival benefit; something they cannot find anywhere else. It's unique among cryptocurrencies, as it boasts the best reliability, uptime, dedicated track record, and protocol developer community. It's unique among monetary assets because it offers properties not instantiated by gold or the USD. There's a reason people choose bitcoin.

Claim: Bitcoin's deflationary characteristics mean that no one uses it

"Why spend $100 worth of bitcoin today if you think it's going to be worth $1,000 in a not-too-distant tomorrow? You wouldn't. And people aren't."

Shameless plug: I urge you to consult my website Coin Metrics, where we make this data free and available so anyone can use it. Conservatively, bitcoin saw $2.5 billion in on-chain transaction volume yesterday. That's omitting all the off-chain transactions that occur on Opendimes, on second-layer networks like Lightning, and internally at Xapo and at Coinbase.

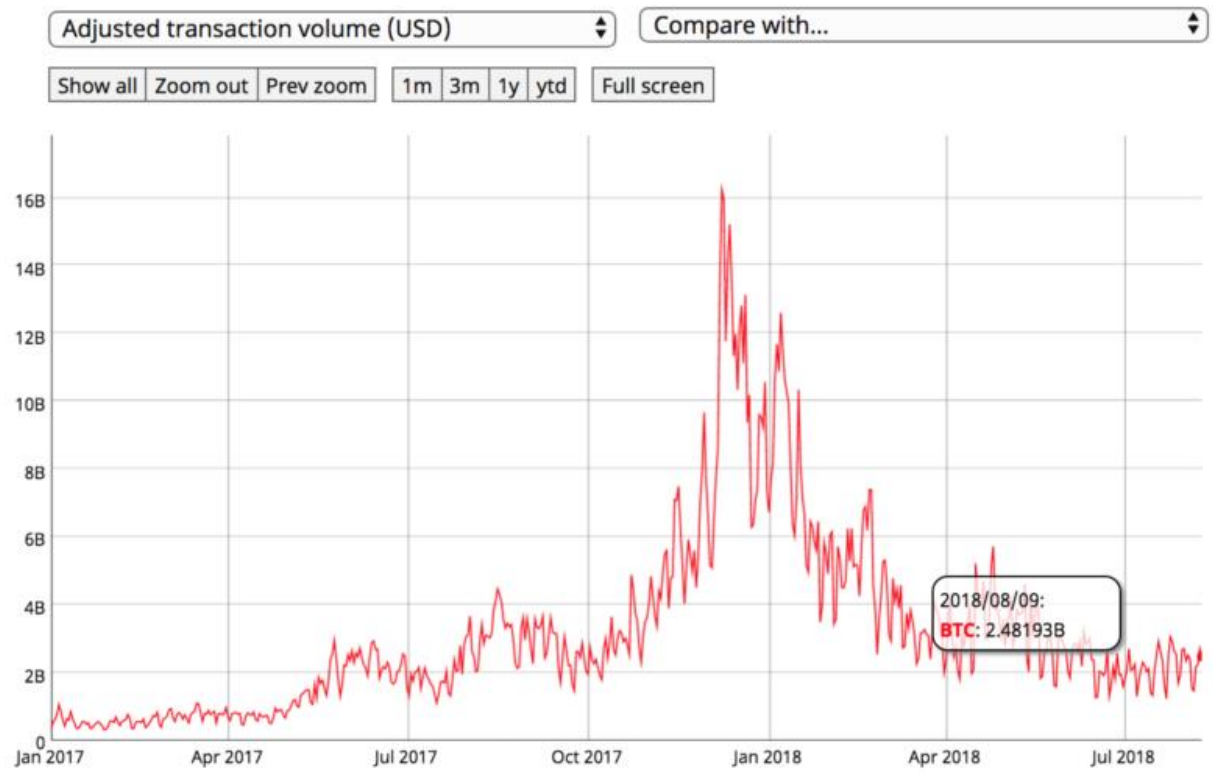


Image: Coin Metrics

In the last year, bitcoin routinely hosted the transfer of $2B worth of bitcoin a day, up to a peak of about $16B of bitcoin a day. That's a lot of fake transactions. The anticipated response to this from the skeptic is that on-chain volumes are just a clearinghouse for the multitude of exchanges worldwide, or simply a way for individuals to access the altcoin casino. The former is probably true; we have good evidence that bitcoin is mostly an industrial network dominated by exchanges and power users rather than one that caters to end-users. Using the rough heuristic that industrial users tend to batch transactions, we can see that 30–40 percent of the network is industrialized in this manner.

There's nothing wrong with this. It simply means that bitcoin acts as a decentralized global settlement network for a number of endpoints that connect it to everyday economic systems, with which users transact at the individual level. This is pretty radical! A decentralized, neutral, untamperable central bank that settles flows on a continuous basis between a global network of smaller banks (exchanges, merchants, and custodians). What a concept.

As for the "bitcoin as an on-ramp to the altcoin casino view," if this were true, then bitcoin would have cratered along with altcoins as they fell 80–90 percent over the last six months. However, bitcoin has shown great strength against altcoins during the bear market. If you look at any index, bitcoin has regained dominance. This pokes holes in the story that it is only used for access to altcoin pump and dumps.

For context, here's the Bletchley total market index quoted in bitcoins since December. Ever since the contraction began in January, bitcoin has strengthened against the rest of the cryptoasset market.

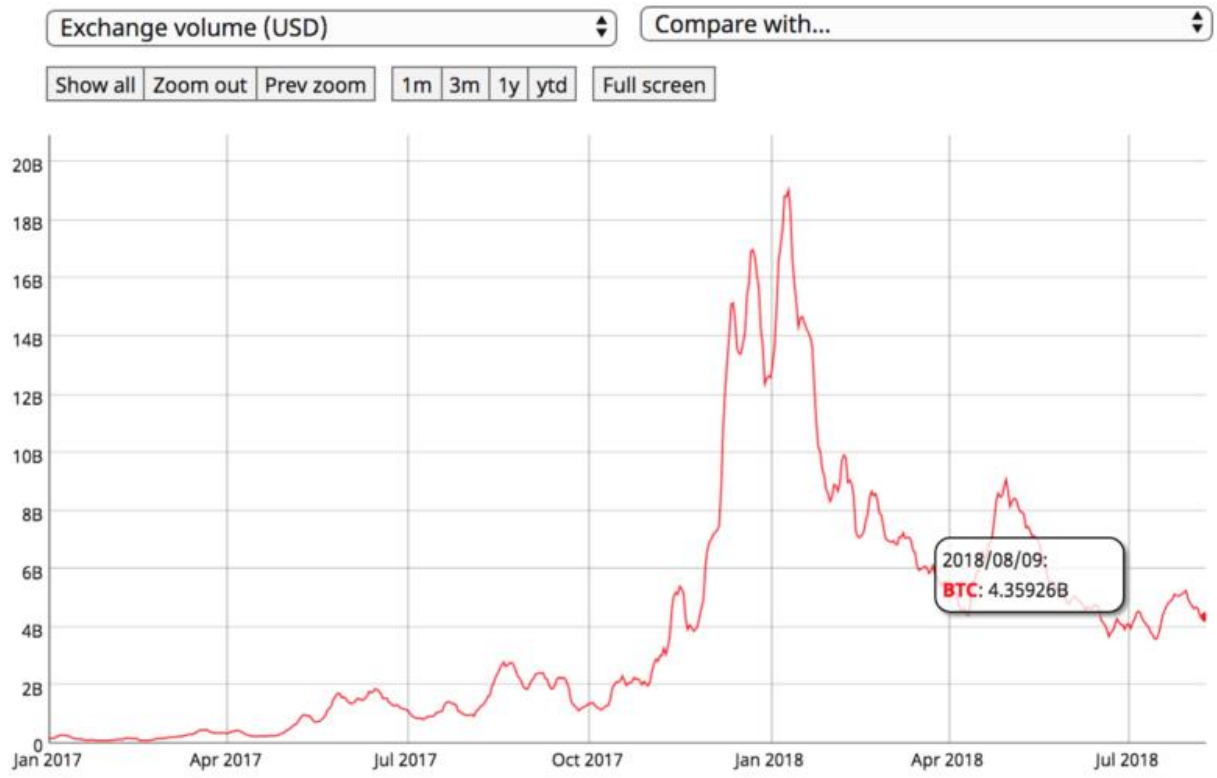
Image: Bletchley Indexes

You wouldn't expect this if bitcoin was only a vehicle for speculation on other cryptocurrencies. Clearly, there is demand for bitcoin in its own right.

Claim: Bitcoin is illiquid and hence manipulated

"*This lack of liquidity makes it pretty easy for a few fraudsters to push the price up quite a bit.*"

This isn't the case, and relies on a flawed reading of the Tether situation. Fundamentally, bitcoin is quite liquid. It has huge volumes on listed exchanges, and probably the same amount again on over-the-counter providers like Cumberland, Circle, Genesis, and Octagon.



Much illiquid. Very manipulation. Image: Coin Metrics

Even if you subtract all Tether volume, and all volume from synthetic exchanges like BitMEX, and all swaps and futures volume from the CME and CBOE, you have robust volumes. The market for BTC → fiat (on the right in the chart below) is also quite liquid.

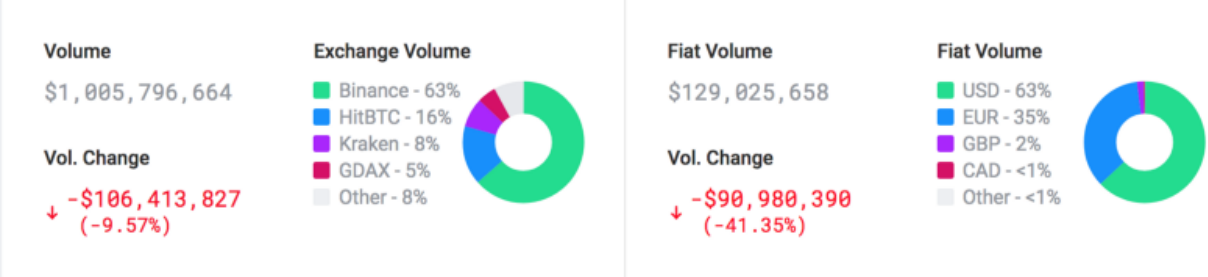
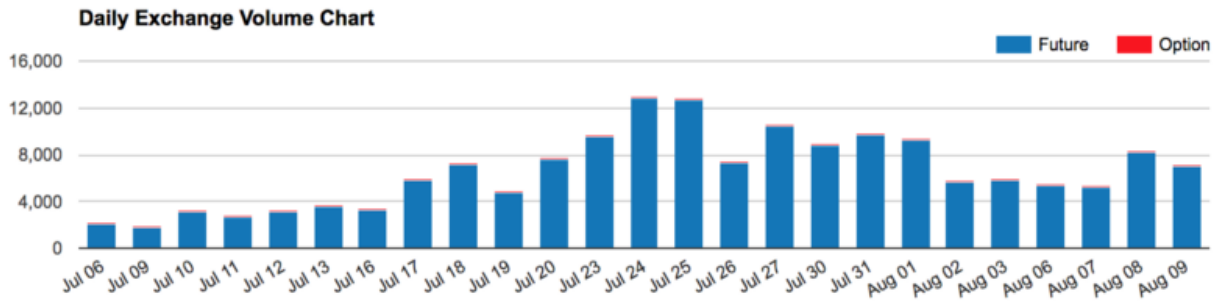


Image: Nomics

If you look at the market for fully-regulated futures exchanges, the picture is sunny.



CME daily volumes (contracts are for 5 BTC). Image: CME Group

Yesterday, 7077 contracts were traded at the CME—equivalent to $215 million. The liquidity picture is strong, and improving.

Claim: Bearer assets are dangerous and illegal

"*There's a reason, after all, why bitcoin has attracted so many scammers: All its transactions are irreversible.*"

You have to take the bad with the good. It's a digital bearer asset, which is completely new. Of course people want to scam with it—it's the best money ever invented. That USD is never used by scammers, right?

"*All of which is to say that if you steal a bitcoin, you get to keep a bitcoin.*"

If you earn a bitcoin, you get to keep a bitcoin. If you mine a bitcoin, you get to keep a bitcoin. Strong property rights are a hell of a thing. This is just an incentive to build more secure wallet and custody software. We're halfway there already.

Claim: Bitcoin still relies on a trusted set of intermediaries

"*Bitcoiners think all of this is worth it. That it's better to have a financial system that is clunkier, costlier and more vulnerable to attacks than it is to have to trust someone—or, more accurately, to_admit _that you have to trust someone.*"

Using bitcoin doesn't rely on trust in an individual. If you run a node, use a hardware wallet or a well-concealed paper wallet, and maintain good opsec, you are pretty much set. Of course, to obtain your bitcoin, you may have to use Gemini/GDAX/Square. But no one is forcing you to hold your bitcoin on an exchange. It's only long-term storage on an exchange which requires significant trust in the institution. And bitcoiners universally, vociferously, encourage people *not to do that*.

Nothing backs bitcoin or pegs it to a basket of assets. That's the point. Bitcoin was designed specifically to avoid the influence of a single authority.

More broadly, bitcoin doesn't remove trust entirely. That's a straw man frequently knocked down by critics. Bitcoin reduces the need for trust in a single institution. Instead, you just have to trust that the code is well-vetted in the typical FOSS [free and open-source software] manner, that the economics that underscore mining continue to hold, and that discrete log problem is still hard. We have plenty of

evidence that these things all hold, and will continue to hold. And we have plenty of evidence that, conversely, a single institution in control of the money supply will *always* abuse its power. If you don't believe me, just check out what's happening in Turkey today. Seignorage is a drug — and it's pretty much impossible to kick the habit.

"*Bitcoin exchanges require some measure of [trust] whether they realize it or not.*"

Centralized exchanges do. There exist non-custodial peer-to-peer exchanges, like Hodl Hodl and Bisq, for bitcoin. LocalBitcoins is another peer-to-peer exchange that places reduced reliance on a single intermediary. Even centralized exchanges can conduct periodic proofs of solvency, if users demand it. And, as with the rest of finance, if the brokerages/exchanges/clearinghouses are regulated under functional regimes, they are strongly incentivized not to run fractional reserves or lose user funds.

The broader point here is that relying on centralized exchanges is inevitable. Many people will trade off decentralization for convenience, and we can't stop that. We can demand that exchanges behave appropriately. There are many exchanges and custodians with long histories of robustness, resilience, and integrity. There is a market for exchanges, and the badly-run ones will fail.

To sum up

The problem with this article is that the pundit in question has settled on a narrative — bitcoin is a poor economic system — and then searched for various datapoints that confirm his view. Bitcoin is volatile, yes. It is an emerging commodity-money that's becoming financialized and growing from a small tribe of enthusiasts to a global user base. Of course it's volatile. Growth is not linear. Only fragilistas demand it to be so.

Nothing backs bitcoin or pegs it to a basket of assets. That's the point. Bitcoin was designed specifically to avoid the influence of a single authority. Bitcoin is priced exactly where it ought to be — this is always true. Manipulation might work on a 15-minute time frame, but it's just implausible in the extreme that a $100 billion-plus asset class has been manipulated into existence.

Yes, bitcoin relies on exchanges to provide exit ramps for individuals that want to reduce their reliance on sovereign currencies. Sometimes those exchanges get hacked and fail. That is entirely natural. Bitcoin continues to chug along unaffected. It's extremely popular; its strong assurances and settlement guarantees grant it daily volumes in the billions. It is a single order of magnitude behind Visa's economic throughput — that's right, just one 10x away. The gap will probably be closed in the next year. It has an unmatched record of reliability, resilience, and resistance to cooption. For a nine-year-old, this is a pretty good track record. If it were a human, it would be midway through the fourth grade.

Pundits will continue to ignore this; not because they're incapable of reading the data, but because they don't want to. They are deeply afraid of the world that bitcoin threatens to bring about. They prefer a paternalistic, easy-money regime, where occupations like punditry are profitable. Bitcoin promises accountability and a hard money standard. It threatens the existence of bailouts, moral hazard, and fiat-inflationism. In Bitcoinland, the only way to acquire wealth is to work for it. Cronyism doesn't work, as the central bank of bitcoin is entirely indifferent to politics and lobbying. This offends the sensibilities of the partisans writing for the *Post*.

Bottom line, the central premise of the article is wrong:

"*There's one thing a currency is supposed to do that bitcoin never has. That's maintain a stable value.*"

Bitcoin isn't designed to have a stable value. That just quite frankly isn't what Satoshi set out to build, and that's not the system we have today. Artificial stability — shorting volatility — leaves you destined for a blowup. That is the fate of any non-fully-backed stablecoin. Bitcoin is designed to solve the double spend problem for digital cash, and to provide a predictable monetary policy. It does that very well, it has done that for the last nine and a half years, and it will continue doing that for the foreseeable future. Demanding low volatility on top of that is farcical, and betrays deep ignorance about the tradeoffs inherent in monetary systems, and the way that financial markets work more generally.

Bitcoin is still an emerging, youthful asset. It hasn't reached maturity. It has somewhere in the realm of 50–100 million holders/users; that's global penetration of a percentage point or two. The base layer still hasn't been nailed down, let alone the next layers up on the stack. Development is deliberate and careful, because this is money we're talking about, not a consumer app. Governance is hard to organize; consensus is difficult to obtain. The internet wasn't built in a day, and neither will the protocols for transmitting value trustlessly.

Since the market is constantly revising its expectations for bitcoin, amid a backdrop of growing, unsteady adoption, its exchange rate is volatile. No one is forcing you to hold it; it is totally opt-in. Bitcoin may not make sense for Westerners who live under somewhat credible monetary regimes, but it might be a good bet for an Iranian, a Venezuelan, a Turk, or anyone else who mistrusts their monetary authorities. Truthfully, mechanisms to bring bitcoin to these disempowered groups are still lacking or nonexistent. But they have the right to money that isn't controlled and minted by a hostile state. This is why bitcoiners work to make global access to this economic institution a reality.

Bitcoin's complexity doesn't acquit these pundits for getting simple facts about bitcoin blatantly wrong. And ultimately, their ignorance hurts their bottom line. Being amateurishly wrong about basic details of a system that is widely-understood undermines their integrity and makes readers question their work. The *Post*'s owner Jeff Bezos should understand this and demand more from his employees.

I f any of this resonates with you, and you want to learn about this novel economic system, here are some sources I recommend for a better understanding of bitcoin:

- Coin Metrics: no-nonsense open data and charting platform informing users about the actual usage of cryptocurrencies (full disclosure: I am a Coin Metrics cofounder)
- Bitcoin Visuals: charts and visuals relating to bitcoin and the Lightning network
- Jameson Lopp's list of Bitcoin resources
- "Bitcoin's Academic Pedigree," Arvind Narayanan and Jeremy Clark
- BitMEX research: long-form investigations into bitcoin economics, the Tether mystery, and market dynamics

Thank you to hasufly and Larry Sukernik for their feedback.

Bitcoin's Existential Crisis

Cryptocurrencies lack leaders — they have no single source of truth. Philosophically, this can get complicated.

By Nic Carter

Posted October 31, 2018

Identity is a troublesome thing — for humans, nonliving systems, and objects alike, especially as they change over time. Humans can rely on essential traits like DNA to serve as stable markers of identity, and nonliving systems (corporations, for example) can rely on governments and legal systems to anoint them with stable identities.

Cryptocurrencies and public blockchains, though, have no such privilege. They aim to decentralize their leadership without relying on a single third party in establishing their identity. Instead, they rely on subjective social- and economic-consensus mechanisms. While some cryptocurrencies use foundations or corporations to resolve disputes and arbitrate core issues of identity, that's a fragile approach and generally not consistent with the objectives of these systems.

The most sustainable approach for cryptocurrency is to dispense with the kingmakers, bite the bullet, and leave it to intersubjective consensus. This requires a commitment to a set of practical values that constitute the essence of the system. Systems with more internal consistency and more universally agreed upon value sets are better equipped to last.

The Ship of Theseus Paradox

A classic question-of-identity paradox goes like this: The Greek hero Theseus asks his crew to rebuild his travel-worn boat, and they replace it plank by plank. When the task is done, he ponders whether his restored boat is really the same boat as before, given that all the parts have been replaced. He further considers that if he were to ask his crew to build a new boat with the planks of the old one, two boats would both have a credible claim to being his old vessel. But which is the true original?

It's compelling because there's no clear answer. The story shows us that the identity of an object isn't absolute — it's assigned, rather than essential.

This comes up even in human contexts: Your cells replace themselves so often that the present you shares very little physical matter with the version of you that existed a decade ago; prisoners held for violent crimes are paroled with the assertion that they have become "a different person" in some vital sense; or — perhaps the simplest example — you might at some time have credibly apologized the day after an intoxicated argument by asserting, "I wasn't myself last night." In all these cases, the person is clearly the same person in one sense of identity, but in another sense, many of the traits that make up the person are mutable.

This is okay because the systems that depend on humans to have stable identities can account for the fact that personalities, memories, and physical selves change over time. On a day-to-day basis, our friends and family recognize us, even with decades-long gaps. Low-stakes identity challenges can depend on the recall of certain things we know about ourselves — Social Security numbers, passwords, birthdays, mom's maiden name, or the name of your first pet. And high-stakes identity challenges can depend on physical markers like fingerprints, retina scans, or DNA tests.

If you build a system meant by its very nature to dis-intermediate third parties and exist independent of governments and legal systems, then you have a problem.

But those human identifiers all rely on the involvement of third parties. And, similarly, certain nonliving systems can use third parties to establish their sense of identity. Creating legal entities like corporations solidifies abstract, malleable sets of individuals and ideas and gives them persistence over time, even if their staffs and business models change entirely. And granting legal assignments like trademarks or patents gives ideas and concepts persistent identity as well as gives their owners exclusivity.

Most nonliving things don't have these kinds of third-party tiebreakers, though, making them especially vulnerable to Theseus problems. If you build a system meant by its very nature to dis-intermediate third parties and exist independent of governments and legal systems, you have an identity problem. And that problem is one public blockchains face.

The Theseus Problem of Blockchains

While I do not much like the term "blockchain," I'll use it here for simplicity. What I am referring is not enterprise blockchains but rather open and permissionless systems like Bitcoin or Ethereum. These two blockchains, in particular, have suffered severe crises of identity over the years.

For Bitcoin, its crisis turned on whether it should attempt to scale up as a P2P payment network immediately (and raise throughput) or whether it should pursue a layered approach. Ethereum had to contend with a reckoning in which participants had to determine their desired level of immutability in response to the DAO exploit.

Both sides had credible cases. There was no constitution that specified, one way or the other, that Bitcoin's blocksize was permanently capped or that Ethereum couldn't use a hard fork to reverse (ostensibly) illicit transactions. (Ethereum has a formal specification, but that is a more technical rather than constitutional document.) Instead, there were messy processes of social-consensus formation, appeals to authority, deep readings of original documents, and, ultimately, rancorous splits.

These are not incidental problems or one-offs; they are a core feature of decentralized systems. Public blockchains like Bitcoin, with no recognized leadership, are exposed to competing views of what they are and should be. In a previous post, Hasu and I made an effort to chronicle those disparate visions over time. For sure, there are developers, entrepreneurs, thinkers, miners, and capital allocators who wield disproportionate influence in Bitcoin, but no single individual or institution exerts unilateral control. Therefore, divergent views of the protocol cannot simply be quashed.

Two Approaches to These Problems

How do we cope with this? There are two ways: One is expedient and the other is more sustainable.

The first and most common method is to give a corporation or foundation rights to a trademark, as is the case with Tezos or EOS.IO. This is the default for non-Bitcoin blockchains and gives an entity the legal force to anoint and ratify a single chain. Of course, no one is bound to follow this, and there could be a fork of Tezos that everyone mutually agrees to use.

However, the trademark carries certain legal protections, and if a fork tried to retain the name, the trademark owner would have recourse, at least where the fork tried to interact with regulated institutions. In this case, the trademark is just one manifestation of the core issue, which is confirmation that the leadership of a blockchain is seeking authoritative ratification of their control. Other activities this entity might engage in would be pressuring exchanges to use one ticker over another or support one fork over another as well as spreading a consistent message to the media. All of these give the entity de facto control over which fork is chosen in a dispute.

Consider just how little persistence Bitcoin's components have. The entire codebase has been reworked, altered, and expanded such that it barely resembles its original version.

The other approach is to throw caution to the wind and spurn any external marker of identity, relying instead on an intersubjective consensus, such that the system can change over time while remaining faithful to its original goals. This is the approach leaderless (or, more accurately, leader-minimized) systems like Bitcoin and Monero go for. Of course, there are influential individuals in both systems, but neither has a foundation or corporation in control of a trademark or a clear decision-making body. Many critics would say that Bitcoin Core, as the author of the dominant implementation of Bitcoin, wields disproportionate control, but that's a reductive reading. It is not an official body, and the dominant implementation that they create does not define the essence of Bitcoin but rather its instantiation. Pierre Rochard puts it well:

Bitcoin's block and transaction validity rules are a social consensus that is automated with software. Where they diverge the software is wrong. This is an uncomfortable reality for proponents and detractors alike.

This concept deserves formalization and a lengthier treatment, and I will cover it in a more detailed manner in a forthcoming post.

To pause for a second, consider just how little persistence Bitcoin's components have. The entire codebase has been reworked, altered, and expanded such that it barely resembles its original version. Core features like multi-signature transactions and pay to script hash have been added over the years, and the protocol only loosely resembles the system described in the white paper — which itself is not a constitution but rather an introduction and teaser. None of the original nodes from 2009 are still running (to the best of my knowledge). Mining has become industrialized and has virtually nothing in common with the hobbyist mining of the early days. The leader has left, as have many of the early developers and stewards of the system, and new sets of developers have sprung up in their place.

The registry of who owns what, the ledger itself, is virtually the only persistent trait of the network, but the ability to copy it at will means it can be splintered. The Bitcoin Cash fork copied the UTXO set and started a new history while retaining the old balances. So it is largely trivial to copy the history and make a claim to the name. Indeed, this was exactly the strategy employed by Bitcoin Cash proponents — strident appeals to Satoshi Nakamoto's vision.

To be considered truly leaderless, you must surrender the easy solution of having an entity that can designate one chain as the legitimate one.

Their argument was, in effect, that Bitcoin Cash more closely recaptures the essence of Bitcoin. Bitcoin may own the name, but we are closer to the system as intended by its creator and, hence, the true heirs. And they were free to do this because Bitcoin has no foundation, corporation, or entity that sets policy and lives entirely outside of the government, which ultimately adjudicates decisions like these in more conventional contexts. The Bitcoin/Bitcoin Cash struggle was so bitter precisely because there is no single entity that can anoint a true Bitcoin, so it had to be fought in the market, in the media, and in the minds of proponents.

Many critics identify this struggle as a shortcoming or flaw of a distributed system and propose alternative mechanisms to adjudicate disputes. Whether these will work are an empirical matter, but ultimately, the tradeoff remains. To be considered truly leaderless, you must surrender the easy solution of having an entity that can designate one chain as the legitimate one. Political consensus as to the true, genuine protocol must be continually sought and found. Without a stable identity, the system is guaranteed to splinter into pieces.

One Solution to Leaderless Identity

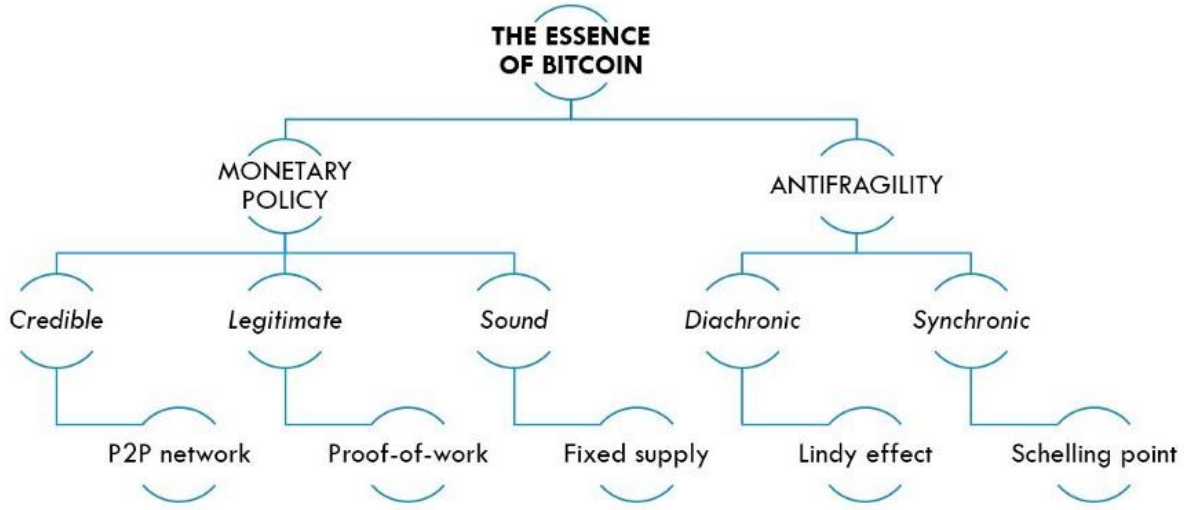
How can you have persistence of identity in a distributed, leaderless system? The cheap solution of having a single entity take de facto or de jure control is unavailable in this context. In fact, the answer is already quite established, although it hasn't been much discussed. The way that Bitcoin has survived a decade of identity crises, absent any single leader, is this: It has a robust and mutually understood set of ideals that constitute the essence of the system.

The stronger the consensus around these shared ideals, the easier warding off competitors and resisting fragmentation becomes. Additionally, the market mechanism of pricing forks (sometimes prior to their birth through futures) enables individuals to receive powerful informational signals about what their peers are intending to do, which propagates consensus-forming signals efficiently.

During the Bitcoin Cash fork, the core question was whether Bitcoin is a protocol for small, P2P payments at the expense of node operators or a system for cheaply verifying P2P payments at the expense of expediency and short-term scalability. The resounding answer (although some still disagree) was the latter.

The challenge is that these rules cannot be "found" anywhere. Much like the U.K.'s government, there is no single written constitution. The rules aren't in the white paper, which is incomplete in many respects. They aren't exclusively in Satoshi's writings on the mailing list or the forum — and given his departure after two years, Satoshi sought to resign from the position of ultimate arbiter anyway. The system is best

described by the original codebase, although that has changed over time. More fundamentally, the core values of Bitcoin are an intersubjective agreement around a few concepts. David Puell makes a credible attempt to capture it here:



Source: David Puell

In fact, codifying and refining these rules is our challenge. By leaving, Satoshi left that task to us. Consistently define the protocol, give it a soul, and let it grow and adapt while being true to its original essence. This is an ongoing challenge, and we learn more and more about its essence with each passing battle, hostile fork, and attempted corporate takeover.

Ultimately, the commitment of the Bitcoin community to these ideals may represent a source of risk. Absolute commitment to the sound monetary policy (the 21 million hard cap) is a core virtue of Bitcoin but limits its design space and ability to pivot if the fee market doesn't work. But this is the tradeoff Bitcoin has opted for. Other protocols instead sought a more malleable set of core values, relying instead on appointed institutions or well-defined leaders to designate the path forward. The more corporate and top-down these are, the less they rely on a shared identity; in other words, they become empty and soulless. I don't believe there's any substitute for diving in at the deep end and relying on essence rather than top-down decrees.

Toward a Bitcoin Ontology

In its 10th year, Bitcoin continues to struggle with these metaphysical issues. It suffers from more existential crises than a philosophy undergrad reading Kierkegaard for the first time. And the reason is that Bitcoiners are strongly opposed to a clear hierarchy for decision-making in Bitcoin. The lack of a benevolent dictator or philosopher king for Bitcoin is held as a strength, even if that makes decision-making less efficient.

In this context, it is not only difficult to forge consensus on key technical issues but also to organize the expenditure of political capital to actually implement those changes. The dispersion of decision-making

power and the lack of a unified developer entity is the "problem of governance" that Bitcoin is said to suffer from.

But, here, the disease is also the cure. Bitcoin's lack of governance is what makes it interesting. It's a set of rules for moving money around that is very difficult to influence in any way whatsoever. Other open-source projects have benevolent dictators, but in a high-stakes game where the developers can serve as kingmakers for how resources are allocated in society, it's wise, in my view, to make interfering with the protocol as difficult as possible. Of course, development occurs, but certain core attributes are walled off and considered largely untouchable.

As for the problem of a stable identity, absent a single foundation that maintains the trademark, Bitcoin must make do on its own. In practice, users, exchanges, miners, businesses, and developers engage in an ad hoc, socio-political process of adjudicating between competing visions of Bitcoin.

I expect this debate will end with three divergent philosophical stances within the Bitcoin camp, although it has implications more generally:

First, you have what I call "essentialists" and "materialists." Essentialists, like myself, believe that the actual code is just a representation of some more fundamental values that the code is trying to express. Essentialists are amenable to rollbacks if something goes wrong in extreme cases because, at that point, the code will have been a poor expression of the form and can be overridden.

I expect there will arise a rival camp of materialists who believe the code is supreme and, in fact, represents the actual substance and reality of the system. Materialists are fond of saying things like "Bitcoin Core is Bitcoin." They don't buy the argument that Bitcoin Core is just an implementation of a more nebulous, uninstantiated specification. They often believe that the creators of Bitcoin Core control Bitcoin more generally.

Just as certain Supreme Court justices are strict constructionists and other justices are loose constructionists, it is the same with Bitcoin.

Leaving materialism aside, essence and essentialists — in practice — come down to differing interpretations of the written materials that Satoshi left us, the broader cypherpunk canon, and subsequent empirical findings (such as asserting that the SPV scaling model Satoshi described doesn't work). Just as certain Supreme Court justices are strict constructionists (believing the Constitution must be interpreted as written) and other justices are loose constructionists (believing the Constitution is a living document that we have to interpret in context), it is the same with Bitcoin.

So, further stratifying the essentialist camp, let's call the white paper enthusiasts "intentionalists" and their opponents "anti-intentionalists." Intentionalists tend to think Satoshi's vision was scaling on the base layer while anti-intentionalists tend to think Satoshi's precise vision is irrelevant and that what matters more is the system he gave us and its evolution over time. Note that anti-intentionalists are still essentialists. They believe that Bitcoin should be able to adapt while remaining true to its essence but that its exact instantiation doesn't have to be true to the original specification.

Labels can be dangerous, and excessive labeling is usually not very useful. But these three factions — materialists, intentional essentialists, and non-intentional essentialists — are what I've identified, and I think making the lines clear will help us clarify any debate.

The last year has been a period of relative respite in the war over Bitcoin's soul. However, the battles will continue. This is the nature of the system; it cannot possibly be another way.

Building a fundamental piece of technology that will bring Bitcoin to the next billion users? Reach out: castleisland.vc

---

Unpacking Bitcoin's Assurances

Dis-aggregating the system's guarantees

By Nic Carter

Posted Jan 13, 2019

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

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

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

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

* proposed name

Bitcoin's assurances by usage phase

Open access

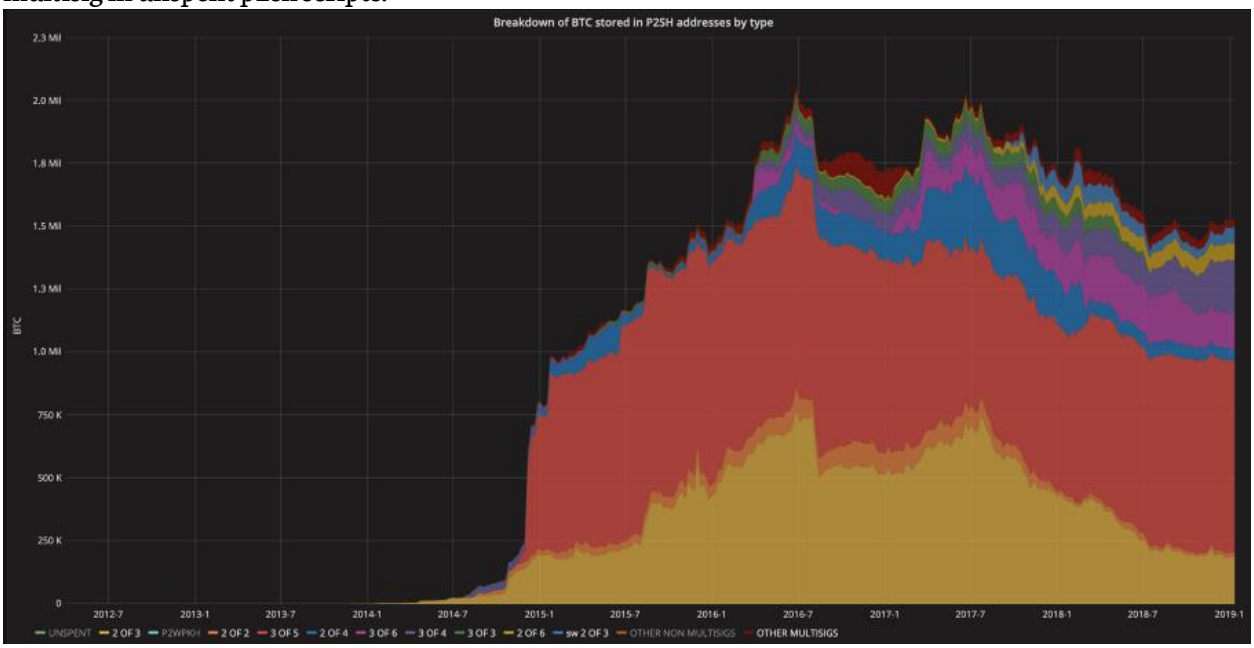
This is the shorthand for "the right to freely acquire Bitcoin." No amount of decentralization in Bitcoin's architecture itself can guarantee this. As many Bitcoiners will point out, free access to the asset requires a vibrant and competitive industry of fiat onramps. The existence of quasi monopolists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

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

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

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

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



Source: p2sh.info

To sum up, open access to Bitcoin is a core component of the system — what use is the asset if you can't easily obtain it? — yet it is somewhat overlooked. It's important to be realistic about this. Bitcoin suffers from a paradox whereby individuals in countries with relatively less need for Bitcoin have frictionless access to it, while individuals dealing with hyperinflation have to reckon with a less developed onramp infrastructure. There is much work to be done here.

Seizure resistance

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

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

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

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

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

Censorship resistance

This is the most celebrated assurance attributed to Bitcoin, so I'll be brief. At its core, Bitcoin allows permissionless broadcast through the p2p gossip protocol and the miner fee incentive. Anyone can make a transaction, although they have to sufficiently compensate a miner to include it in a block. If there is a lot of traffic, this could entail a delay or a higher fee. The other required component here is a well-connected network of nodes available to route transactions. If full nodes were to become very expensive and difficult to run, full node counts might decline, making broadcast more difficult. That said, node counts would have to drop precipitously to impair network performance, so this isn't an immediate concern.

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

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

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

Counterfeit resistance

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

Comparing Bitcoin to gold, the ability to run a full node is akin to owning a professional-grade XRF spectrometer to check the integrity of your bullion. Compared to the expensive and tricky tests to verify gold's authenticity, verifying the integrity of one's Bitcoin is a breeze. Running a node costs a few dollars a year and can be done on consumer hardware and bandwidth with little difficulty. This very accessible counterfeit resistance only persists as long as running a node is relatively cheap — a significant increase in the bandwidth, computation, or memory required to run a fully validating node would hinder it significantly. Right now, Bitcoin is growing at a stable rate, and physical plug-n-play node hardware has made full nodes more accessible than ever, so this assurance seems safe for now. For individuals and enterprises that don't want to run nodes directly, a good diversity of managed node software exists.

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

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

Free exit

Free exit — the ability to sell Bitcoin unencumbered — is another aspect of the system that is sometimes overlooked. It's not strictly a Bitcoin guarantee, but Bitcoin's usefulness is significantly downgraded in its absence. The real world consequences of overzealous chain analysis companies (whose heuristics implicate

innocent users through false positives) make themselves felt when those users attempt to sell their Bitcoin for fiat. Since fiat offramps are the most easily regulated and are run by risk-averse institutions, they are a natural target for entities that create blacklists and ascribe taint to individual UTXOs.

There are a few strategies to reckon with this. One is to obfuscate the origin of funds through collaborative tumblers like the Wasabi wallet . Another approach is to reverse-engineer the heuristics that chain analysis firms use and develop mixing strategies that implicate everyone in taint (thus rendering those heuristics incoherent) or that avoid detection altogether through specialized transaction types. This is the general approach of the folks behind the Samourai wallet. Routing around the centralized, highly-regulated exchanges is another option, either on the p2p marketplaces or by exchanging BTC for goods and services, rather than fiat.

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

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

How to scale Bitcoin (without changing a thing)

Why Bitcoin banks need to prove their solvency

By Nic Carter

Posted April 14, 2019

Almost from inception, the "scaling debate" in Bitcoin, and cryptocurrency more generally, has been framed in what could be called Hegelian terms.

- **Thesis**: peer-to-peer cryptocurrencies are useful for online commerce
- **Antithesis**: online commerce requires millions of transactions a day
- **Synthesis**: to succeed, cryptocurrencies must scale

This has been the default backdrop for discourse in the industry and the onlooker press for the better part of the last decade. In this piece I'll posit that this obsession, which has driven discourse in Bitcoin land for the better part of a decade, misses the point, and I'll suggest an alternative framing. I believe that *institutional scaling* presents an under-appreciated scaling vector, and it is quite possible to employ it without significantly compromising Bitcoin's assurances.

By this I mean the Finneyan view of Bitcoin in which Bitcoin banks emerge and issue notes against deposited Bitcoin. If you look carefully, a proto version of this system is in place today. However, for cherished assurances like scarcity to be upheld, exchanges and custodians need to start making routine attestations that their reserves match their liabilities.

Before we start, a tiny literature review (optional):

- Spencer Bogart on Bitcoin's strong assurances
- Hasu on how Bitcoin supports non-state property rights

- Yours truly on the quality of Bitcoin's touted assurances
- Jameson Lopp on the exact technical guarantees and near-guarantees that PoW gives you
- Davidson, De Filippi, and Potts on how public blockchains are a new type of institutional technology
- Saifedean Ammous on how Bitcoin could function solely as a settlement network

Prescience on the mailing list

The very first public comment on Satoshi's white paper, coming as a response on the cryptography mailing list five hours after publication, was this astute observation from James A. Donald:

If hundreds of millions of people are doing transactions, that is a lot of bandwidth — each must know all, or a substantial part thereof.

What James understood is something that has escaped many who scampered down terabyte-block rabbit holes: Bitcoin only works because anyone can retain a copy of the ledger and stay in sync. If you make syncing with the current state of the ledger too expensive, only a privileged few can stay up to date, effectively adding a hierarchy to a system which must be flat to function.

Satoshi's answer to this question, interestingly, involved SPV proofs, which, bathed in a present-day epistemic light, appears somewhat naive. SPV proofs ostensibly allow a non-full node to know that a transaction has been included in Bitcoin without downloading the whole chain. Casually invoking SPV proofs as the solution to scaling is a bit like the scientists behind the Apollo program remarking: "Oh, a trip to Alpha Centauri? Just the simple matter of faster than light travel."

Suffice to say, SPV proofs have been virtually abandoned as a viable scaling method today. Under a variety of scenarios, they tend to collapse into users having to validate the entire chain anyway.

James was spot on. He immediately understood that Bitcoin was a single ledger which all of the nodes in the network had to continuously reaffirm at 10 minute intervals. Since everyone had to see everything, hundreds of millions of transactors would simply overwhelm the system.

Stairway atop Diana's Peak, St Helena

But what if this teleological premise — *Bitcoin is for global, online, peer-to-peer commerce at the individual level* — was flawed? Enter Hal Finney.

Hal's vision

In 2010, digital cash pioneer Hal Finney famously made the case for what could be called the institutional approach to scaling Bitcoin.

Actually there is a very good reason for Bitcoin-backed banks to exist, issuing their own digital cash currency, redeemable for bitcoins. Bitcoin itself cannot scale to have every single financial transaction in the world be broadcast to everyone and included in the block chain. There needs to be a secondary level of payment systems which is lighter weight and more efficient. Likewise, the time needed for Bitcoin transactions to finalize will be impractical for medium to large value purchases. Bitcoin backed banks will solve these problems. They can work like banks did before nationalization of currency. Different banks can have different policies, some more aggressive, some more conservative. Some would be fractional reserve while others may be 100% Bitcoin backed. Interest rates may vary. Cash from some banks may trade at a discount to that from others.

In a brilliant stroke of foresight, Hal understood that base layer Bitcoin would never scale to the desired level in its current format. (Unfortunately, many Bitcoin evangelists failed to understand this, and their misapprehensions led to the bitter blocksize wars of 2015–17.) In Hal's view, Bitcoin would be a high-powered money mediating large settlements between financial institutions, rather than a payment token used for the online equivalent of petty cash payments. He realized that Bitcoin's rather slow settlement times (compared to physical cash or credit cards) combined with the inefficiency of the chain itself meant that directing Bitcoin to the brick-and-mortar payments use case was a square peg in a round hole.

What Hal envisioned was a system where banks could be auditable, transparent in their capital ratios, and accountable. A free market for reserve/capital ratios could even develop, as depositors would be able to select banks with varying levels of reserves to suit their risk preference.

Undercapitalized banks might fail — but this would be a healthy market signal, a culling of weaker entities to render the herd stronger overall. Compare this to the system that became unraveled in 2008/09: financial institutions heaping on leverage, knowing that they would be bailed out if something went wrong. Since the government made it clear that it would not allow banks to fail, the market was robbed of that valuable feedback mechanism and risk became increasingly abstracted, obscure, and hidden.

In the words of Elaine Ou:

Financial institutions make people feel safe by hiding risk behind layers of complexity. Crypto brings risk front and center and brags about it on the internet.

In finance, risk never truly disappears, even if hidden — and suppressing it often has the nasty effect of unleashing it in a more dramatic fashion later on.

Just as risk crept up on us, unheralded, and financial institutions failed one after the next in a cascade of toxic balance sheets in 2009, so too will the long-suppressed forces of systemic risk unleash themselves when our present monetary experiment finally unwinds.

Can Bitcoin mollify this? Perhaps not. But its very structure facilitates the creation of an alternative financial system which is far more transparent and open about risk than the present one. This is the Finneyan view of Bitcoin: Bitcoin as a virtual commodity sitting in provable reserves in financial institutions. No one's liability, a provable virtual commodity which a bank can rely on to attest to its viability.

Winding road through Glencoe, Scotland.

Scaling assurances

Let's briefly revisit what we mean by scaling, anyway. It's clear by now that simply opening up the block space throttle doesn't work. This is because Bitcoin is designed to be auditable, and auditing the blockchain requires the full, unabridged ledger.

Fundamentally, Bitcoin relies on everyone being aware of every transaction. Can this be scaled without compromising this core feature? Let's see how the major classes of scaling innovation fare under this lens:

1. **Deferred settlement/reconciliation**(chiefly lightning). What lightning and other defer-reconcile models of transacting do is grant users the ability to create relationships which are then settled at a later date. The chain's assurances are still present and available, they just aren't employed for each transfer. These models do however trade off by (temporarily) weakening assurances — final settlement is no longer instant and you have to be online to receive a payment, for instance.
2. **Database model** (massive base layer scaling). As mentioned, simply increasing the ledger size compromises the assurances of the blockchain — not everyone is able to maintain the ledger. There may be a way to do this in a trust-minimized way with SPV and fraud proofs, but we haven't found it yet.
3. **Extending assurances to other chains** (sidechain, security inheritance, merged mining). This model blesses other block space with Bitcoin's security or extends Bitcoin's own block space. Merged mined coins like Namecoin, proof-of-proof approaches like Veriblock, and sidechains like Rootstock are all roughly in the same family of approaches to the problem. These represent a compelling potential avenue to scaling, as they extend Bitcoin's settlement guarantees to a potentially unbounded block space, but it is still under explored. However, assurance impairment is possible — risks remain that miners might censor sidechain closures or otherwise interfere with the sidechain. The productized implementations that we've seen like Liquid have used consortia rather than relying on PoW.
4. **Trust-minimized institutions**. This approach takes the assurances of Bitcoin — natively auditable, scarce digital cash — and applies them in the context of a depository institution. In short, rather than individual users being the clients of Bitcoin, institutions like exchanges, banks, and custodians adopt the end user role, with their own users indirectly benefiting from Bitcoin's assurances. Trade offs remain, and some features of Bitcoin don't apply in a custodial context, but if protocols like Proof of Solvency are implemented, some of Bitcoin's guarantees can shine through, even if filtered through an intermediary.

What should Bitcoin banks look like?

Is Hal's vision of a world of banks backed by Bitcoin plausible? In one sense, it's the world we have today, as many users only touch Bitcoin indirectly, through custodians and intermediaries. While most exchanges are presumed to be full-reserve, and indeed generally claim to be, in practice this isn't universally the case.

Scaling the base layer. Rockport MA.

It's becoming clear, for instance, that QuadrigaCX was running a fractional reserve for most of its existence. I don't need to recap the sordid history of malfeasance and negligence at cryptocurrency exchanges.

Something as simple as a Proof of Solvency protocol would have made the Quadriga situation evident long before it folded. Rather, what would have happened in practice (imagine a world where solvency attestations were universal among exchanges) is that Quadriga would have refused to prove their reserves, and would have rightly come under suspicion, pre-emptively saving users a lot of heartache and lost coins.

An ideal Bitcoin bank would employ schemas like Proofs of Solvency to *pass through Bitcoin's assurances to depositors*. Of course, these aren't faultless, and can be cheated, but it's a high bar to clear. You *can* lie to your auditors if you're a publicly traded company, but you'll likely be found out at some point, and now you've broken the law. Any serious Bitcoin bank engaging in an audit would likely only do so if they felt that they were going to pass it. As mentioned above, if this became popular, it would segment the Bitcoin depository industry into reputable, trusted banks which routinely proved reserves, and untrusted banks held in suspicion due to their unwillingness to provide these audits.

To be clear: I am not denying that IOUs circulating within and among banks generally fail to instantiate the properties of Bitcoin. What I am suggesting is a way to make those IOUs more Bitcoin-like, by providing depositors with certain assurances.

Selected Bitcoin properties by usage method

Property	Bearer asset nature	Permissionlessness	Scarcity	Programmability	Verifiability
Definition	*The holder is presumed to be the owner; ownership is not beholden to a third party*	*Users can transact without asking permission of any third party*	*Only 21 million units will exist; no third party can alter the rate of production*	*Basic conditional contracts can be created*	*Users can verify that the core protocol rules are not being violated*
Strength					
Base layer Bitcoin	Strong; the Bitcoin protocol treats anyone with a key to unlock a UTXOs as the owner	Strong; base-layer Bitcoin does not require permission to send or receive	Strong; PoW ensures that the creation schedule is adhered to	Limited programmability with script: multisig, HTLC's	Strong; full validation allows a user to verify the correctness of the entire chain
Lightning-held Bitcoin	Strong w/ caveats; Bitcoin in channels is encumbered but ultimately available	Non-custodial LN users can transact permissionlessly	Strong; LN cannot be used to create new Bitcoin	Vastly enhanced programmability, still featuring bitcoin assurances	Strong albeit requiring more active monitoring
Exchange-held Bitcoin	Weak. Redemption required to obtain genuine Bitcoin	Virtually absent. Permission is required to operate	Can be impaired; fractional reserves can temporarily inflate BTC supply	Limited programmability, lacks the assurances of Bitcoin	No verifiability
Exchange held-Bitcoin + Proof of Solvency	Weak, although depositors can trust that liabilities can be met	Still absent as above	Strong; given a credible solvency protocol, users can be assured that deposits are as claimed	Limited programmability	Some verifiability regarding no inflation possible; albeit less than running a full node

This table demonstrates that, while Lightning and other on- or near-chain layered approaches expand Bitcoin's assurances to other domains, exchanges with proofs of solvency can chip in as well. Sidechains (if they ever get figured out) and Lightning are not mutually exclusive with the proposed institutional model: I envision them as parallel and complimentary approaches to scaling Bitcoin. The important thing to note is how little an IOU at a non-proof-of-reserve exchange means. It is very remote from base-layer Bitcoin.

Something else which is worth calling out: Lightning and other L2 approaches may well become mainstream approaches to scaling, but they do so *under a different set of assurances*. The assumptions that hold in Bitcoin are different in Lightning! There is nothing inherently wrong with this — and Lightning enthusiasts and developers will admit this — but they aren't *quite* as ironclad as the settlement assurances that vanilla Bitcoin gives you. So the precedent that Bitcoin scales under various alternate tradeoffs is well-established, and should be generalized to institutions as well.

Credit creation on Bitcoin

Many Bitcoiners will recoil in horror at the words "fractional reserve," even though they were uttered by Satoshi's first disciple himself, Hal Finney. However, I believe that the risk of fractional reserves can be managed, **if they are accountable to the free market** and **if the banks are transparent about their actual reserves.**

The problem with exchanges running fractional reserves is not, I'd argue, that they fail to operate at full reserve, but that they *misrepresent their risk to depositors*. While this is a heated debate among Austrian economists, I personally support a free market for user deposits, with exchanges running at various reserve or capital ratios.

The important thing is that they are transparent about it, so that users can adequately assess the risk of insolvency. As we well know, full reserves are not required for a bank to operate in practice, as users do not

typically redeem all of their deposits at once. In the US, for instance, larger depository institutions must maintain a reserve equal to at least 10% of reservable liabilities. For a history of reserve requirements in the US, see this article by the Fed. I don't know what the right number is in Bitcoinland, but I believe in the market's ability to find that number. It's evident by the popularity of lending facilities like BlockFi that some users will prefer interest-bearing accounts, and as such will tolerate some more risk at their bank.

Robust to external shocks: Bova's bakery. Boston, MA.

What do proofs of solvency actually prove?

So far I've been treating proofs of solvency/reserve as largely homogenous, which does them a disservice. In fact, I should be more precise about the nomenclature. A proof of reserve involves proving **what you actually own,**and it is generally meaningless without a corresponding proof of liability, which is a proof of **what you claim you owe**. Together, if executed correctly, they can serve as a conditional proof of solvency.

Proof of Reserve	+	Proof of Liability	=	Proof of Solvency
You own what you say you own		*You owe what you say you owe*		*Your reserves match your liabilities*

The first method to prove solvency was formalized Greg Maxwell and Peter Todd, which we'll call the **Merkle approach.**Presented at length here by Zak Wilcox, the Merkle approach allows users of the exchange to verify that their balance is included in the list of all customer balances that the exchange publishes in their attestation. There are two parts to the process, proving what you owe, and demonstrating what you own. As described by Greg Maxwell:

<@gmaxwell> First you show how much funds you have via signmessage for actual coins on the chain. Thats easy enough.

Then you need to prove how much you should have. This is a little tricker. You could just publish EVERYONE's balances e.g. by account ID but thats undesirable for privacy and commercial reasons.

Proving reserves is actually the easy part — the exchange signs a transaction with all of their UTXOs. Everyone can now see that the exchange owns x BTC. Of course, the exchange can borrow Bitcoins for this.

This is why the attestation only works on an ongoing basis, and should be paired with an analysis of cash flows (imagine an exchange that habitually borrowed 10,000 BTC every quarter, the week before their solvency attestation, and paid it back the next day!)

The challenging part is proving what you owe — that is, what your liabilities are to depositors. This is where the Merkle tree comes in — it allows users to verify that their accounts and balances are included in the final hash without leaking the details of everyone's balances and account information. Like herd immunity, users can have relatively strong assurances that the exchange is not lying if a sufficient number of them verify their balance.

A malicious exchange can of course cheat by publishing 0 balances for dormant accounts that they expect not to perform the check; but they run a big risk in doing this — if even one of the zeroed accounts makes the check, the exchange is exposed.

As Zak says, the Merkle approach

[...] gives you the means to check your own belief of the exchange's liability/obligation to you is included in their publicly declared one, and to let you make an informed decision about whether to continue doing business with them if those numbers differ.

Steven Roose of Blockstream has formalized the proof of reserve portion of the process with a BIP and a Github implementation. This should be paired either with the proof of liabilities (as described above) or a credible auditor.

The problem with the Merkle approach is that it makes public the exchange's liability, which many exchanges may not want to do. Thus in 2015 Dagher, Bunz, Bonneau, Clark and Boneh published *Provisions: Privacy-preserving proofs of solvency for Bitcoin exchanges* . Addressing the shortcomings in the Merkle approach, Dagher et al set out in *Provisions* to:

[E]nable an exchange E to publicly prove that it owns enough bitcoin to cover all its customers' balances such that (1) all customer accounts remain fully confidential, (2) no account contains a negative balance, (3) the exchange does not reveal its total liabilities or total assets, and (4) the exchange does not reveal its Bitcoin addresses.

Provisions consists of three protocols:

- Proof of assets (/reserves): the exchange uses some ZKP trickery to prove that it owns a certain number of BTC, without revealing that number (read the paper for more detail)
- Proof of liability: the exchange commits to the total sum of user balances, also allowing depositors to privately verify that the exchange is committing to the right balance
- Proof of solvency: the exchange proves in zero knowledge that the proof of assets and liability sum to 0

This is an improvement over the Merkle + signmessage approach, as it doesn't leak the exchange's balance, instead outputting a simple 1 or 0 — the exchange is solvent or not.

Other work on the topic that I wont summarize includes:

- Decker, Guthrie, Seidel, Wattenhofer (2015),*Making Bitcoin Exchanges Transparent*
- Mohan and Devi (2017),*Privacy Preserving Non-interactive Proof of Assets for Bitcoin Exchanges*
- Narula, Vasquez, Virza (2018),*zkLedger: Privacy-Preserving Auditing for Distributed Ledgers*

In short, between the Merkle approach, and the various ZKP approaches that have been proposed, copious tools exist to enable Bitcoin banks to prove their solvency. Today, they have little reason not to.

Where are the Bitcoin banks?

So if Finney's Bitcoin banks can help scale Bitcoin, where are they? The large exchanges and custodians (I'm using exchanges, custodians, and other depository institutions that take Bitcoins interchangeably with 'banks' here) are just another set of trusted third parties. As the gatekeepers to Bitcoin, they often do more harm than good, impairing open access and free exit.

Ok, so the title was a slight exaggeration. Coinbase-BTC-IOUs and Bitfinex-BTC-IOUs and Xapo-BTC-IOUs don't grant users the same transactional assurances as raw, commodity Bitcoin, but they still represent an under-appreciated scaling vector. Those who have professed their belief in institutional scaling include Xapo CEO, Wences Casares:

We have a lot of transactions that happen within Xapo. Because the Xapo to Xapo transactions don't need to go through the blockchain so they don't. They can happen in real time and for free. So today we see about 20 Xapo to Xapo transactions for every transaction that we run through the blockchain.

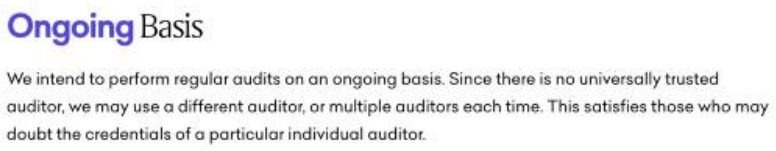
It's easy to see how a bitcoin bank could issue actual notes against deposits, serving as the pegs in a sidechain. For it to be credible though, you need redeemability. This is the same issue that Tether faced — for a time, no one believed that they could actually redeem USDT. Ongoing attestations to reserves would help with this.

As stated, a proof of reserve audit allows a depository institution to prove that they hold a certain amount in reserve, which would then — with the help of a trusted auditor — be used to demonstrate that their liabilities matched their reserves.

Alternatively, you can let users determine that internal balances exist to match their own deposits; if enough users do this, you can have reasonably strong assurances that the exchange is solvent. It should be noted that proofs of reserves are by no means a silver bullet. Coindesk's Danny Bradbury notes that both Bitcoin reserves and fiat operations should be proven, and that snapshots are far inferior to an ongoing reserve proof.

Historically, many exchanges have conducted proofs of reserves. These appear to have mostly been catalyzed by the Mt Gox insolvency. Interestingly, the history of proofs of reserves is mostly one of broken promises. Several exchanges have deleted any trace of their previous proof of reserves attestations and others have backtracked on promises to perform proofs of reserves on an ongoing basis.

- June 2011: Mark Karpeles constructs a crude proof of solvency with the famous 424,242 BTC transaction
- February 2014: Coinkite posts a now-deleted proof of reserve audit
- February 2014: in the wake of the Gox insolvency, executives at Coinbase, Kraken, Bitstamp, BTC China, Blockchain.info, and Circle publish a joint statement promising audits and more transparency. Only Kraken and Bitstamp prove reserves, and none on an ongoing basis
- February 2014: Coinbase summons Andreas Antonopoulos to review their storage practices, although he does not conduct a formal review. He subsequently deletes his blog about it
- March 2014: Bitstamp publishes an outside attestation as to their solvency, in the process creating the largest transaction in history (at the time)
- March 2014: Kraken proves reserves using the merkle approach,claiming that they "intend to perform regular audits on an ongoing basis." They do not.



- April 2014: British exchange Coinfloor issues their first provable solvency report. Unlike every other Bitcoin exchange in existence, they follow it up with another report the following next month. And again. And again. Last month, they published their 60th report, far more than every other exchange combined.
- August 2014: Stefan Thomas announces that he has completed a successful proof of reserve audit for OKCoin. However, in a now-deleted reddit post, the outgoing OKCoin CTO subsequently claims that OKCoin misled Thomas and partially faked the audit. A CCN article entitled "OKCoin passes proof of reserve audit" is also later deleted

I can confirm OKCoin removed a number of accounts (used by OKCoin bots) to pass the Proof-of-Reserve audit in Aug 2014. In essence, these bots trade on fractional (or fictional) reserves. Stephan Thomas was lied to during the audit. This is an unfortunate limitation of the proof-of-reserves method.

- August 2014: Huobi releases a proof of reserve audit administered by Stefan Thomas
- June 2015: Bitfinex issues a press release stating that, using Bitgo's multisig software, they will rid themselves of their omnibus model and store user coins in segregated accounts, so that depositors could verify their holdings on-chain in real time. In August 2016, Bitfinex is hacked to the tune of of 119k BTC and they abandon the segregated multisig method. Bitfinex subsequently publishes BTC, EOS, and ETH coldwallet addresses for public scrutiny
- November 2018: Tether issues a quasi-proof of reserves; their banking partner Deltec Bank and Trust Limited attests to their cash balance. This matches the amount of Tethers in circulation, although skeptics aren't quite satisfied

Waiting for exchanges to follow up on initial proofs of reserves

One commonality emerges: exchanges and depository institutions tend only to issue attestations or proofs of reserve under extreme duress. The flurry of activity in 2014 was precipitated by the Gox insolvency. Despite claims that proofs of reserves would become enduring and routine processes at these exchanges, not one has honored that promise aside from Coinfloor.

Perhaps things are changing. New depository institutions like Fidelity Digital Assets, Square Crypto, Bakkt, and ErisX are entering the market, several of which have announced their intention to be more accountable to Bitcoin users. As regulators become more sophisticated, it doesn't seem inconceivable that they might one day expect cryptographic audits from Bitcoin banks. Now that QuadrigaCX is being exposed as not an accidental key loss but an actual insolvency and potential fraud, 2019 might be an opportune time for some of these exchanges to revisit their proof of reserve protocols. If they don't, the new breed may well eat their lunch.

Conclusion

Bitcoin is an institutional technology, a nation state without an army. Perhaps instead of trying to force it into a mold that ill-suits it, we should instead try to reckon with its present reality. Yes, a messy patchwork of custodians and banks has emerged, many of them taking a devil-may-care attitude to user deposits. Over a billion dollars have been stolen or misappropriated from these honeypots.

How, realistically, can this state of affairs be amended to suit Bitcoin's nature? Despite a refrain of "not your keys, not your coins," the Bitcoin banks are here to stay: the convenience tradeoff is simply too compelling. What if we acknowledge that they will persist as long as they perform a useful service, and focus instead of bringing Bitcoin's assurances to them?

Ten years on, Bitcoin has entered its adolescence. Perhaps by seeing it for what it is — a peculiar beast, suitable for a narrow set of things — it can become more comfortable in its own skin. By adding institutions to the set of entities accountable to Bitcoin's innate transparency, we can radically improve the state of affairs in Bitcoin's depository industry today.

Objections

Bitcoin Banks are inherently incompatible with Bitcoin

There is a somewhat nihilistic view present in Bitcoinland which starkly denies the importance of exchanges and custodians, as if they didn't exist. This is often born, in my opinion, of a nostalgia for the 2010–12 era when the network was genuinely quite flat and non-hierarchical. Of course, you can't inhibit free enterprise and commerce, and smart entrepreneurs decided to create useful services of exchange, custody, and banking for bitcoiners.

Far from being a dark irony, as most pundits maintain, I think this is a perfectly natural evolution. Banks are now a meaningful portion of our network, and we have to live with that. Yes, running a node to verify incoming payments matters, but factually, some nodes matter more than others. In particular, exchange nodes, the nodes powering block explorers, blockchain API companies, merchant services, and one day, big lightning hubs. There's nothing wrong with this, and it doesn't compromise Bitcoin.

It is fashionable to declare *not your keys, not your bitcoin*, and while absolutely true, this also misses the point. What do we do about the people that have decided to surrender their keys in exchange for IOUs at a bank? Do we smugly deride them for being unwilling to self-custody (still not intuitive for most normal people)? Or do we empathize with them, and try and ameliorate their situation by holding exchanges accountable? I strongly suggest we do the latter .

Why would anyone start proving reserves now, given that it's so out of favor?

There is a perverse feature of the cryptocurrency industry that could be referred to as the paradox of transparency. Put simply, the more transparent you are, the more attack surface you open up, and the more opportunity your critics have to undermine you. As a consequence, being open and transparent is disincentivized. Since this industry has been lightly regulated so far, most successful projects are highly obscure in their operation. There is no equivalent of a 10-K for established projects or an S1 for new token launches.

The same goes for Bitcoin depository institutions: they are regulated under a vague patchwork of regimes with no domain-specific regulation in place (in the US at least). Against this backdrop, it is often advantageous to them to disclose as little as possible about their operations. Additionally, proofs of reserves are costly; and in the lasts three years exchanges have not sought to differentiate themselves on credibility but rather liquidity and number of listings.

I believe that there are several catalysts for exchanges to start proving reserves:

- The growth of SROs. Absent any new legislation or more activist regulators, self-regulatory organizations may come to play a larger role in the US and other developed nations. Japan leads the way already. SROs will need to advocate to their national governments that they are imposing standards on exchanges, and asking member organizations to prove solvency is an easy (and not overly onerous) carrot.

- The extended fallout from QuadrigaCX. The full details from the scandal have not yet been revealed, but it is increasingly likely that it was not a case of misplaced keys. Forensic evidence is pointing to a deliberate, years-long fractional reserve. This kind of deception is unprecedented in Bitcoin; in Gox, the exchange was hacked rather than deliberately stealing funds from depositors.
- A bifurcation into grey/black market and compliant exchanges. A split is coming where a set of sophisticated, regulator-friendly exchanges emerge make a clean break from the underclass of unregulated exchanges.This new cohort will seek to differentiate themselves, not on the basis of the number of tokens traded, but in terms of credibility and security. Introducing audits which include proofs of reserve will be a natural source of differentiation.

Fractional reserves at banks permanently destroy the value proposition of Bitcoin

There is a common misconception that a Bitcoin bank running a fractional reserve permanently impairs Bitcoin's assurances. For sure, a fractional reserve at a bank inflates the supply of credit (loosely, money) for the period that it persists. QuadrigaCX did exactly this: they didn't have sufficient reserves, and they *covertly* increased the supply of Bitcoin, if you include Bitcoin IOUs in your assessment of Bitcoin's supply.

However, covert fractional reserves are unsustainable — they typically get found out, as happened with Gox, and Quadriga, etc. When this happens, the Bitcoin credit supply shrinks as the fraud is uncovered and those IOUs lose their convertability. Fractional reserves are leveraging, and their discovery is a deleveraging. So the covert inflation of the money supply only occurs while that covert fractional reserve is running. The largest banks — Coinbase, Bitfinex, etc — have a strong incentive not to misrepresent their solvency, because they have reputations to uphold, and executives face jail time if they do. And as this industry matures and more regulated banks come to account for a larger fraction of the market, most funds under custody will settle with the most responsible banks.

Fractional reserves are inherently bad/evil

This is more of a philosophical position than one that can be settled empirically. I happen to believe that non-full-reserve banking on Bitcoin is inevitable, and since it is inevitable, we might as well advocate for it to be as responsible and transparent as possible. I believe that the reason fractional reserves at Bitcoin banks are bad is not due to any inherent problem with fractional reserves themselves because they misrepresent the solvency of an exchange. Full reserve exchanges can always redeem deposits; fractional reserve exchanges occasionally default on that obligation.

If I lend my friend Bitcoin for a month, I have created credit. Genesis, BlockFi, and Unchained Capital all do this, but on a bigger scale. Institutional prime brokerage — the same concept, but on a much larger scale — is just around the corner. When a bank runs a fractional reserve, they are doing the same thing. They create credit by lending out a portion of user deposits and they make money by charging a higher rate on those loans than the interest that they pay depositors. So for fractional reserve skeptics to be consistent, they have to be against *all lending activity* relating to Bitcoin. I have actually seen this view expressed, but it seems extremely draconian — and unrealistic to boot. There is a clear demand to borrow and lend Bitcoin.

I take a similar attitude to fractional reserves as I do to the existence of custodians: they are inevitable, so we might as well make them as transparent as possible. I propose exposing Bitcoin banks to the same forces that gave rise to Bitcoin itself: the free market. Right now we have a market for custody which everyone naively believes is fair, and is periodically beset by shocks as fraud is exposed. Why not a market for custody where the varying reserve ratios on offer are made transparent?

It's impossible to effectively audit a Bitcoin bank

One of the harshest critics of the reserve currency model of Bitcoin is Eric Voskuil. In a post on his Libbitcoin wiki, Eric pushes back at the Ammousian view of Bitcoin as a sound reserve to be used by commercial or central banks, similar to the way our monetary system used to operate with gold. (Eric also gave an interesting talk on the topic at Baltic Honeybadger 2018).

Eric dismisses the notion that paper certificates against depository Bitcoin are credible, stating:

The ratio of issued [Bitcoin IOUs] to BTC in reserve cannot ever be effectively audited.

It seems that Eric's critique relies on a few beliefs:

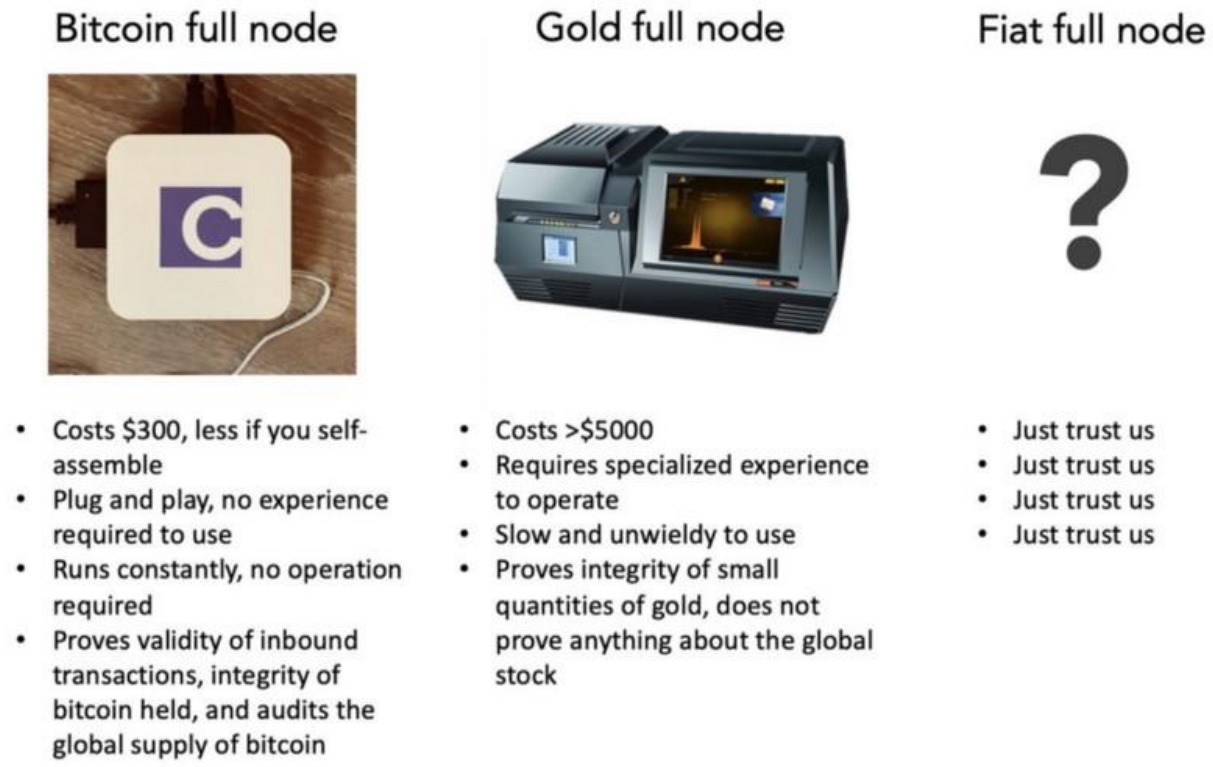
- That commercial banks would be coopted by the State — indeed, that banks are mere extensions of the State
- That proofs of reserves can *never* provide adequate guarantees to depositors
- That reserve ratios must be upheld by trust and hence would fail to be enforced
- That the entire bitcoin market would be consolidated within these depository institutions would would settle IOUs against each other

I don't have the space to give them a full treatment here; I would defer to Juice's excellent point-by-point rebuttal. To be frank, I just flat out disagree with Eric on a few key areas here. I think that proofs of reserves, if done correctly and with a reputable auditor, can provide depositors assurances of solvency *in spades*. I also don't believe that the government would immediately come to control the entire money supply in a bitcoin depository setting; commercial banks are independent, and in a non fascist state, would remain so.

Let's rewind a bit. To believe that a Bitcoin banking system can escape the problems that doomed the gold-based system, you have to believe that there are advantages that Bitcoin has relative to gold as a reserve asset. I would venture that it is the case. In particular:

- Bitcoin is auditable by design. What an individual does when they run a full node is that not only do they continuously audit the supply and make sure that the rules are being followed, but they audit the entire sequence of historical transactions to make sure every single one was legitimate and within the rules
- Auditing Bitcoin's M1 is cheap. It costs a few dollars a month to run a node. Gold nodes, by contrast, are expensive. XRF Spectrometers are pricey and tricky to operate. A fully trusted gold supply chain is so expensive that there only a handful in the world, with London being by far the biggest. In practice, in the private gold market, the cost of verifying any given lump of gold is so

high that entire trusted supply chains have been created, so that gold circulates within a walled garden and doesn't have to be reverified at every step. If you are curious, read the LBMA's good delivery rules. $300b worth of gold is currently held in London within this framework. Alternatively, central banks just custody large quantities of gold themselves and never move it.



- Assessing the amount of Bitcoin credit outstanding is at least plausible, whereas for gold it's impossible. If exchanges issue IOUs redeemable for Bitcoin deposits, as they do today, we have the tools to verify that they aren't lying to us

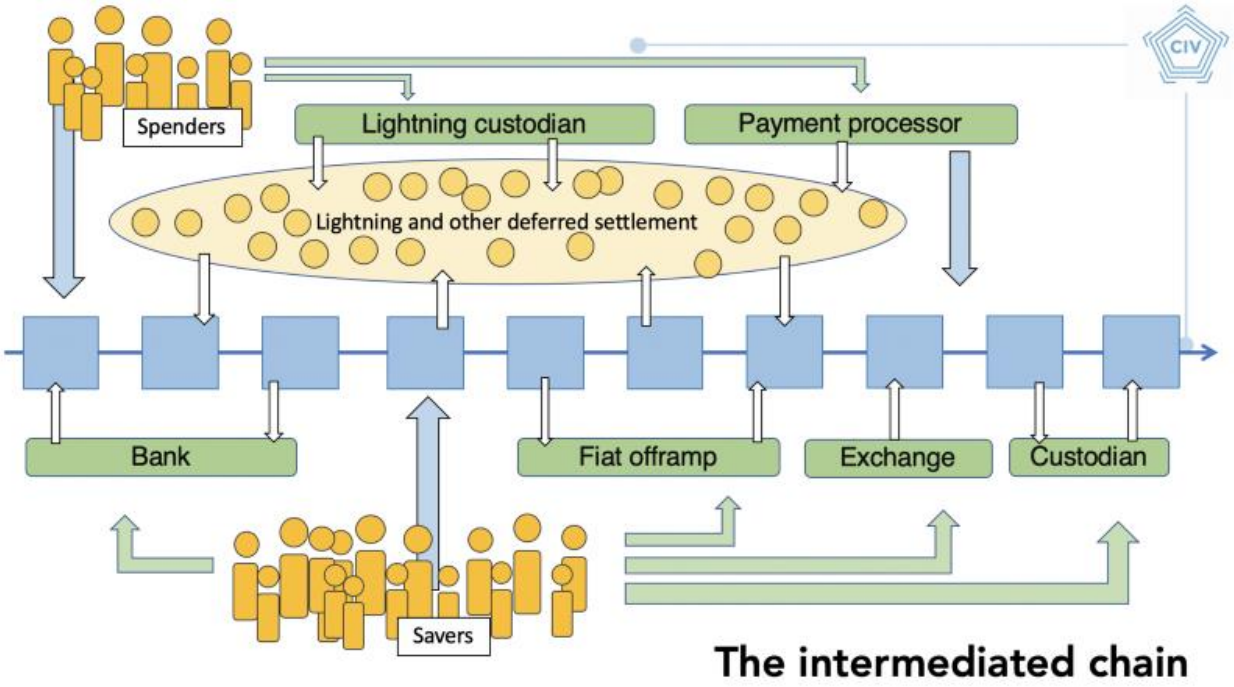
In short, Bitcoin provides auditability guarantees that are incomparably better than those provided by gold, doing away with the need for a trusted supply chain, costly overhead for storage, or costly inbound verification. The cryptographic nature of Bitcoin, which can be extended through simple proof of reserve attestations, is exactly what makes it so amenable to trust-minimized custodianship.

Why are you settling for intermediation? Why not push for a world where Bitcoin is used directly by all?

I'm aware that my approach could be perceived as settling. However, I think the opportunity to live in a world where non-intermediated Bitcoin is the sole mode of usage has long passed us by. Normal people have a voracious demand for custodians and banks — and that makes sense. We don't self-custody our

stock certificates either. These things are a challenge to custody ourselves, and the additional benefits of banks — earning interest, providing peace of mind, and so on — have made them extremely popular.

According to Coinshares, about 2.9m BTC are currently held in the custody of entities like Coinbase, Xapo, the Greyscale Bitcoin trust, Binance, and so on. Coin Metrics tells us that about 14 million Bitcoin have been active in the last 5 years (total issued supply is 17.6m, but significant portions of supply are lost or inert), so that leaves us with **20 percent of the effective bitcoin supply** in the hands of third parties!



Slide from my presentation at BH2018

I don't happen to believe that we will all collectively wake up one day and decide to self-custody. I see this industry going two directions: one where custodians continue to breach our trust and lose user deposits, or one where we hold them accountable to a high standard. For the latter to occur we need to acknowledge that they are an important part of the Bitcoin economy, for better or for worse. If the existence of intermediation implies that Bitcoin has failed, then the dogmatists should abandon the project.

And, to be frank, even if you don't like the idea of Bitcoin banks, you have nothing to lose from demanding that they prove their reserves. Normal financial institutions deal with stringent regulations because the consequences for failure are so severe. In lieu of a regulatory regime covering institutions which take Bitcoin deposits, we might as well lobby exchanges to audit themselves.

What if [bad thing] happens to Bitcoin? Is this generalizable?

The framework I'm proposing applies to any auditable digital bearer asset. That's the distinction between gold and virtual currencies/commodities: they are natively auditable, whereas gold is extremely cumbersome to audit and verify. Privacycoins are more challenging but there are ways to audit them with viewkeys or selective disclosure.

Lending by Bitcoin banks effectively inflates the supply of BTC

Canny readers will remember their Econ 101 classes where it was demonstrated that the cascade of deposits and lending at banks with low reserve ratios leads to the effective creation of new money — far more money than existed in deposits.

This would be the case if a vibrant industry of non-full-reserve Bitcoin banks were to appear. In fact, if you squint a bit, this reality is the case today. Nominal volumes on the Bitcoin derivatives exchange Bitmex eclipse those at spot exchanges. Far more Bitcoins trade there than exist in deposits at the exchange, precisely because Bitmex extends loans to users in the form of margin. That's credit creation.

I don't think there is anything inherently wrong with the creation of credit, as it is the most basic component to finance. If credit is being created in a transparent way, on top of a reserve asset that is no one else's liability, that's a significant improvement over our current system. And I think it's something worth pursuing.

Thanks to Hasu , Matt Walsh, and Warren Togami for their feedback and assistance with this article.

Bitcoin bites the bullet

Some of its most puzzling tradeoffs explained

By Nic Carter

Posted June 19, 2019

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

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

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

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

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

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

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

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

Managed/unmanaged exchange rates

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

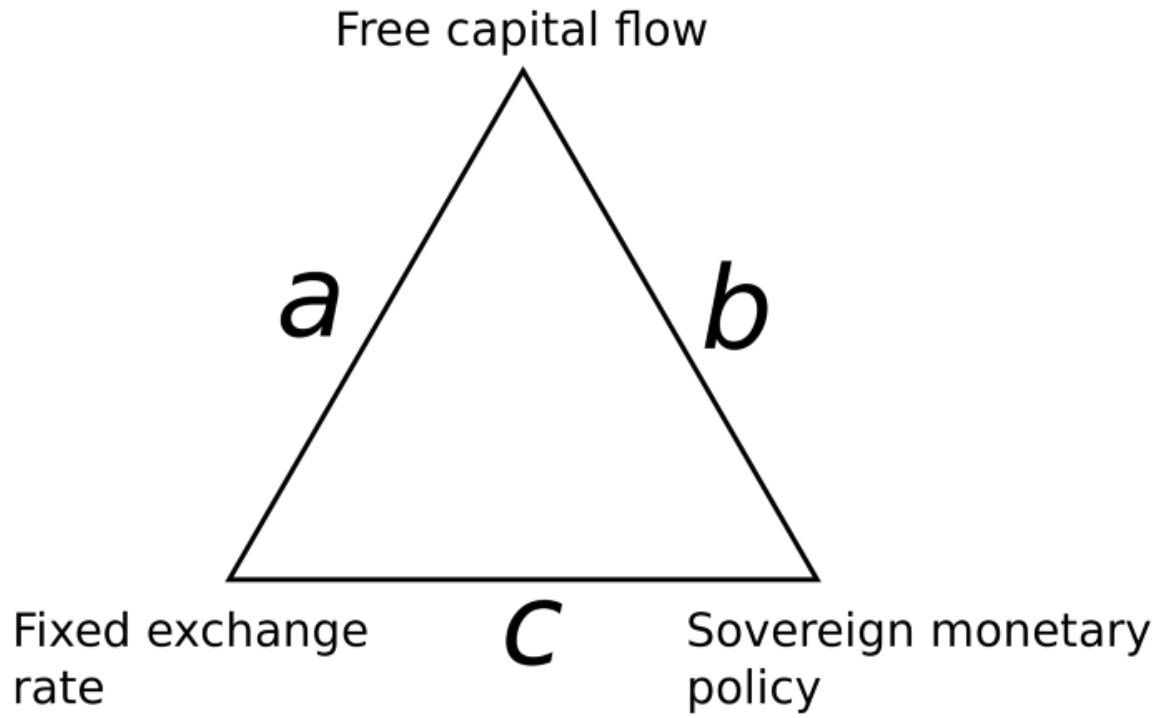
For now, virtual currencies such as Bitcoin pose little or no challenge to the existing order of *fiat* currencies and central banks. Why? Because they are too volatile, too risky, too energy intensive, and because the underlying technologies are not yet scalable.

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

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

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

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



The 'impossible trinity' of monetary economics

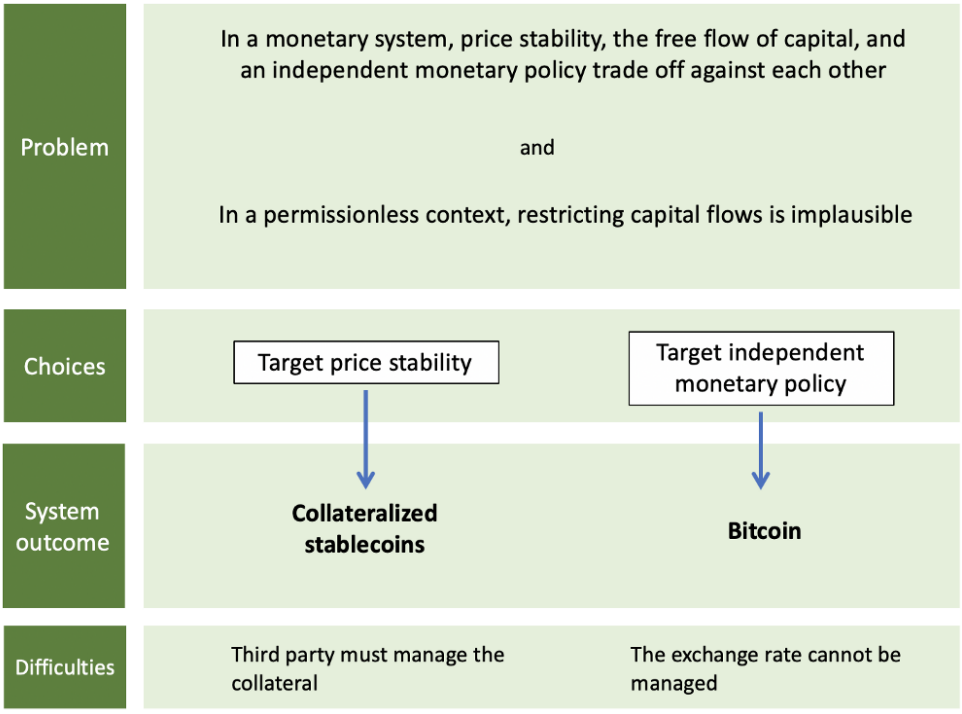
The Bank of England was infamously reminded of this constraint in 1992 when Soros and Druckenmiller realized that its peg with the German Deutschmark was fragile and could not be defended in perpetuity. The BoE had to admit defeat and allow the Pound Sterling to float freely.

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

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

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

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



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

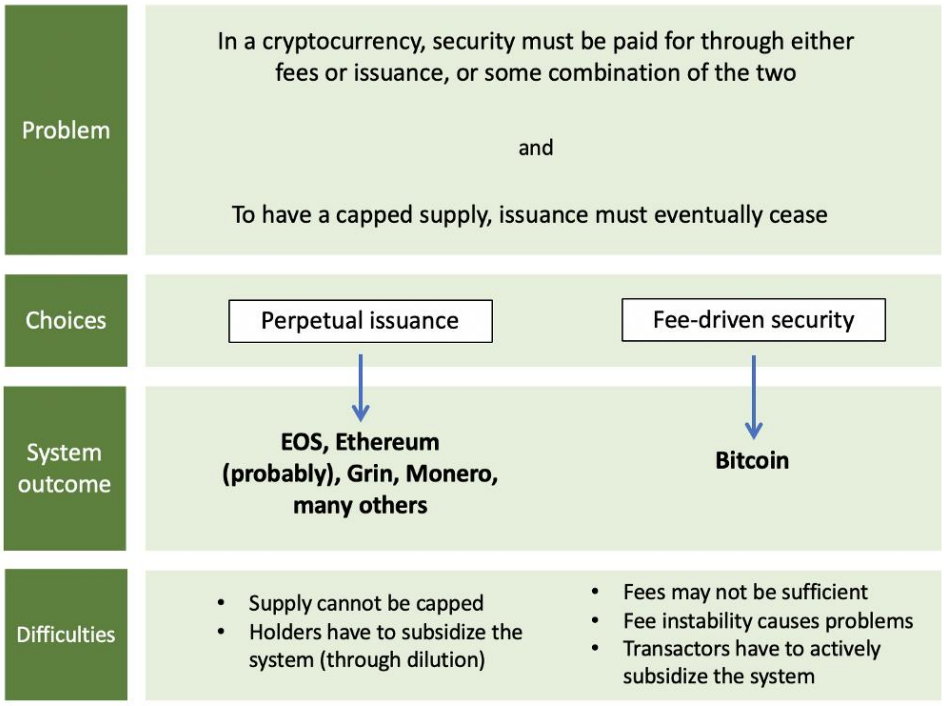
Uncapped/capped supply

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

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

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

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



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

However, Bitcoin, in typical bullet-biting fashion, selects the less palatable of the two choices — capped supply and a fee market — in order to obtain a trait its users find desirable: genuine, unimpeachable scarcity. Whether it will work is to be determined; Bitcoin will have to grow its transaction volume and

transactors will have to remain comfortable paying for block space in perpetuity. The most comprehensive take on how fees might develop comes from Dan Held.

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

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

Frequent/infrequent hard forks

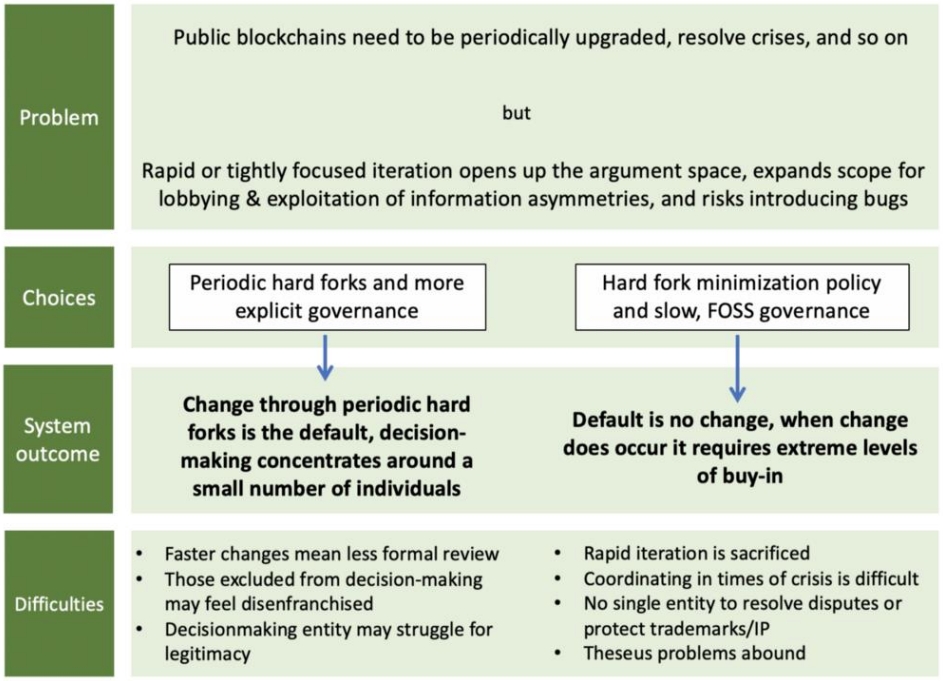
The frequency of forking among cryptocurrencies tells you a great deal about their design philosophies. For instance, Ethereum was positioned as the more innovative counterpart to Bitcoin for a long time, as it had certain advantages like a (functioning) foundation, a pot of money which could be used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

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

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

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

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



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

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

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

Discretionary/nondiscretionary monetary policy

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

Russian composer Igor Stravinsky said it well:

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

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

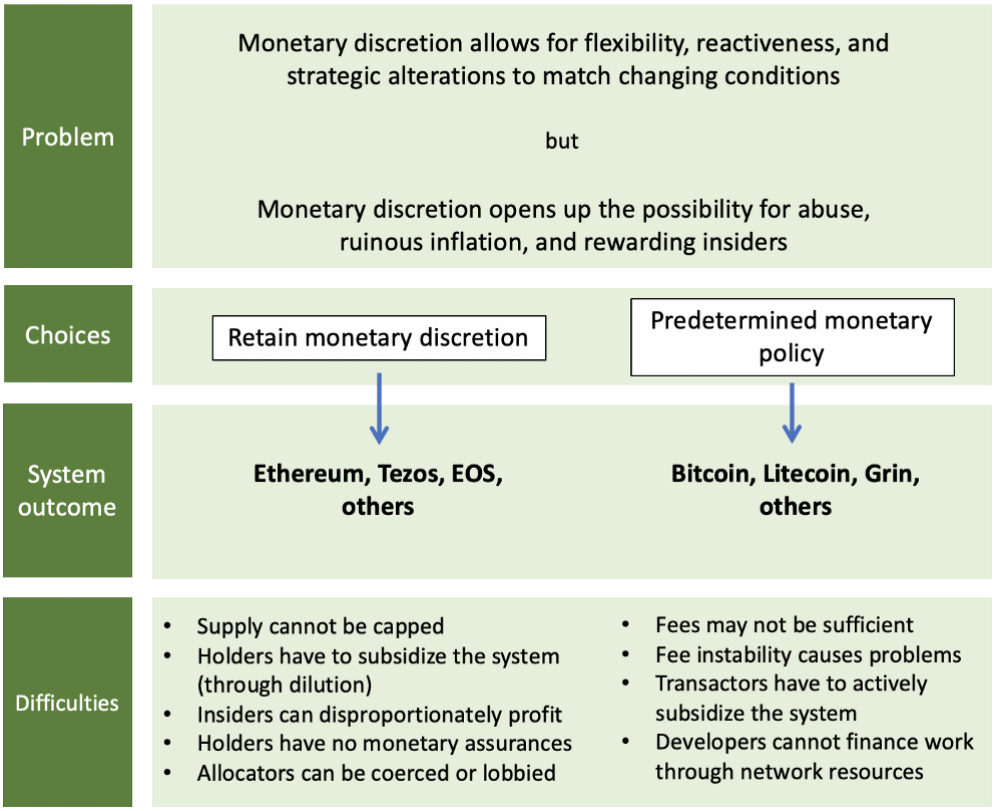
[S]carcity salience activates a constraint mindset that persists and manifests itself through reduced functional fixedness in subsequent product usage contexts (i.e., makes consumers think beyond the traditional functionality of a given product), consequently enhancing product use creativity.

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

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

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

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

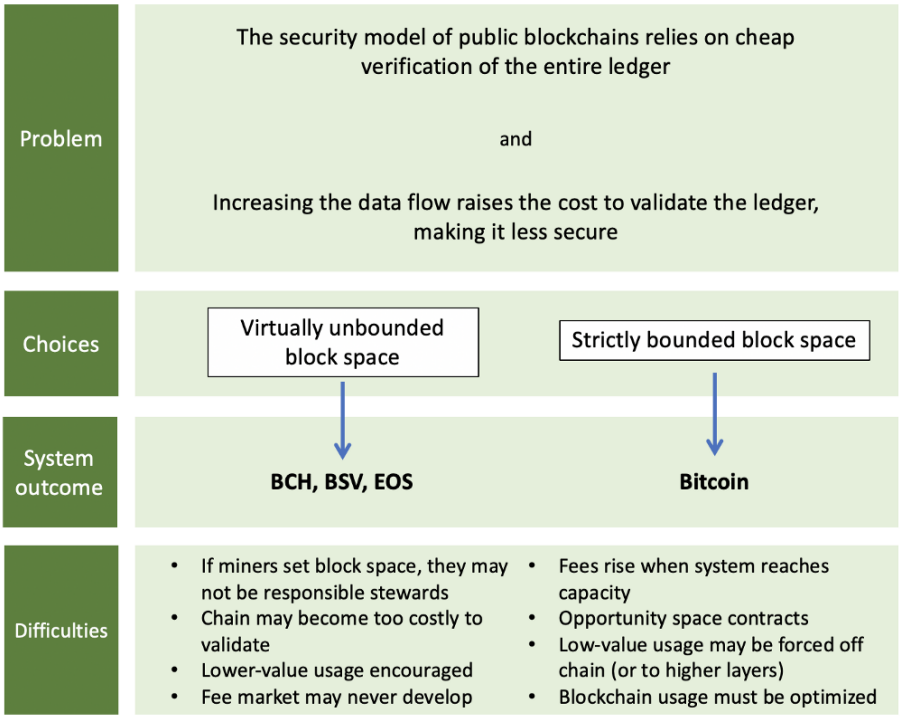


I'll note that some of the projects in the left hand column have not actually arbitrarily inflated supply to achieve policy objectives, but they have essentially written that possibility into the social contract — that supply is a lever which can be pulled if the stakes warrant it.

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

Unbounded/bounded block space

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



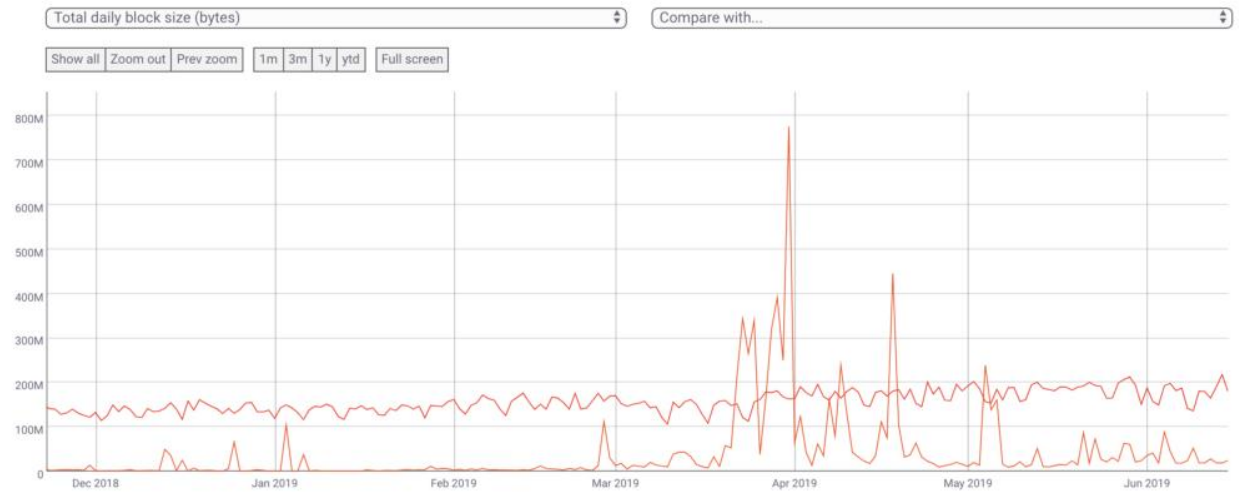
The standard proposal in forks of Bitcoin like Bitcoin Cash or BSV is that miners, not developers would set the blocksize cap — well above Bitcoin's effective ~ 2 mb cap (the 1 mb cap is a myth). However, this is problematic, as block space is an *unpriced externality*. It doesn't cost anything to a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

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

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

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

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

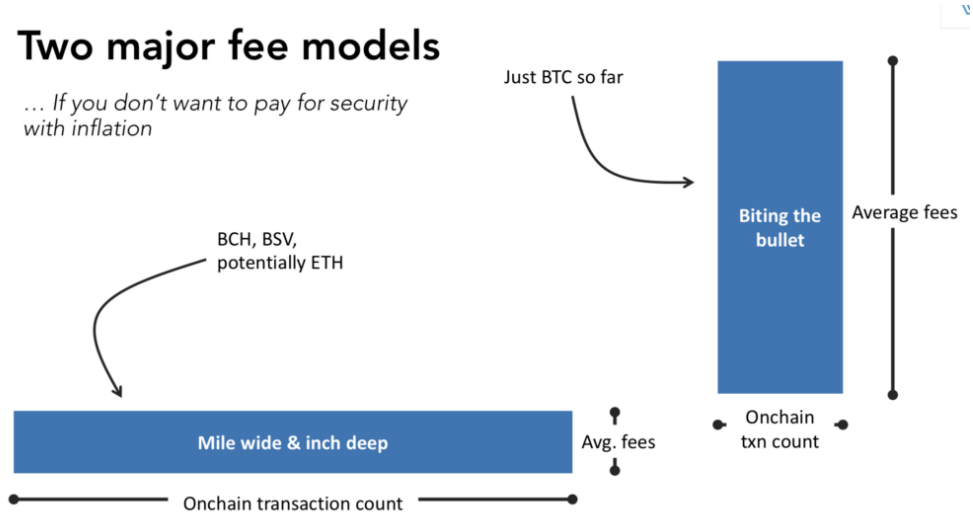


Bytes transmitted on chain per day in Bitcoin (red) vs BSV (orange). Coinmetrics

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

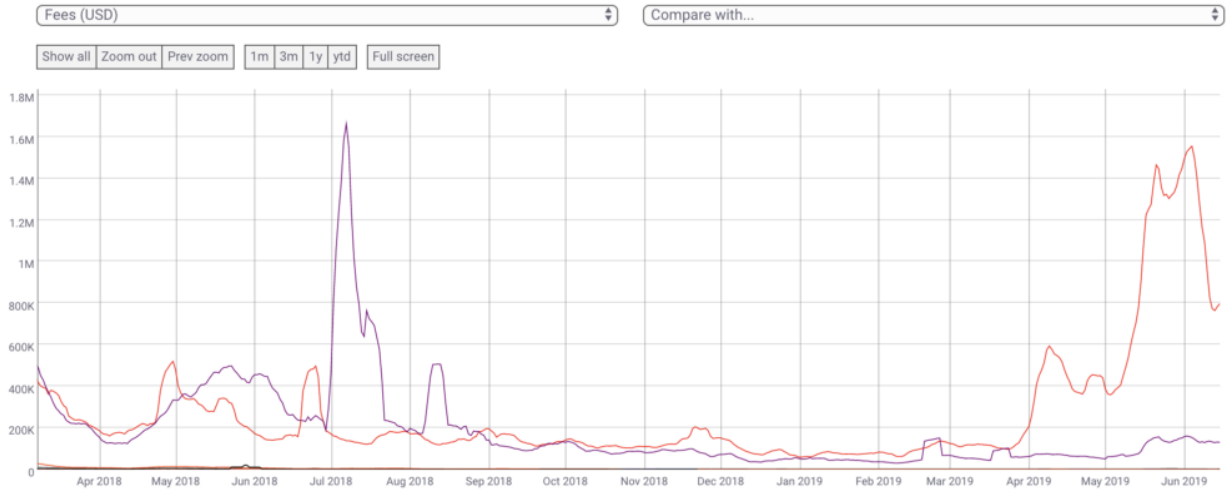
So you had millions and millions of ledger entries created through the weight of economic incentives (to promote the chain or certain dApps), burdening the chain with borderline spam. This has had very real consequences. In EOS today, for instance, it is a badly-kept secret that running a full archive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

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



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

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



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

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

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

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

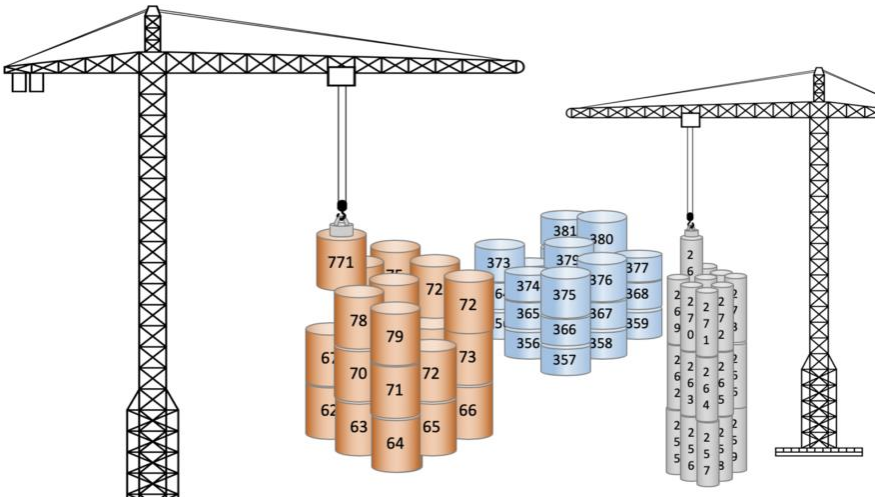
Thank you to Allen Farrington and Matt Walsh for the feedback.

It's the settlement assurances, stupid

How to evaluate blockchains

By Nic Carter

Posted July 22, 2019



It's the settlement assurances, stupid

What is the time to finality on major blockchains? How long should I wait before considering a Bitcoin transaction settled? What are the risk factors which might cause me to demand additional confirmations? How do confirmations affect settlement?

Surprisingly, none of these questions have good answers, even in 2019, over 10 years after the first Bitcoin block was mined. Rigorous investigation into the properties of proof of work has been hampered both due to a perception that it's just a temporary staging ground for some future, superior consensus/sybil resistance mechanism, and due to a belief among Bitcoiners that its quality is inviolate.

But these questions are fundamental. If you believe that public blockchains with open validator sets and distributed convergence mechanisms will persist and mediate value transfer for the foreseeable future, they are worth pondering. And if you are an exchange and your livelihood depends on correctly assessing the number of required confirmations on a variety of blockchains, these questions are critical. First, let me explain why I think settlement assurances are the primary thing worth contemplating about any public blockchain.

What's the interesting thing about Bitcoin?

This is a surprisingly difficult question to answer. Ask ten different Bitcoiners, and you'll get a dozen different responses. Disagreements about what what Bitcoin is for, its teleology, nearly tore the community asunder in the 2014–17 period. Hasu and I tried to chronicle these competing visions in a piece a while back. Others have noticed this and have covered it in detail. I particularly like Murad Mahmudov and Adam Taché's take. Daniel Krawisz covered the topic ably in 2014.

In Krawisz' piece, he posits that Bitcoin is understood very differently by two major tribes: the investors and the entrepreneurs. The investors, he posits, believe that Bitcoin is a new form of high-powered money which primarily upholds the sovereignty of the individual. The investors tend to believe that Bitcoin will

catch on because of the innate strength of its monetary properties. For them, evangelism is pointless: price is the best evangelist. The 'entrepreneurs', as he dubs them, are more interested in Bitcoin as a global payments system, and emphasize its use in commerce. As anyone who paid attention in 2015–17 knows, these two sides fought a bitter civil war over Bitcoin's *telos*(purpose) with the block size being the main battleground.

Perhaps these views can be harmonized. I tend to believe that the interesting thing about Bitcoin is its capacity to facilitate the transfer of value through a communications medium with extremely strong assurances. (I made an effort to disentangle and evaluate those assurances here.) I think that Bitcoin is a novel institutional technology— high-assurance wealth storage and transfer *without* reliance on the State or a financial system — which will unlock new modes of human organization and will enable productive commerce in places where property rights are poorly enforced.

So if the assurances you get around settlement are the most interesting thing about the system, how can we evaluate them? And how do we make consistent comparisons between Bitcoin and other systems with open validation?

Evaluating settlement

So what are settlement assurances exactly? They refer to a system's ability to grant recipients confidence that an inbound transaction will not be reversed. Wire transfers using a messaging system like SWIFT are popular in part because they are practically impossible to reverse. They are considered safe for recipients because originating banks will only release the funds if they are fully present in the sender's account.

This is why the thieves behind the $1b Bangladesh bank robberyused SWIFT and bank wires; they wanted to leverage their settlement assurances. In other words, they chose to use a system for the theft which they knew would be hard to reverse. Ultimately, $61m from that heist remains unaccounted for. Far from being evidence of a failure of SWIFT + bank transfers, this demonstrates the system's strengths. Even in this case, where virtually everyone involved wanted to reverse the transaction, they could not. The system is resistant to rollbacks, discretion, and post-hoc edits. This doesn't make it a bad system. This makes it a system that gives counterparties a good deal of reassurance that a transaction will be final.

In a similar manner, Bitcoin is a useful system because it provides users powerful settlement assurances. Just *how* good, we don't know exactly. LaurentMT wrote probably the most scientific exploration in his excellent Gravity series. Generally though, the properties of Bitcoin's PoW have not been fully explored. It has suffered a few reorgs in its history, but, as far as we know, no deliberate, adversarial reorganizations where money was stolen. And we know that miners allocate a staggering amount of real-world resources into mining transactions. This means that recipients of a Bitcoin transaction can have extremely high confidence that, once buried under a few blocks, a transaction is unlikely to be reversed.

However, this isn't the case for many competing cryptocurrencies. While they look cosmetically similar to Bitcoin in many cases, none have the same settlement assurances. This isn't necessarily because of any design flaw, but simply because Bitcoin's block space has more accumulated costliness — and hence cost to attack — per unit time, and because Bitcoin is a near-monopolist on its hash function and has dedicated hardware. Somewhat surprisingly, many weaker chains haven't been exploited, even if the cost to do so has

been low. This is likely to due to the fact that monetizing a 51% attack requires exploiting an exchange, which introduces additional complexities. And quite frankly, most smaller coins aren't worth much in the first place (and don't have any liquidity on the short side), capping the yield from an attack.

To get an idea of just how vulnerable many cryptocurrencies are, take a cursory look at crypto51.app. The methodology somewhat unrealistically assumes an attacker can rent sufficient hardware on Nicehash, but it still nicely depicts a lower bound of the cost to attack these systems.

So what are they key variables for evaluating settlement in a public blockchain system? Let's divide them into to the easily quantifiable ones and the harder-to-quantify variables.

Before we jump in, let's pause for a tiny literature review to credit some prior work in the space:

- For a much more succinct take on the matter, read Anthony Lusardi's Understanding (and Mitigating) Reorgs.
- For a comprehensive investigation into the qualities of Bitcoin's Proof of Work, see:Beyond the doomsday economics of "proof-of-work" in cryptocurrencies by Raphael Auer of the Bank for International Settlements
- For a fascinating implementation of a what a model incorporating some of these variables might look like, see A Lower Bound on Miner Rewards, by Kevin Lu of BKCM

Quantifiable settlement variables

Ledger costliness

Ledger costliness is the most profound and direct variable available to us to evaluate a blockchain's settlement guarantees. Put simply, it is equivalent to **the amount paid to validators/transaction selectors per unit of time**. In Bitcoin, miners receive a per-block subsidy and transaction fees as an incentive to stay honest and "play by the rules." In proof of work, miners attach an unforgeable proof that they have burned some energy and hence incurred a cost to each block proposed. At the time of winning a block, the miner necessarily has to have burned resources roughly equivalent to the value of the block (typically with a small margin), unless they are extraordinarily lucky. Because of this, miners are incentivized to create valid and rule-following blocks.

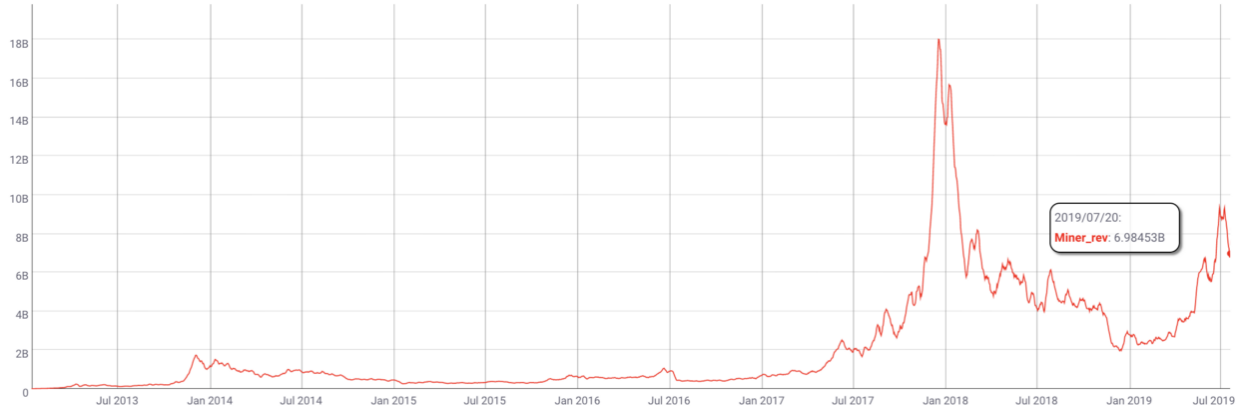
Think of it as a bit like a school project where you had to read a book and produce a book report. You need to prove to your teacher that you read the book, so you produce a book report (a valid block hash with a sufficient number of leading zeroes) which you could only have created if you actually read the book (computed sufficient hashes). Because your teacher is a stickler for style, you also have to format your book report correctly (produce a well-formed and valid block). It would be a tragedy to read the whole book, only to present a digest which is malformed and ends with you getting an F. Proof of work is the same: the work is upfront, with the payoff only coming later. You've incurred a real cost, and your business depends on you carrying out the final bureaucratic steps to collect your reward, so you do your best not to screw that part up. Recently, a miner did all the requisite work to be eligible for a block but fell at the last hurdle by creating an invalid block.

For a more complete description of how the PoW incentive works, read Hugo Nguyen's piece:

The Anatomy of Proof-of-Work Proof-of-Work (PoW) was originally invented as a measure against email spams. Only later it was adapted to be used in...bitcointechtalk.com

So why does more ledger costliness per unit time mean more security for transactors? Because a greater salary to miners (who are presumed honest) means you need a larger army of mercenaries to defeat them. These resources have to come from somewhere: you need to marshal resources and hardware capable of producing hashes, electricity, and so on. (There's an argument out there that since attackers collect the subsidy when 51% attacking, only fees provide security in PoW. I don't have the space here to engage with this fully here—for now I'll just maintain that the subsidy, especially with dedicated hardware, is itself an enormous cliff which must be scaled before 51% scenarios can be theorized.)

To sum up, outbidding the set of honest miners dutifully producing blocks on Bitcoin is very expensive. They collectively take a salary of **$6.9 billion dollars per year**right now, and many of them have presumably invested in their businesses in anticipation of future cashflows (meaning that the hardware active on the network might be even higher than current miner revenue would imply).



Annualized Bitcoin miner revenue, USD terms. Data: Coinmetrics.io

So Bitcoin is protected not only by the daily salary that the protocol pays its miners, but by the discounted rewards these miners expect to earn in the future. This means Bitcoin isn't just protected by the reality on the ground today, but miner *expectations* about rewards in the future.

We don't have an easy way to model expectations, so the easiest thing to do is to simply take the **miner salary per unit time and compare blockchains on that basis**. If you stopped reading this article now and just retained that one sentence, you would already have a better understanding of security than most people. Very few entities, even those for whom the stakes are very high like exchanges, bother benchmarking blockchains like this.

Usefully, Anthony Lusardi has already done some great expository work on the topic. He introduces the BitConf — demonstrating how many confirmations are required for one Bitcoin confirmation's worth of security on other blockchains, like Litecoin.

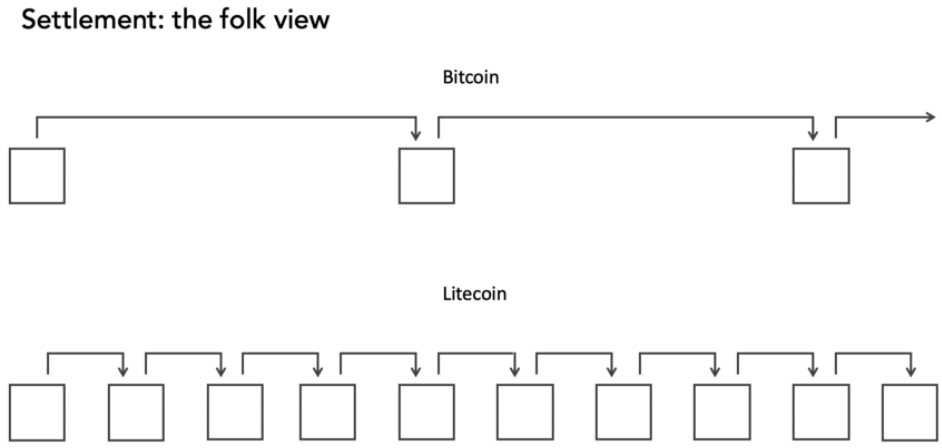
Your Exchange Needs More Confirmations: The BitConf Measure In cryptocurrency we regularly advise against accepting zero-conf transactions but are entirely happy to accept...medium.com

Suffice to say, most people do not use BitConfs, or try to index settlement to work done. Quite the contrary, the 'folk theory' of settlement holds that settlement is a linear function of the number of confirmations. This is sadly a very common view. Even the Litecoin Foundation website implicitly makes this claim:

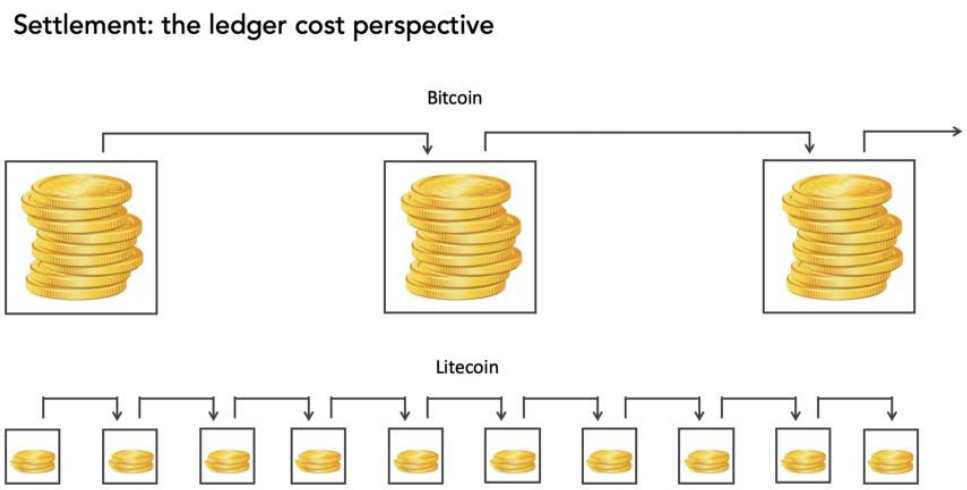
Litecoin transactions are confirmed faster than other cryptocurrencies like Bitcoin because it generates a block every 2.5 minutes as opposed to Bitcoin's 10 minutes. This means your money gets to its destination quicker.

The initial moment when a transaction is plucked out of the mempool and included in the chain is indeed reliably faster in Litecoin, but in cryptocurrency probabilistic settlement must be contemplated. In other words, if you only care about the first confirmation, then Litecoin is "faster", but the moment you start to care about longer term settlement (over multiple confirmations), it becomes clear that it is much slower.

If you believe that Litecoin and Bitcoin confirmations confer the same amount of settlement guarantees, then you might depict settlement as follows, with Bitcoin apparently slower:

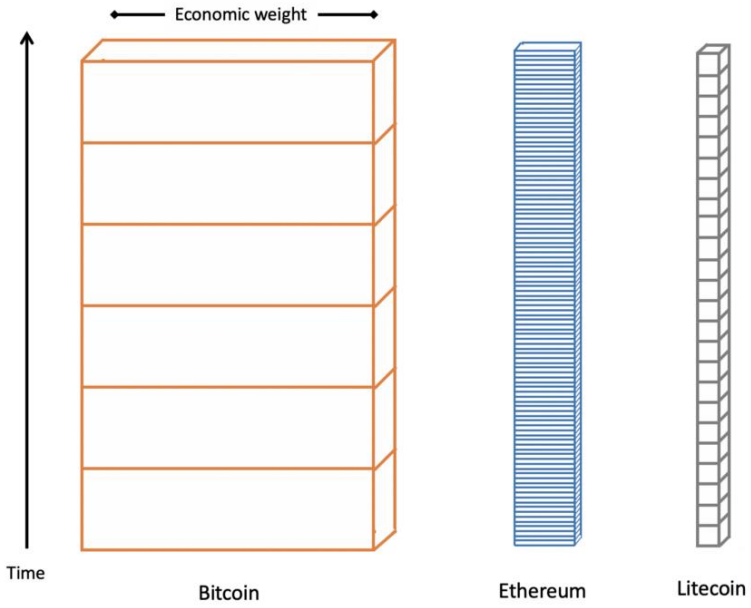


But this is mistaken. Litecoin has more blocks per unit of time, but it accumulates ledger costliness much more slowly. In reality, Bitcoin pays its private army of miners far better, and as a consequence, they produce far more security per minute in the form of hashes.



Bitcoin blocks are 'heavier' with accumulated cost than Litecoin blocks are. Even if Litecoin had a 10 minute block-time, a Bitcoin block would still be worth 14.5 times more than its Litecoin equivalent. Confirmations don't really matter. The opportunity cost incurred by miners per unit of time does.

You could alternatively visualize ledger costliness as blocks getting piled on top of their predecessors, with transactions getting more and more final as they are buried deeper and deeper in the pile of blocks.



Block width is roughly proportional to the relative security spend of each blockchain

As more and more blocks get added to the heap, it becomes more and more implausible that they would be reverted, and transactions become more final. In this graphic I've scaled the width of blocks to the relative ledger cost incurred, and depicted the granularity of blocks.

The point here is that settlement in a blockchain system is a flow. Block time is largely irrelevant. Ethereum has many more blocks per hour than Bitcoin does, but settlement should be compared between the two based on ledger cost, rather than number of confirmations.

Yield from reversal: transaction size

Ledger costliness isn't the only thing that matters in settlement. Also important is the incentive someone might have to try to reverse a transaction. The purest codification of this incentive is simply the size of the transaction. If you are a recipient of a 50,000 BTC transaction, you might wait more than the six block rule of thumb out of an abundance of caution. If you are receiving 1000 sats, one confirmation is likely sufficient. In short, transactions have more or less perceived settledness based on the stakes at hand.

Elaine Ou formalized this concept in a fantastic Bloomberg article, arguing that recipients should wait **until the transaction's value and ledger costliness match** to consider a transaction settled.

Elaine's formulation handily conjoins two of the most important quantitative variables in blockchain settlement: ledger cost and yield from reversal. If you wanted to settle a $10m inbound transaction in BTC, according to this rule, you'd wait 60 blocks, or 10 hours. (It's a neat coincidence that at a price of $13,330 Bitcoin accumulates ledger costliness at a rate of exactly $1m/hour). Henceforth, I'll refer to this simple formula as the **Ou Rule**.

Now that we have the two most critical settlement variables enumerated, let's put down some numbers and compare the major PoW networks.

	Daily miner revenue (7 dma)	Miner revenue per 10 mins	Days to settle $1m (Ou rule)	BTC finality multiplier
Bitcoin	$ 23,972,000	$ 166,472	0.04	1
Ethereum	$ 4,159,000	$ 28,882	0.24	5.8
Litecoin	$ 1,655,000	$ 11,493	0.60	14.5
Zcash	$ 718,734	$ 4,991	1.39	33.4
Bitcoin Cash	$ 711,419	$ 4,940	1.41	33.7
Bitcoin SV	$ 346,040	$ 2,403	2.89	69.3
Dash	$ 262,325	$ 1,822	3.81	91.4
Ethereum Classic	$ 188,818	$ 1,311	5.30	127.0
Monero	$ 179,670	$ 1,248	5.57	133.4
Bitcoin Gold	$ 49,087	$ 341	20.4	488.4
Dogecoin*	$ 48,396	$ 336	20.7	495.3
Verge	$ 13,800	$ 96	72.5	1,737.1
Vertcoin	$ 6,503	$ 45	153.8	3,686.3

* = Dogecoin is merge mined with Litecoin

Numbers as of 07/15/2019. Data: Coinmetrics.io

Needless to say, Bitcoin is by far the fastest-settling blockchain (just including these two variables and none of the other salient ones). Settling even a $1m inbound transaction can be extremely slow on many blockchains. Aside from Bitcoin, Ethereum, and Litecoin, it takes over a day for every other decentralized ledger (I'm not including Ripple and Stellar in these examples because they don't have meaningfully decentralized validation). Smaller chains simply do not have enough miner reward to make settlement suitably quick.

Luke Childs' Howmanyconfs offers a dynamically updated version of parts of this table:

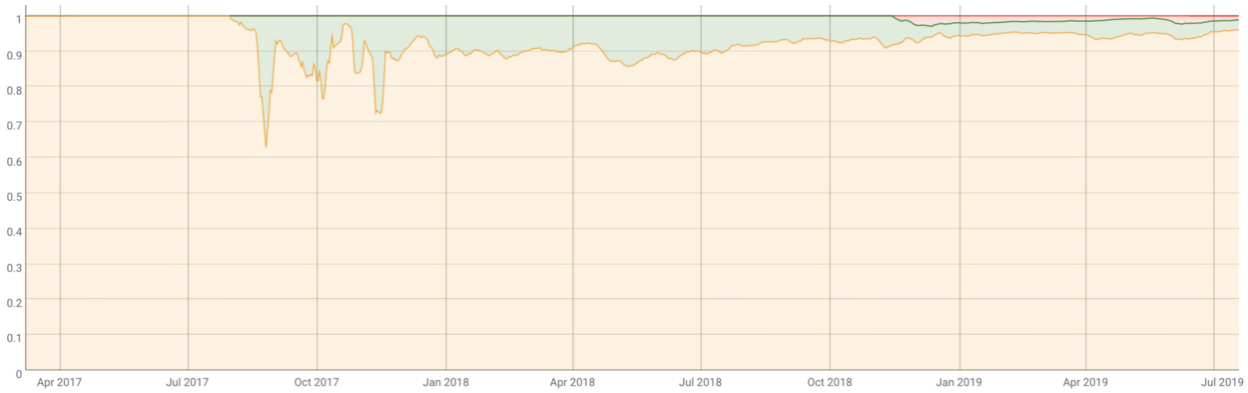
How Many Confs? How many confirmations are equivalent to 6 Bitcoin confirmations? howmanyconfs.com

It's also worth calling attention to the fact that Bitcoin Cash and Bitcoin SV settle transactions 33 and 69 times more slowly than Bitcoin, respectively. While they are functionally identical to Bitcoin in most respects, because they offer miners less of a bounty, they are vastly slower. This directly contrasts with their common positioning as "faster" blockchains.

This is also an interesting case study in how Bitcoin resists duplication. You can create something which looks cosmetically similar to Bitcoin, but you cannot replicate the settlement assurances which derive from the costliness of the ledger. Miners obey economic reality and cannot be cajoled to lend their support to a protocol which doesn't pay them well enough. In fact, as we will learn, Bitcoin Cash and Bitcoin SV are even worse off that this table suggests, because of a third variable.

Monopolist on its own hash function

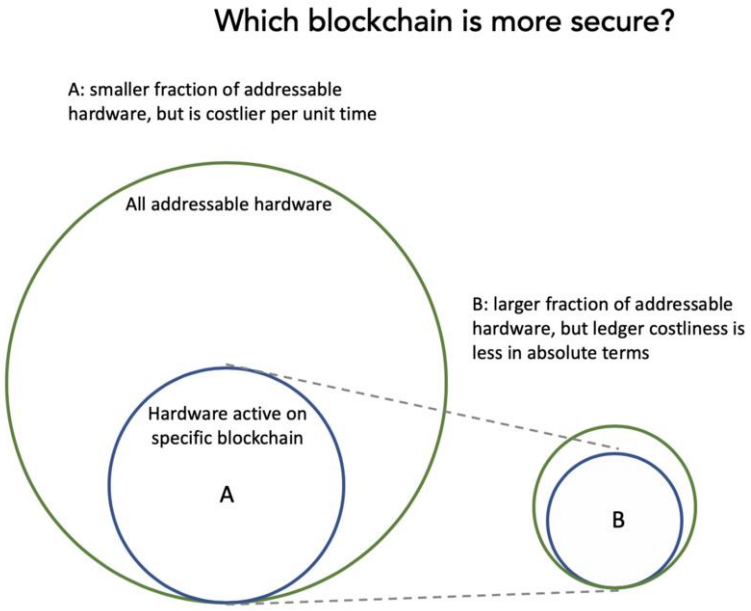
So far, I haven't mentioned a third critical variable which directly affects the settlement guarantees of a given blockchain: whether or not it holds an effective monopoly over the hardware which is addressable to its hash function. As I implied above, Bitcoin Cash and Bitcoin SV are at a massive disadvantage relative to Bitcoin because they have a minute fraction of all the SHA-256 ASICs. What this means is that even a mid-size or small pool mining Bitcoin could temporarily redirect its hashpower to one of Bitcoin's smaller forks and 51% attack it at will.



Relative share of miner revenue; BTC (orange), BCH (green), BSV (red). Coinmetrics.io

The fact that these blockchains have not been attacked yet is not evidence of their security. It may well be the case that there are no miners on Bitcoin willing to maliciously interfere with either minority fork today — but depending on the goodwill of miners makes for an extremely tenuous security model. Since this risk is ever-present, it could be posited that neither blockchain ever reaches effective finality, regardless of the number of confirmations. This is because there are ample mining pools on Bitcoin which could create a 100+ deep reorganization in BSV for instance without too much difficulty.

This variable introduces more complexity into the analysis. It is not the case that more hashrate means that a blockchain is more secure; it must also occupy a large fraction of the addressable hardware.



In this example, I'd characterize blockchain A as less secure than B, even though it has more ledger costliness in absolute terms, because it is theoretically easier to marshal enough hardware to attack A.

So consider this variable to be a boolean; if the blockchain is a monopolist on its own hardware the analysis is straightforward. If it is in the unfortunate position of splitting hardware with one or many other blockchains, and retains a minority share of that hash-function-specific hardware, it is likely fundamentally unsafe. But it's hard to determine just how unsafe it is; the risk of an attack is a function of the attackers ability to amass sufficient electricity and hardware.

Less quantifiable settlement variables

The three variables mentioned above aren't exhaustive, but simply the easiest to quantify. With those, you could probably build a plausible model which is superior than those used by many exchanges today. But there are many more factors to consider.

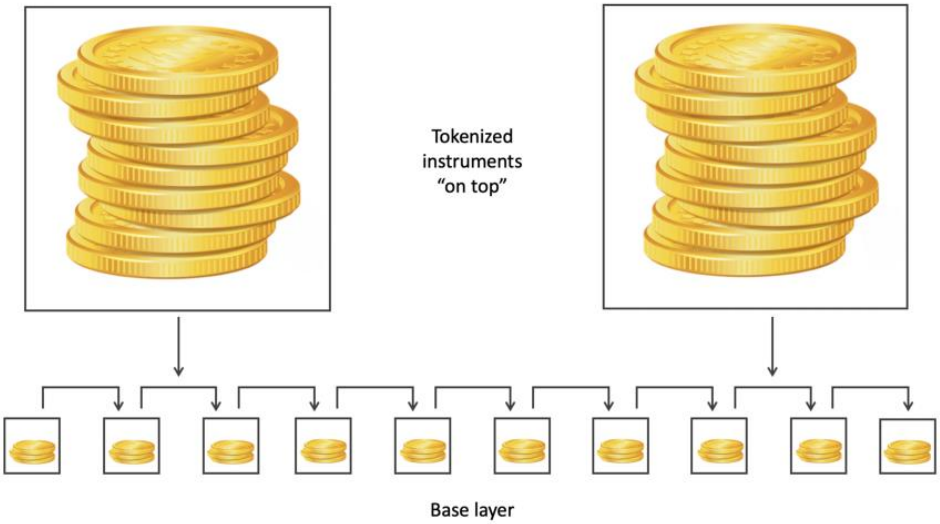
Yield from reversal: goldfinger attacks

Goldfinger attacks take their name from the Bond film in which the villain plans to irradiates all the gold in Fort Knox, making all of *his* gold more valuable. The term describes a class of attacks where the attacker is motivated by some extra-protocol financial interest. Joseph Bonneau more scientifically describes themas attacks where the "attackers [have] an extrinsic motivation to disrupt the consensus process."

The risk of these attacks is virtually impossible to quantify, since attackers have a variety of different motivations, and they tend not to disclose them *a priori* (before an attack). Here I'll give two further examples where the yield from reversal dramatically increases, rendering settlement guarantees less certain.

Top Heaviness

This refers to the condition in which a large number of financial significant assets are created as tokens *on top* of some base layer protocol — for instance Omni assets on Bitcoin or ERC20s on Ethereum. As these tokens inherit their security from and are wholly dependent on the base layer, they are vulnerable to attacks on the underlying chain.



As the asymmetry develops between the value of the instruments on top and the cost to attack the base layer, the top heaviness problem starts to manifest. If the asymmetry becomes large enough, an attacker might seek to take out a short on some instrument on the top layer and simultaneously attack the base layer, either by mining empty blocks and DOSing the tokens in question, or creating reorgs and confusion.

We have real world examples of the consequences of top-heavy systems. Attackers have recently made a habit of attacking the underlying index which sets the price for derivatives on Bitmex. Since there's a big asymmetry between the collateral present on Bitmex (the top) and the underlying reference market (the bottom), it's lucrative to burn funds market-selling on Bitstamp because the attacker can monetize by causing an outsize move on Bitmex as margin positions are liquidated.

I don't believe any blockchain faces this problem today, but as more instruments are tokenized and inserted on top of blockchains the returns from attacking the base layer will increase.

Liquid derivatives markets

This is rather straightforward. Derivatives, options in particular, give financial market participants the ability to obtain leverage and magnify their returns even relative to a small move in the underlying. As with the top heaviness condition, the risk to the blockchain comes when a significant asymmetry exists between the cost to mount an attack and the returns from an attack.

The creation of liquid derivatives markets enables attackers to magnify their returns from predicting price action; and if they can induce a drop in the price of the asset by mounting an attack, the settlement

guarantees of the chain are potentially at risk. As the return from an attack grows, so does the amount of resources that an attacker is willing to contribute to an attack. So the creation of leverage on the short side potentially impairs a blockchain's settlement assurances. But due to the heterogeneity of actors and uncertainty about the ability to monetize such an attack, it's impossible to quantify this risk and add an appropriate security discount.

Of course, one counterbalancing factor here is the potential unwillingness of an exchange to pay out on a successful bet if they suspect that the trader in question was coordinating with an attacker to interfere with the blockchain.

Additional hardware considerations

Implicit in the earlier point on hash function-specific hardware is the well-documented notion that GPU-mined coins *cannot ever* be monopolists on their hardware because there are so many GPUs in the world (thanks to gaming and other non-cryptocurrency applications). I won't belabor this point: David Vorick has cleanly laid out the case for why GPU-mined chains are fundamentally at risk, and why long term incentive-alignment (in the form of ASICs) is so critical.

Choosing ASICs for Sia We recently announced that we would be manufacturing and selling ASICs for Sia, an announcement that received a lot...blog.sia.tech

Thus GPU-mined coins should always be assessed additional confirmations. It's hard to know exactly what the ratio should be for one GPU-mined unit of ledger costliness to an ASIC-mined unit. But there absolutely should be a discount for GPU-produced security. It's simply too easy to acquire hardware to mine a GPU-mined chain.

Case study: Kraken's confirmation requirements

Startlingly, from my conversations with exchanges, who have a lot to lose from miscalibrated rules around settlement, it appears to me that they tend to give little thought to confirmation rules. I couldn't find much detail on how many inbound confirmations exchanges reserve until a transaction is considered settled. Helpfully, Kraken have made their criteria freely available.

I decided to benchmark Kraken's confirmation requirements against what a naive implementation of Lusardi's BitConf would look like — simply requiring that all chains provide the equivalent of six confirmations on Bitcoin.

	Block time (mins)	Kraken confs required	Bitcoin 6-conf equivalent confs	Kraken settlement time, mins	BTC equiv. single conf time, mins	Confs for $100,000 worth of security
Augur	0.22	30	173	6.5	346	160
Ethereum	0.22	30	173	6.5	346	160
Gnosis	0.22	30	173	6.5	346	160
Melon	0.22	30	173	6.5	346	160
Dash	2.50	6	548	15	5,483	220
Dogecoin	1.04	20	290	21	869	84
Ethereum Classic*	0.24	120	15,235	28	7,617	3,245
Litecoin	2.50	12	174	30	869	35
Monero	2.00	15	2,001	30	8,005	401
Tezos	1.03	30	5,230	31	10,461	1,013
QTUM	2.00	24	67,036	48	167,589	8,389
Bitcoin	10.00	6	6	60	60	0.6
Tether (Omni)	10.00	6	6	60	60	0.6
Zcash	2.50	24	800	60	2,001	80
Bitcoin cash	10.00	15	505	150	2,022	20

*Deposits are halted

Source: Kraken Deposit Processing Times, Coin Metrics estimates

The results are startling. Depending on how you put it, Kraken makes either extremely stringent demands of Bitcoin transactions, or extremely loose demands of non-Bitcoin chains. While Kraken asks for six Bitcoin confirmations to consider deposits settled, they ask a mere 12 of Litecoin (where the equivalent in Bitcoin security terms would be 174), 30 for Ethereum (Bitcoin equivalent: 173), and 15 for Monero (where Bitcoin-indexed security would demand 2000).

My guess is that six confirmations is massive overkill for Bitcoin, making Kraken's lesser settlement demands of other chains more reasonable. Still — when the ledger costliness variable is consistently applied, the results are occasionally comical. QTUM, for instance, if held to the same standard as Bitcoin, would need 67,000 confirmations, equivalent to a wait of 115 days. (QTUM may well have some alternative settlement mode I'm not familiar with: I computed the numbers simply based on the payouts it makes to validators).

Of course, this is a very naive implementation of the model. A more sophisticated version would include higher security demands for non-monopolist chains, GPU-mined coins, large inbound transactions, and so on. I would encourage exchanges like Kraken to consider a systematic ruleset for inbound transactions, if they don't already. Whatever the particular formula chosen, it would likely suggest fewer confirmations for Bitcoin and more for smaller chains.

Some takeaways

What's the practical significance of all this? Well as we continue to await the formalization of these variables into a model that makes sense and is directly applicable to everyday usage of cryptocurrency, here are a few takeaways:

I. Block time is arbitrary, and changes little

The only thing that a lower blocktime alters is reducing variance in the time to the initial confirmation. If you are impatient, you probably prefer a blockchain with a 2.5-minute blocktime, but this doesn't mean that settlement is any "faster". Ledger costliness still accrues at the same rate, being a function of issuance and unit value per coin.

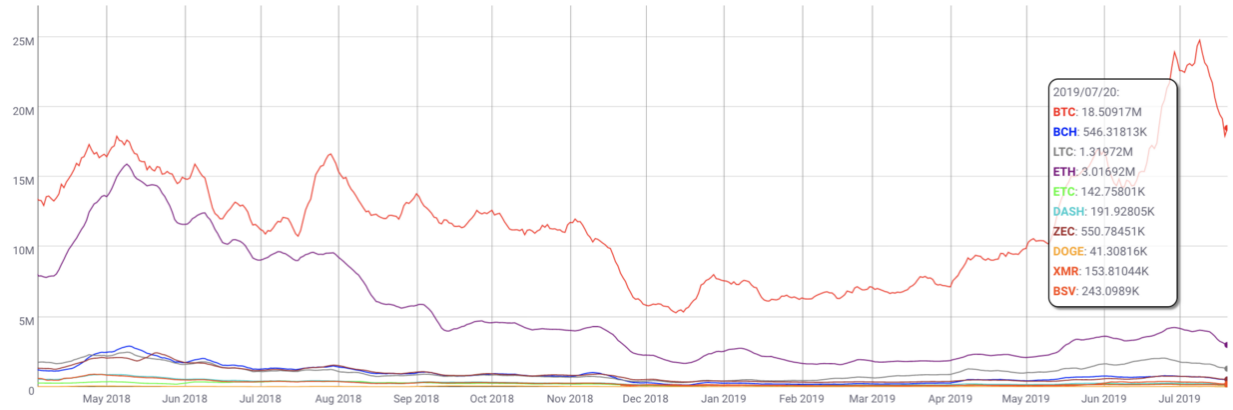
Indeed, Bitcoin could reduce its block size by 25% and switch to a 2.5 minute blocktime and virtually no one would notice the difference. The system would be functionally identical — the six block rule of thumb

would become a 24 block rule of thumb. Satoshi opted for 10 minute blocks because he did not know how well the system would be able to come to convergence. Latency and large blocks interfere with validation, and make convergence among nodes more difficult. A healthy 10-minute blocktime gives the system plenty of breathing room — and also gives us an indication of what kind of a system Satoshi was envisioning (hint: not suited for in-person, petty cash payments).

It's true that the first confirmation matters some small amount, since your transaction cannot start to be buried under the weight of subsequent blocks until it is included in a mined block. Additionally, a lower blocktime reduces variance in variables like daily issuance. However, aside from that, blocktime is completely arbitrary. The security spend per unit of time, in addition to the *quality* of that ledger costliness, is what matters for settlement. A lower blocktime just means that you're chopping up that security flow into smaller bits. It doesn't make final settlement any faster.

II. Bitcoin is either providing massive security overkill, or other blockchains are critically at risk

This is the clearest takeaway from the various benchmarking exercises I did for this article. If you measure blockchains purely based on the salary paid to transaction selectors (miners and validators) per unit of time, for the most part, they look devastatingly weak compared to Bitcoin. Just have a look at this chart. Aside from Bitcoin, Ethereum, and Litecoin, virtually nothing is visible on the chart, because their security spend is so minimal.



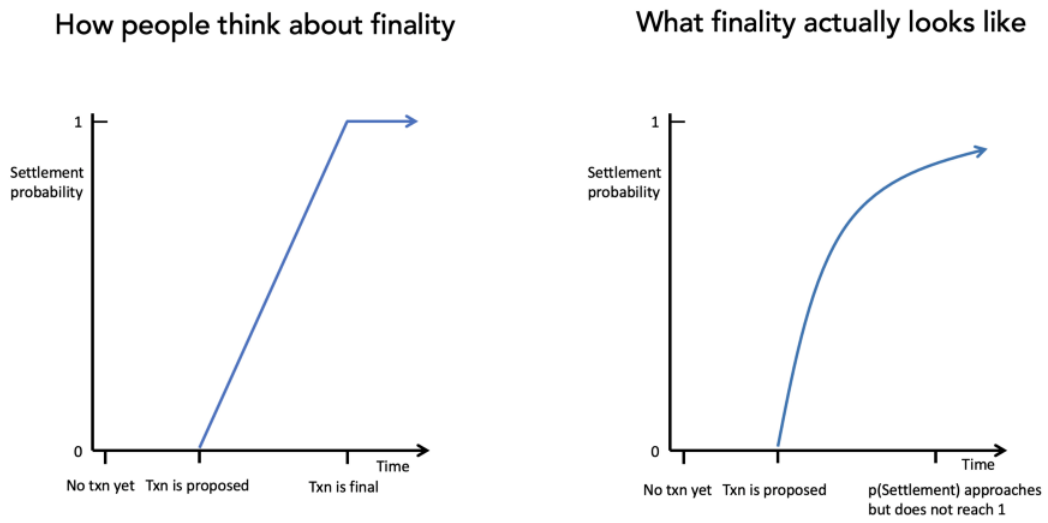
Daily USD miner revenue, smoothed (7dma). Coinmetrics.io

This isn't necessarily fatal. It could be the case that Bitcoin is way overpaying for security, for instance, and that proof of work is 'better' than we think. This is actually my current view — that due to the current subsidy conjoined with the high unit value of Bitcoin, Bitcoin is probably spending "too much" on security. But it does wrap the protocol in a warm blanket which gives it a good degree of protection as it enters its teenage years.

So this data is not necessarily apocalyptic for smaller blockchains. After all, even though Satoshi ordained the six-block rule of thumb, it could be the case that for most transactions 1 or 2 blocks are sufficient. This would lessen the heavy load placed on other blockchains trying to match Bitcoin's security spend.

III. Settlement is always probabilistic

I will admit that I chafe a little bit when new blockchains tout their 'absolute finality'. The only way to truly have finality is to have an organization vouch for transactions, effectively endorsing them. But when this happens, authorities that might have an interest in reversing transactions (say if they suspect they are related to criminal activity) will typically ask that entity to facilitate the rollback, poking a hole in the perceived finality.



Take the example of EOS. EOS has a concept called the Last Irreversible Block which, according to EOS Canada,

[M]eans that you can trust with 100% confidence that that transaction is final, fully confirmed, and immutable. If the block number of a block is lower than the Last Irreversible Block, that means it is considered final.

According to EOS Network Monitor, the current Last Irreversible Block is trailing the chaintip by 330 blocks, equivalent to about 2 minutes and 40 seconds. All together, this makes EOS' claimed time to finality very short.

Except there's a catch. EOS has (had?) a bureaucratic process through which individuals could appeal to the 'EOS Core Arbitration Forum' and ask for funds from suspected thefts to be frozen and returned to the victims, effectively reversing long-settled transactions. One batch of these reversals took place in June 2018. This was possible because there were only 21 entities (the block producers) tasked with processing transactions, and all were known to the leadership and hence accountable.

While many onlookers cheered the return of stolen funds, from a settlement perspective this undoes the qualities that transactors seek when they use a blockchain. In practice, any mechanism which can reverse settlement can be abused. The reason credit cards embed a fee into transactions is because chargeback fraud is rampant.

Imagine a sophisticated scam where someone sold EOS for fiat in a p2p transaction, and then appealed the transaction to the ECAF, and managed to get the EOS in the transaction returned to him under the guise of having been scammed. These are the kind of schemes that result from administrative exceptions to finality.

There are any number of examples I could give on this topic, but I'll stick with one for now. In practice, many of the blockchains that claim to have full and effective finality also insert the capacity to create discretionary rollbacks and account freezes into their systems. You still have to consider the probability of a reversal, even if it's not explicitly codified.

IV. By being open about its security model, Bitcoin's PoW is usefully transparent

Echoing Elaine Ou once again, one of the most useful features of Bitcoin's security model is how transparent and easily apprehensible it is. The precise guarantees are not easy to determine ("how many confs to settle $1b?") but the resources being spent to backstop the system are. At any point, an onlooker can trivially determine how many hashes, and by rough extension, how much energy, it would take to overpower the system. For years now, it has been clear that no entity outside the most potent state actors could muster sufficient resources to outweigh the honest majority.

By contrast, other blockchains seek security through obscurity, security through complexity, or through untransparent institutional modes of finality. Verge, for instance, conjoined five different hash functions in its exotic proof of work model, and that was ultimately its downfall. An attacker realized they could perform a 'time warp attack' by targeting just one of the hash functions and lowering difficulty to 1. Far from providing extra security, the insertion of more complexity into the system introduced new attack vectors.

Summing up

If there's anything I could have you take away from this piece, it's the following. Instead of viewing settlement as a function of some preconceived number of confirmations, think of settling a transaction in a proof of work system as the process of wood petrifying slowly. It happens at a given rate and can't be accelerated. The rate is determined by the variables enumerated above: chiefly, ledger costliness, transaction size, and the availability of addressable hardware. Once completed, the wood has been replaced by minerals and is rock solid, no longer soft and malleable. The features of the wood are forever frozen in time.

Similarly, as Nick Szabo has said, blockchains are computational amber. Amber starts life as tree sap, only later becoming hardened, in the process storing bits of information (insect DNA and so on) within it. The essential process of burying past changes to the ledger under unforgeable cost, provided by proof of cost incurred, provides the same slow-moving settlement assurances. As more blocks accumulate, the gravity of the blockchain exerts itself, and makes distant rewrites colossally expensive and unwieldy.

The bounty available to miners — and hence the cost incurred — is a function of issuance, unit price, and fees. None of these aside from issuance can be directly programmed. And a high issuance alone cannot guarantee security, as investors have to buy into the chain's prospects and backstop its value. In this sense, strong settlement assurances in a proof of work system cannot be planned for, they can only emerge. Whether you find this to be a dismal conclusion or not is up to you.

In this article, I tried to enumerate the variables which I believe are most critical for evaluating the settlement assurances of blockchains, especially those built on proof of work. But you'll notice I provide no formal model nor a recommended solution to the problem. Many of these variables cannot be easily quantified and there are likely some which I am leaving out. A more comprehensive — or implementation-focused — model I will leave to subsequent authors.

If we ignore these questions, they will be forced upon us through necessity. As short-side liquidity emerges for a larger share of the market, whole new classes of attacks will open up and exchanges will find themselves targeted more and more. Equally, as major custodians and clearinghouses start to take cryptocurrency deposits totaling hundreds of millions or billions, they will need to devise formal rules for what constitutes settlement. They would do well to think deeply about the security of the blockchains that they are reliant on.

Thanks to Anthony Lusardi, Hugo Nguyen, and Matt Walsh.

A most peaceful revolution

By Nic Carter

Posted September 7, 2019

Art by Jason Benjamin (@perfecthue)

People should not be afraid of their governments. Governments should be afraid of their people.

– V, V for Vendetta

It's submission," Rediger murmured. "The shocking and simple idea, which had never been so forcefully expressed, that the summit of human happiness resides in the most absolute submission.

— Michel Houellebecq, Soumission

Make no mistake, Bitcoiners are revolutionaries

Libertarians had it all wrong. They sought to shrink the State's influence by participating in the democratic process. This has been and remains a hopeless, Sisyphean task. Like Tolkien's Ungoliant, the State hungers without limit, and its most engaged constituents duly reward it with votes for more growth, receiving in exchange ever-greater entitlements. Libertarians are, in a word, stuffed. Like the creeping gelatinous menace in The Blob, the State grows regardless of what you throw at it. Participating in

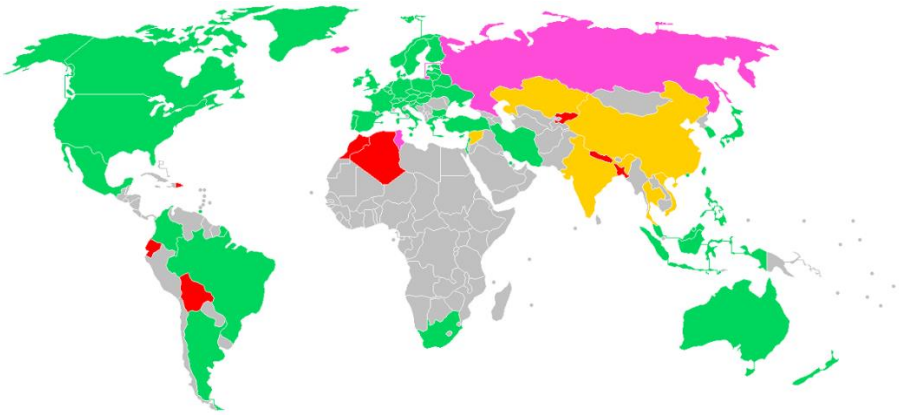
democratic processes empowers it and entrenches the Orderly Civic Ritual as the only legitimate mode of political engagement.

Bitcoiners reject this: they understand that the only winning move in politics is not to play.

Instead, they kicked over the chessboard and strutted around as if they had won. Bitcoiners chose to abandon the rules of engagement and began work on a monetary system totally outside the purview and supervision of the State, entirely without restriction. Ultimately, they anticipate a system which permits unfettered commerce, provable-reserve free banking (unlike the obscure socialized-loss mess we rely on), renders capital controls obsolete, frees savers from state-sanctioned theft by inflation, and eventually disempowers the State entirely, shrinking its monetary toolkit.

This proposition predictably enraged the State-dependent intelligentsia, the pundit class, and the press, which has backslid from its Fourth Estate perch as a proud critic to a feeble establishment mouthpiece. No surprise at all that Bitcoin's most hysterical critics overwhelmingly benefit from their proximity to or membership in the Beltway bureaucracy or the overseas equivalent. Academics, the beneficiaries of a rampant government-guaranteed student loan bubble; politicians and ex-politicians, who time and time again manage to turn their political clout into personal wealth (how curious!); journalists, reduced to meekly passing on State messaging in a futile effort to build a moat against insurgent media startups and Youtubers with 1000x their clout; economists, forced to peddle Keynesian narratives for grants and tenure.

Thus, met with the screeching bile of the chattering classes, Bitcoiners went from utopian tinkerers to dissidents in short order — even as the movement was still in its infancy. Check the financial pages of your newspaper of record; you will find nothing but derision and mockery (and the very occasional nod of grudging acceptance). This is for an asset class which went from 0 to $200 billion in a decade, with no venture backing, no IPO, no corporate entity, an absent founder, and a purely open-source body of maintainers. In the U.S., the government saw fit to give Ross Ulbricht two non-parole-eligible life sentences plus 40 years for the crime of creating a free market denominated in Bitcoin. China has banned the formal exchange of bitcoins; India is mulling over legislation to make mere ownership illegal.



Legality of Bitcoin — Green: permissive; Orange: some restrictions; Pink: contentious; Red: Hostile. (Source)

We aren't in the prelude to war; we are living it. Of course, war doesn't look much like the savage romps of yore. But this has been the case for a long time. Gone are the days where men nobly lined up in front of each other and fired until one side ran out of able bodies. We no longer scramble out of the trenches at the sound of a whistle to the chatter of machine guns. Open warfare is virtually obsolete. Instead, contemporary conflict consists of a melange of insurgencies, IEDs, sanctions, emotionless drone strikes, and strategic infrastructure targeting through operations like Stuxnet. Since conventional warfare has migrated to the virtual, why not rebellion, too?

And it is a rebellion, make no mistake. Cryptocurrency, despite the earnest protests of some of its lily-livered adherents, remains manifestly independent and ultimately hostile to the State. It cannot be regulated, captured, or rendered compliant. The Silk Road was not an aberration or historical anecdote to uneasily chuckle over in hindsight. It was a profound demonstration of Bitcoin's superior purpose and utter indifference to the shackles burdening the financial system. The current State, in its bloated and rapacious form, craves not only your corporeal submission, but it demands an endless torrent of metadata and analytics too. Your finances are not your own; they are scrutinized and require approval at every step. If you operate even slightly outside of the mainstream, you risk getting your savings confiscated with no recourse. Those armored personnel carriers aren't going to pay for themselves.

Cryptocurrency tilts at the State

Rare image of Bitcoin in physical form

Just as sixteenth century Protestants began to question the official doctrine of indulgences and the scope of the Pope's authority, so too came to wonder a ragged bunch of nerds and cypherpunks: is inflation really necessary? In a free market economy, should central banks really have the right to arbitrarily set the price of money? Should the State really have full discretion over one's saving and spending? Should savers really be forced to trust banks (and ultimately, the taxpayer) to redeem and honor their savings? What does an entry in a bank's database really mean?

Genuine cryptocurrencies — alternative monetary systems, really — threaten the State and its hangers-on. Bitcoin is absolutely profane, so much so that it hardly bears contemplation. It challenges the State's most treasured privilege: its ability to finance itself through inflation and seignorage.

Cryptocurrency, chiefly Bitcoin so far, has already begun to affect central bank policy. I am not exaggerating when I stress its geopolitical significance. Combine a free market for money with the distribution rails of the internet and you get a very toxic stew. Let's consider a few ways that cryptocurrency has begun to affect the state.

First off, as noted by Gina Pieters (2016), the existence of liquid Bitcoin markets poses a significant threat to countries that rely on capital controls in order to retain a managed exchange rate.

Bitcoin creates a problem for Argentina and similar countries; it makes circumventing capital controls easier. As demonstrated in Pieters and Vivanco (2016), government attempts to regulate the globally accessible bitcoin markets are generally unsuccessful, and, as shown in Pieters (2016) and Chart 4, bitcoin exchange rates tend to reflect the market, not official exchange rates. Should the flows allowed by bitcoin become big enough, all countries will have, by default, unrestricted international capital markets.

This is not insignificant; a good fraction of the world's population lives under capital controls, including residents of Brazil, Russia, Indonesia, Taiwan, China, and Argentina. A critical piece of the State's monetary toolkit is being eroded.

Being highly liquid and traded globally, Bitcoin also has the practical effect of casting light on exchange rate manipulation, as discussed in another paper by Dr. Pieters. Bitcoin trades can be used to derive a passthrough estimate of the 'street price' of local currencies, even when the government is publishing false exchange rates. Bitcoin is fast growing into its role as a universal measuring stick.

One example: publishing information on the street value of the Bolivar is illegal in Venezuela, as the regime has a strong interest in maintaining a tight grip on the narratives around their currency. The most popular exchangerate-tracking website in Venezeula, DolarToday (run out of Miami) uses LocalBitcoins trades to derive an implicit USD-Bolivar Soberano street price.

Source: https://dolartoday.com

It's no surprise that the world's most vibrant p2p Bitcoin markets tend to be in States with capital controls, highly inflationary sovereign currencies, or capricious governments. This analysis by Matt Ahlborg, again relying on LocalBitcoins data, demonstrates that Bitcoin is most traded on a per capita basis in Russia, Venezuela, Colombia, Nigeria, Kenya, and Peru. It is sometimes said that currency competition is like outrunning a bear; you only have to outrun your slowest friend. The dollar is probably not threatened by the existence of Bitcoin, but the world's couple dozen most inflationary currencies absolutely are.

As Hasu has written, Bitcoin provides a stable system of property rights*without* any reliance on the State (and the implicit threats of violence that underscore it all). This is mostly irrelevant in the West where property rights are generally respected; but it is a matter of life and death elsewhere. No small irony, then, that cryptocurrency's staunchest critics tend to be precisely those individuals that have never had

reason to mistrust their government with their savings. One's reaction to Bitcoin is a shibboleth; it reveals whether an individual is aware of the vicious effects of inflation and an unreliable banking system. The loudest Bitcoin deniers simply reveal their ignorance and anglocentrism.

Indeed, new findings from Raskin, Saleh, and Yermack evaluating currency crises in Turkey and Argentina confirm that the cryptocurrency has its most immediate applicability outside the developed world.

At first blush, Nakamoto's vision did not pan out, except insofar as a new option was created that a majority of people choose not to use. When one investigates the developing world, however, the story is a little different. [...] [Turkey and Argentina] are the first currency crises since the creation of bitcoin, and therefore they offer an opportunity to investigate the impact that alternative digital currencies have on unstable sovereign currencies. Extrapolating out, this may show that Nakamoto's vision has come to fruition. Although private digital currencies have not replaced the dollar, their mere existence may have a counterfactual impact in that they exist as a check on both fiscal and regulatory policy.

Specifically, the authors find, somewhat unsurprisingly, that "citizens gain from the existence of the private digital currency," in particular through a new option for diversification, which "generates welfare gains for citizens."

Critically, the authors also find that

[T]he existence of the private digital currency disciplines monetary policy by creating an alternative to local fiat. That monetary policy discipline reduces inflation and results in higher returns from investment which in turn encourages higher local investment.

As economics 101 holds, busting a monopoly (governments are effectively local monopolists in the market for money) by introducing competitors should make the market fairer for consumers. Faced with no alternative, citizens were previously forced to save in their local currency and tolerate inflation. Now with an effective off-ramp, citizens have the choice to exit the local monetary regime, at significant cost to the central bank (selling their local currency increases the velocity of money and worsens inflation). So the mere existence of Bitcoin instills monetary discipline on a central bank which might otherwise pursue a ruinous level of debasement.

Not for the faint of heart

Because of the extremely high stakes, reinventing a monetary system is a profoundly unpleasant task. It takes irrational zeal and an unwavering commitment to a firm vision of the future. Given the immensity of this task, and the existential threat it poses to the state, only the most committed could possibly take up the cause. The great sin of altcoiners is not that they backed the wrong horse, but that they did so with insufficient conviction. They sold a dream that they themselves did not truly believe.

How many cryptocurrency entrepreneurs would tell you with complete sincerity that they were building a system to last decades and face the State head on? How many would willingly face jail for their beliefs? Very few, I suspect.

The insipid tone at the top percolates throughout the organizational pyramid. Hence the distinction between the "communities" of underwater holders that urge each other to buy the dip as their coins bleed, and a resilient community that embraces the volatility and keeps the faith. Superficially, Bitcoin and its many blockchain-employing clones are similar. The main differentiator is soul. It's not that alternative chains are immoral or opted for an inferior set of values, it's that they are entirely nihilistic. Progress and cosmetic innovation is prided over building lasting, non-State institutions.

For sure, the profit motive drives many towards Bitcoin. Yet something far deeper and more primordial drives Bitcoiners too — the possibility of building a parallel, reliable financial system which is functional, open, and independent of governments or unaccountable corporations. Of course, this motivation does not drive Bitcoiners alone. But Bitcoin has undeniably made the most progress towards the separation of money and state, and has suffered the brunt of political attacks so far. No other project has been exposed to so much media hysteria and so many early roadblocks.

Not the case, for the would-be alternatives. Success for upstart cryptocurrency founders is an exit. The presale; the markup; the dump on retail. The allure of launching a new blockchain was simple; money has the largest TAM of any product in existence, and to own even a fraction of it all by minting a new currency and retaining some share promised Crassus-tier wealth. But wealth does not inspire, especially when it is obtained at the expense of the would-be converts. Dumping one's presale is no way to win the dogmatic, undying support of millions of willing footsoldiers.

As Taleb says: don't tell me what you think, show me your portfolio. What better case study than Block One, creator of EOS, the would-be Blockchain 2.0, divesting its treasury and choosing to hold 140,000 BTC on its balance sheet?

The only questions that matter

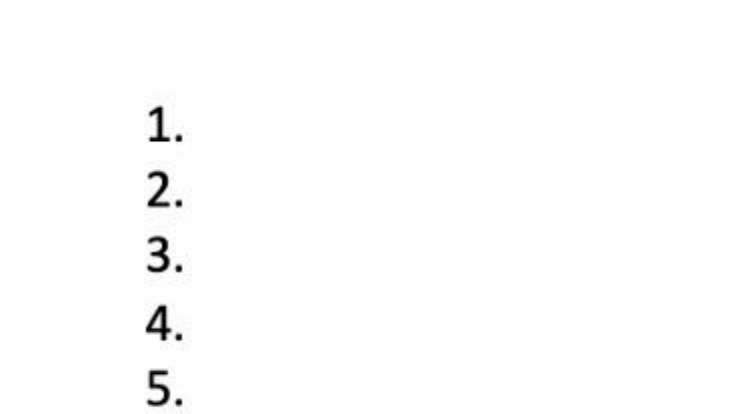
After ten years of experimentation, misallocated capital, and hubris, we have learned valuable lessons about value accrual. The scientists and engineers mistook the monetary and political revolution for a technological one. Their experiments were impregnated with an insistent prescriptivism:

"If only we can create a more efficient or performant database structure or sybil resistance algorithm, we can crack the case and create the ultimate winning cryptocurrency." This mindset, astonishingly, is still prevalent today. But it is hopelessly flawed. These are political and social experiments first. The most important factors in minting an entirely new monetary system from scratch are not the technical implementation details, but rather the provision of compelling answers to questions like:

- what gives you the right to mint a new currency and to have disproportionate influence over its fate?
- why are you choosing to reject all of the alternatives and proposing to replace them with your own?
- from where do you derive your authority?
- how are you enshrining fairness and equality of opportunity in the distribution of this new money?

- how will you ensure that the system is free from corruption when even the U.S. Federal Reserve is vulnerable to political capture?

Bitcoin has clear answers to all these questions. Its imitators do not. Not only do they not have reasonable answers, their creators aren't even aware that these are the appropriate questions to consider.



Above: a list of all the utility tokens that fulfilled their stated purpose and saw meaningful adoption

We know now that utility tokens are chimeras. It didn't take a genius to spot this, but the empirical reality has set in for good now. A utility token world is analogous to one in which a frictional forex transaction is required not for interstate travel as is the case today, but from one store to the next. Utility tokens proposed a dismal regression, and we are better off now that they have been repudiated. The only cryptocurrencies worth creating are those that aim to be money; and this necessarily entails tilting at the State.

But going toe to toe with the State requires tens or hundreds of millions of diehards that believe in a stable set of values and are willing to put capital to work supporting it. Clever cryptographic primitives and tinkering with new byzantine-fault-tolerant algorithms cannot inspire and win devotion. There must be some core set of values which are prided over everything else. Most monetary pluralists in the industry justify their stance with recourse to trite cliches like being "pro innovation". This is incoherent; if they reject incumbents like Bitcoin and agitate for some alternative project, they too will face objections from the crypto progressives to their left.

"Why settle for x blockchain 2.0? Why not p, q, or r?" The question is a compelling one. Absent deeply held shared values clearly instantiated by one's chosen project and one's chosen project alone, there is no defense of the crypto-progressive's alternate chain, aside from sunk costs. Out of necessity, the progressive becomes a reactionary.

Values set Bitcoin apart

So what are these values that Bitcoiners hold dear? Bitcoinism is an emergent political and economic philosophy combining strains of Austrian economics, libertarianism, an appreciation for strong property

rights, contractarianism, and a philosophy of individual self-reliance. Some libertarians will recoil at social contract theory, understanding it to be coercive (since one is not actually offered a political contract to sign at birth or at maturity). Not so with Bitcoin. No one is defaulted in: it offers a fairly explicit contract to would-be users. You have the right but not the obligation to participate in the most transparent, auditable, debasement-free, and and well-defined monetary system the world has ever known.

Other values which I would consider critical to Bitcoin include cheap validation (so anyone can participate), full auditability (so no unexpected inflation), fairness in issuance (everyone regardless of status paid "full market price" for their BTC, either on an exchange or by mining), backwards compatibility (soft forks rather than hard forks preferred), and of course the open validator set, to prevent validator collusion and the inevitable censorship it leads to. Pose the question to your favorite Bitcoin alternative. What are the values that motivate the project? If they exist, you will notice that they are generally weakly held; innovation is prided over consistency.

Thus Bitcoiners strike a profound contrast to the opportunists who envision success as a financial exit from their token project. For Bitcoiners, success consists of a day when no exit is required. Their admittedly eschatological philosophy anticipates a time when they will be able to participate in a closed loop Bitcoin economy, free from the vicissitudes of the legacy financial system. They do not dream of a financial exit, at least not in the venture sense. They crave instead a system built on a monetary standard which does not arbitrarily debase savings because ***monetary discretion of any sort is completely absent.***

And they are serious about retaining these foundational qualities. Not only must the predefined supply schedule be kept, but it is so completely fundamental to the protocol and system of property rights that to alter it would cause the old system to cease to exist. Capped supply is not a feature of Bitcoin; the supply cap *is* Bitcoin. It is ontologically critical, like the consent of the governed is an inalienable component of the U.S. Constitution. Sure, you could overthrow the government and install an autocratic government identical in name, but that would not be the original. Its very substance, relying as it does on foundational values, would be changed. The ideals are not contingent. They are not a mere implementation detail. The values are the system; the system encodes the values.

And what better role model than Satoshi himself. Satoshi is the ultimate sacrificial hero — he spent an age building Bitcoin from scratch, released the code, ran the project for a brief time, and then stepped away, permanently. The coins he mined — out of necessity, to support the network when no one else would — were left untouched. To call this effort Promethean is almost painful in its aptness. Satoshi daringly stole the State's most treasured possession — its right to unencumbered money creation — and gave it to the people in the purest way possible.

So what of the State? If the threat is so severe, why does it not intervene? Frustratingly, Bitcoiners tend to have an answer to every objection.

The reality is that a ban wouldn't stop Bitcoin, unless you believe that the international community, increasingly trending towards chaos and an anarchic morass, would unite to tackle this threat. Imagine

that! North Korea, Iran, the U.S., China, Russia, and Saudi Arabia all aligned in a common cause. And this is considered one of the best arguments against Bitcoin by its critics.

Damned if they do, damned if they don't

Let's say major countries colluded to ban Bitcoin. This would merely turn Bitcoin into a black market commodity. But it would not be sufficient to obliterate it. Consider for a second another widely banned commodity, reliant on significant energy for creation, produced by a mixture of industrial and informal entities, chiefly circulated on the black market, enjoyed by millions. I'm referring of course to cannabis, and you can probably obtain it from a dealer nearby — legal or not — in under 30 minutes. To believe a ban would abate Bitcoin's popularity is comical. It would only reinforce Bitcoin's literal *raison d'être*: protection from the whims of the capricious State. A State so obviously threatened by a financial commodity would reveal itself to the world as paranoid and controlling, making its true parasitic nature very clear.

Ironically, the State's best response to Bitcoin and Bitcoin-inspired private monies is to meet the demands of the techno-Austrians and reform itself.This would require ending the debasement of currency, ending the inequality-boosting loose money regime, ceasing interference in economic cycles (which simply makes them more severe), ending the hubristic attempts to set a price for the time value of money, and ending the use of financial institutions as weapons of war.

For any of this to change in the near term seems vanishingly unlikely. The neo-Keynesian theory _du jour _is a delightfully accelerationist atrocity named "Modern Monetary Theory," according to which the State can ostensibly purchase unbounded quantities of any good available for sale in its own currency, consequences be damned. Our current moment is one in which socialist-bordering-on-fully-collectivist politicians are elevated and hankered for by their ever more subservient constituents. Bernie; Elizabeth Warren; Ocasio Cortez; Jeremy Corbyn. In the developing world, you have Kirchnerism retaking control in Argentina, sending all financial assets spiraling towards 0 as collectivism reasserts itself. In Argentina's typically more free-market friendly neighbor Chile, two unabashedly communist lawmakers are now setting the agenda. Venezuela — well, Venezuela. In the UK, Labour has embraced a startlingly confiscatory policy, advocating for illiberal measures like mass forced divestment. And the free markets capital of the world, Hong Kong, is under literal assault from its murderous and autocratic occupier.

Suffice to say, free markets and strong property rights — the cornerstones of functioning capitalist economies — are under global assault. This is unlikely to reverse. The global underclass, increasingly futile, craves intervention, and will tolerate gross immiseration if it means a reduction in inequality.

And our monetary institutions have surrendered any semblance of reason. Our current age brings us the entertaining if harrowing spectacle of the President of the United States openly warring with the Federal Reserve Chief over the price of money. The stakes: squeezing a little more juice out of our wholly financialized economy in time for a reelection bid. That was all it took to capture the purportedly nonpolitical Federal Reserve. Hedge funds, in a display of breathtaking paperclip-maximization, now spend millions of dollars on machine learning algorithms predicting interest rates from the eyebrow twitches of our monetary high priests as they read the chicken entrails. Money well spent.

At your disposal: the always-on financial machine

Negative interest rates are now orthodoxy at virtually all central banks in developed countries. The IMF openly speculates about how to impose ever-deeper negative rates, including the forced depreciation of _physical cash. _Regardless of whether you believe savers have a divine right to a positive yield, they certainly start to bristle when you propose confiscating their savings. If arbitrarily negative rates are permissible to achieve policy outcomes, at what point do central banks pause for breath and give savers a reprieve? Already in untrammeled territory, it seems unlikely any restraint will materialize this ends-justify-the-means approach to monetary policy.

Savers may not panic at negative 1%, reasoning that the bank is providing a useful service, after all. They may grumble at -3% and start to wonder if their monetary overlords really have it all figured out. At -5% — they pile into gold and start to wonder about that Bitcoin thing.

Because many people fail to appreciate the strength of the system, let's summarize Bitcoin's first decade:

- $1 billion has cumulatively been paid in transaction fees
- Miners have cumulatively collected $14 billion in exchange for their services in securing the network
- The average cost basis of all Bitcoin holders is approximately $100 billion
- The market value of all outstanding bitcoins is approximately $190 billion
- The network has settled roughly $2 trillion worth of transactions
- The Bitcoin network now produces 80 exahashes per second (that's $8 * 10^{19}$ hashes). These hashes cost about $19.8 million dollars a day on highly specialized equipment

You may deride Bitcoin, no matter. Bitcoin will be there for you when you need it. You may not need it now; you may not need it ever. But as we plunge into a more despotic, authoritarian, and chaotic world, you may one day feel comfort knowing that the world's highest assurance wealth protection system in history is waiting patiently for you.

Until then, it will keep ticking along.

The cat is out of the bag

By Nic Carter

Posted December 29, 2019

Bitcoin is everyone's problem now

Evey: Remember, remember, the Fifth of November, the Gunpowder Treason and Plot. I know of no reason why the Gunpowder Treason should ever be forgot... But what of the man? I know his name was Guy Fawkes and I know, in 1605, he attempted to blow up the Houses of Parliament. But who was he really? What was he like? We are told to remember the idea, not the man, because a man can fail. He can be caught, he can be killed and forgotten, but 400 years later, an idea can still change the world. I've witnessed first hand the power of ideas, I've seen people kill in the name of them, and die defending them... but you cannot kiss an idea, cannot touch it, or hold it. Ideas do not bleed, they do not feel pain, they do not love... – **Evey Hammond, V for Vendetta**

An exorbitant privilege

Bitcoin is first and foremost a monetary phenomenon. The social climbers and false prophets who proclaimed it is a payments revolution have either come around or been repudiated by the market and washed out, embittered. Most who understood it that way are now moving on to new things. The world did not need another Paypal. **The world needed a new monetary institution**.

As Bitcoin went from a proof of concept, to a toy, to a joke, to a collectible, and then to a movement, a few policymakers came to realize that it posed a threat to the established system. Not because of its present form, but because what it represented: a profane insult to the carefully calibrated monetary system. All done in a mocking, insouciant fashion — a band of nerds and ne'er-do-wells insolently challenging the state's monopoly on seigniorage. Satire is what despots fear most, and the rise of Bitcoin made our present monetary system look patently absurd.

Critic: Nothing backs Bitcoin.

Bitcoiner: What backs the dollar?

Critic: Nothing intrinsically — our ability to compel foreign nations to accept our currency as the numeraire of international trade, our ability to force citizens to pay taxes in dollars, and our military assets required to enforce both conditions.

Bitcoiner: How persuasive!

The visceral hatred elites feel about Bitcoin? Perfectly justified. How else would you react to a upstart aimed at usurping your sacred monetary privilege?

Such is the potency of Bitcoin that it compels the high priests of U.S. imperialism to reveal the unwritten rules about the role the dollar plays in power projection abroad. In May of this year, U.S. Representative Brad Sherman (D-CA) spoke out against cryptocurrency on the floor of the house. His statement laid bare the normally veiled post-Bretton Woods doctrine in which the dollar is employed not only a monetary tool but a strategic one, too.

An awful lot of our international power comes from the fact that the dollar is the standard unit of international finance [...] and it is the announced purpose of the supporters of cryptocurrency to take that power away from us [...]. Whether it is to disempower our foreign policy, our tax collection, or our traditional law enforcement [...]. the purpose of cryptocurrency [...] is solely to aid in the disempowerment of the United States and the rule of law.

Representative Sherman is practically a soothsayer. He understands *precisely* where the world is going.

His mistake is not in the diagnosis, but in the cure. He mistakenly believes that Bitcoin can be reckoned with. But Bitcoin is an idea, not a product. The notion of a weightless, virtual commodity was productized for good in 2009 (although the idea long predated Bitcoin), and it has been eroding the state's monetary monopoly ever since.

It could not have been created at a better time; one wonders how Bitcoin would have fared if it had been created in the 1980s or 90s when the US economy was fairer, the monetary system was totally unquestioned, and the US was the sole dominant global superpower. Against today's backdrop, Bitcoin insists on itself. It has *urgency*. In the halcyon days of Pax Americana, Bitcoin would have mattered much less. In the twilight of the American empire, however, it is more relevant than ever.

Our monetary system is disastrously redistributive

The wealth of political elites derives primarily from privileged access to the monetary spigot. This is no longer a secret. The heavenly mana of seigniorage has opened, first a trickle and now a flood. The world is grappling with inequality, and the dozens of populist revolts active in the world today are patent evidence of this. Yet the resurgent socialist parties misdiagnose the situation. The enemy is not a nebulous form of capitalism, but rather a form of socialism itself — a low-rates fueled perma-bailout to the owners of financial assets. It's no coincidence that asset prices have steadfastly risen in the last decade, as the Fed has embarked on a ludicrously unshackled period of money creation.

Many ask: against the backdrop of monetary issuance, where did the inflation go? It went of course into financial assets. But this benefits the paltry few. Did you know that the decade-long rally in the S&P500

has been characterized by historically low participation from retail investors? The riotous gains in asset prices have sidelined mom and pop. They accrue instead to institutional investors and corporate insiders who returned capital to themselves through buybacks. In the 90s, Wharton MBAs convinced investors that the ideal mode of corporate governance was making large equity and options grants to corporate directors to create incentive alignment. Well, the grants were made, and the directors rewarded the shareholders by spending corporate earnings on buying back the stock, thus juicing earnings per share and triggering options payouts for directors. They just so happened to forgot to generate corporate value along the way. That pesky real economy… that was secondary.

Why are politicians so rich? Why do they become rich *after* leaving office? Why do regulators go work in industry? Why is the Secretary of the Treasury a former Goldman banker and hedge fund manager?

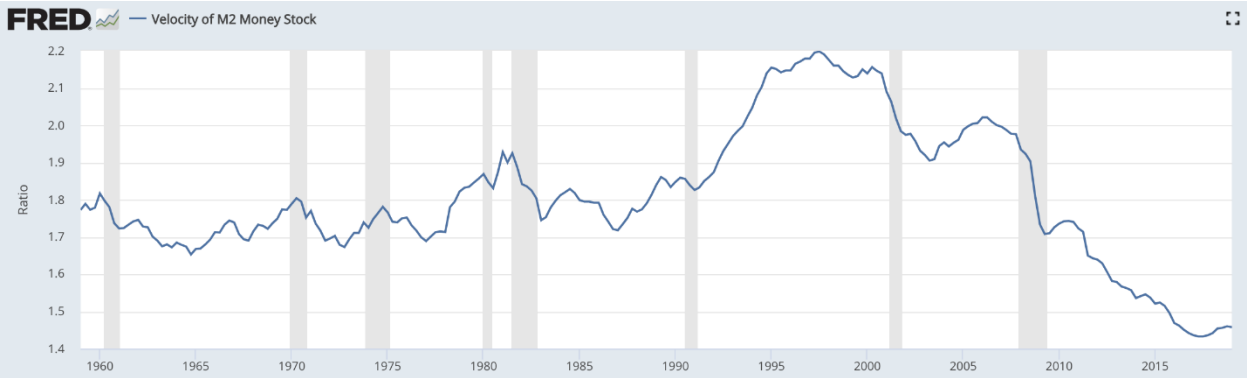
The Cantillon effect pictured

Why are renters historically disempowered, whereas landowners are historically privileged? Why has the cost of higher education and healthcare outpaced inflation by orders of magnitude? Why is the CPI a sad, pathetic joke? Do consumer goods account for most of your expenditures, or does rent, healthcare, and education?

What are you more exposed to? The cost of a TV, or property values?

Even if you didn't know what the Cantillon effect was, you felt it vividly in the last decade. The hopelessness felt by many in today's society is the consequence of this monetary misalignment; the introduction of eye-watering money into the economy, but an uneven distribution. Who benefited from historically low rates? Normal folks dealing with predatory credit card loans, or owners of financial assets who were able to put historically cheap capital to work? And no, cheap financing didn't help the middle and lower class get a foothold in property… because property values were horrendously inflated in the first place! Property, treated as a store of value for the rich, is precisely where so many of the Fed's newly-minted dollars settled. Reflect on those hollowed-out city centers in Vancouver, New York, and London — full of empty homes used as capital warehouses for absentee millionaires.

If there's a single graph that evidences the impact of a decade of freewheeling monetary stimulus on the economy, it is the following:



Monetary velocity in the U.S. is at its lowest since modern records began. If you think about the equation of exchange (MV = PQ), a decline in V is sufficient to offset an increasing money supply (M) to keep prices (P) stable. And that's just about what happened: the purchasing power of the dollar has remained relatively stable even as supply has expanded dramatically. "Where is the inflation?" is the common refrain, but the question should instead be "where has the new money supply gone?" It is clear that it has settled, inert and unproductive, in financial assets mostly owned by the ultra-rich, bidding them up to century highs in relative valuation terms.

This is why our perverse form of zombie capitalism is often referred to as socialism for the rich. If you can position yourself close enough to the money spigot and arrange to share in the spoils of the monetary redistribution, you can profit handsomely. If you have access to financial assets and can benefit from a low cost of capital (whether you are an investor or a corporate director with discretion over buybacks), you can make low rates and quantitative easing work for you. If you cannot, you are utterly frozen out of the system, and indeed disadvantaged, as pricier capital assets immiserate the non rentier class.

Bitcoin is a system that explicitly rejects identity

Critics often ask who, exactly, Bitcoin is for. This perhaps a misspecified question. Bitcoin does not serve a "who," or a subset of whos. It just serves, indifferent its end users. Bitcoin, by design, does not require identity data to work. Your counterparty could be on the OFAC sanctions list, they could be a sentient toad, or a few lines of code. Bitcoin has no way of knowing, nor does it care. The only requirement to send a payment is to provide a valid signature which meets the criteria sufficient to unencumber a UTXO.

Traditional payment and credit relationships, on the other hand, enshrine identity. My credit card company is *very _interested in knowing that it is me who is using the card. If I inform them that a stranger has absconded with my card, they consider all the spends post-theft _totally invalid*. The call with the fraud department goes like this:

- 'Can you vouch for the $10.51 purchase on 2/24 at Chipotle?' Yes, that was me. Extra guac.
- 'Can you vouch for the $463.39 purchase on 2/29 at Lululemon?' No, I don't habitually buy athleisure gear.

Identity data is inextricable from traditional payment networks. This is because they are many layers between payments and final settlement. An incredibly large and profitable business exists to assess the credibility of transactors and facilitate deferred-settlement transactions between them. This is because credibility and mutual trust enables massive efficiencies. You can lend your neighbor a lawnmower without demanding he provide a bond to cover its value because you *trust him*. Credit card networks just scale this up: they are trust underwriters, determining quantitatively how trustworthy I am, and passing along those assurances to merchants with whom I transact.

If they get it wrong, and it turns out I'm the kind of person who racks up a $10,000 credit card bill with no intention of ever paying, they swallow the cost! It was their bad. They should have done a better job assessing my trustworthiness.

The compact you implicitly agree to when you use Bitcoin is between you and the protocol, not between you and all the other users of Bitcoin. The only trust required is users trusting that the cryptographic and economic assumptions hold. So far, they have.

It has become trendy to denounce popular Bitcoiners as uncompromising, unreasonable assholes, and imply that there is something wrong with Bitcoin as a consequence, too. But Bitcoin is indifferent to this. It is a protocol for encoding and conveying value through a communications medium. Bitcoin isn't even aware of what the price of Bitcoin is, let alone the political trends of the day. It knows very, very little about itself.

As stated above, Bitcoin is attractive and useful precisely because it *rejects* any identity data from the conditions required for a spend. The only thing that has to be furnished is knowledge of a private key corresponding to a public key. When you receive Bitcoin, you do not need to be aware of the identity of the sender, because Bitcoin settles probabilistically. You can simply define your own threshold for finality — say, requiring $500,000 of work to be done before you consider a transaction final. That would correspond to waiting, at current rates, for 4–5 blocks under which your transaction should be buried.

This is what allows me to accept funds from people that I mistrust, and why Bitcoin is carving out a niche in these frontier transactions. Think of a ransomware hacker and his victim. These people mutually mistrust each other. They victim has been wounded and attacked. But the hacker still trusts that the $500 sent to them for the ransom in the form of BTC is a valid, unlikely-to-be-reversed payment. You may not like this. But Bitcoin flourishes on the margins of society. These are increasingly widening, as banking becomes politicized and used as a political tool, as the U.S.-driven settlement system is coopted for strategic objectives, and as identity requirements for payments networks become ever more rapacious.

Transacting with people you have no reason to trust is precisely why Bitcoin exists. The internet allowed us to transact with people on the other side of the globe, but internet commerce is beset by fraud. The reason credit cards are expensive is because the costs of remediating fraud and chargebacks are socialized.

If you aren't comfortable with evil people using Bitcoin, you should abandon it now

Of course, the jettisoning of counterparty trust (and risk) comes with some perceived drawbacks. Principal among them, you cannot evict someone from your network. This is very uncomfortable to people who believe that money ought to be a political tool, to be exploited to disempower political foes of the day.

There is a particular paradox in demanding that the members of a network you have inserted yourself into adhere to a certain moral code of conduct. As stated above, Bitcoin, and fast-settling hard money more generally, exists to facilitate commerce between individuals that do not have a pre-existing bond of trust. What did inter-continental traders use to transact in the 17th century? They certainly didn't use IOUs, wampum, collectibles, or credit relationships. They knew that they might never see each other again, so they used the hardest money they had available — gold and silver. Monetary metals speak for themselves; they are no one's liability.

In this same way, Bitcoin is a means to transfer wealth between individuals who both have an interest in final settlement. It is not a means to establish a credit relationship (although Lightning is an early move in this direction). Bitcoin is deliberately amoral, it has no requirements to entry and asks nothing of the user aside from a valid signature. It facilitates commerce between people who explicitly disagree with each other. Thus trying to impose a moral code on Bitcoin is contrary to its very nature. If everyone who used Bitcoin agreed with each other, then no one would need Bitcoin — they could all exchange IOUs backed by their mutual trust in each other. But because the world is messy, and people disagree with each other, hard money is warranted. Our chaotic world practically demands it.

So if you are the kind of person that rejects a useful transactional medium because someone you dislike is using it as well, it wasn't suited for you in the first place. Bitcoin is edgy precisely because the world needs a payment and savings system which cannot be interfered with on moral or political grounds. To repudiate these transactional constraints is to violate the carefully poised moral setting that has seized the West. If stepping out of line isn't for you, stick to Paypal instead.

Bitcoin is an apocalyptic death cult...

As Bitcoin hater-in-chief David Gerard so elegantly puts it, Bitcoin is in fact an apocalyptic death cult. Apocalyptic, because Bitcoiners recognize the futility of the current monetary system, and appreciate that it is likely to end in tears. Death, because States won't give up their monetary privilege easily. Bitcoin is veiled in eschatological overtones. Cult, because you have to be somewhat deranged to take a pill this black.

Freedom is not "Free".

So spare a thought for the Bitcoiners. They are fully awakened to the pending grief and strife that await us, Cassandras warning governments and citizens alike to the disruptive effects of truly sovereign currency (sovereign, as in free, not as in State-owned). But unable, most of the time, to convince their fellow man that the State's monetary machinations may not be sound. Most people are content to surrender all freedom and autonomy to the Leviathan, as long as the pot they are in boils slowly.

… but it's open to all

The exact reason that Bitcoin is despised by so many— identity, creditworthiness, and trust are irrelevant in this system, making it a fertile ground for criminals — is the exact reason why it's so inclusive. Unlike Paypal, Venmo, or traditional payment processors, it cannot deplatform you for wrongthink, holding subversive political views, being a sex worker, or legally selling cannabis. Ours is the biggest possible tent. Don't be distracted by the online discourse. Bitcoin is utterly indifferent to the political views of its users. Its core developers, the high priests of the protocol, can barely change it: (implementing a fairly routine upgrade, SegWit, took them _years _of cajoling and pleading). Getting it to do anything other than produce blocks, accept valid spends, resolve forks, and relentlessly march onward is virtually impossible.

Whether Bitcoin will challenge the State, or whether that task will be left up to a successor, is yet to be determined. That the State's monetary privilege has been permanently eroded is evident though.

It died a little that day in January 2009 when the *Chancellor [was] On the Brink*, and it has been shrinking ever since.

By Nic Carter, Oct, 2019

An Introduction to the Efficient Market Hypothesis for Bitcoiners

What the EMH does and does not say

By Nic Carter

Posted January 4, 2020

Curbstone brokerage on Broad Street in Manhattan, 1902 (Public domain image from the United States Library of Congress)

As we approach the Bitcoin halving due in May 2020, a heated debate has raged among Bitcoiners about whether the issuance change is being anticipated by the market or not. Those who downplay the purported impact of the issuance change tend to make references to market efficiency. This concept has thus become a source of great rancor and debate. The disagreements are often intractable, as strawman versions of the EMH are presented, and the parties cannot converge on shared definitions. Mutually understood concepts are a prerequisite to a useful debate. Since the concept is widely misunderstood, I thought I'd explain it from scratch, assuming little prior financial knowledge.

Origins of the EMH

The efficient market hypothesis has been attributed to several thinkers, among them Benoit Mandlebröt, Louis Bachelier, Friedrich Hayek, and Paul Samuelson. Hayek's *The Use of Knowledge in Society* is useful background reading for the concept, although it never makes reference to the EMH specifically. His seminal essay argues in favor of distributed, market-based economies, in contrast to centrally planned ones. The key insight: markets are information-aggregation mechanisms that no central planner, no matter how skilled or well-resourced, can match. Consider the following passage (emphasis my own):

[T]here is beyond question a body of very important but unorganized knowledge which cannot possibly be called scientific in the sense of knowledge of general rules: the knowledge of the particular circumstances

of time and place. It is with respect to this that practically every individual has some advantage over all others because he possesses unique information of which beneficial use might be made, but of which use can be made only if the decisions depending on it are left to him or are made with his active coöperation.

[...] And the shipper who earns his living from using otherwise empty or half-filled journeys of tramp-steamers, or the estate agent whose whole knowledge is almost exclusively one of temporary opportunities, or **the arbitrageur who gains from local differences of commodity prices, are all performing eminently useful functions based on special knowledge of circumstances of the fleeting moment not known to others.**

In the bolded section you can begin to see how Hayek views markets: as forces that aggregate a multitude of different views and expectations into prices. Hayek understands market-derived prices as information — a particularly high signal source of information at that. The beauty of markets, to Hayek, is that simply by selfishly acting according to their own interests, individuals participating in the economy create signals in the form of prices. The EMH orients this perspective specifically towards financial assets, holding that investors collectively surface relevant information which is incorporated into prices through the mechanism of trades.

Following a series of studies about stock returns like Samuelson's 1965 *Proof that Properly Anticipated Prices Fluctuate Randomly*, the EMH was finally codified for good in 1970 by legendary finance academic Eugene Fama (you may have heard of the Fama-French model). In a paper entitled *Efficient Capital Markets: A Review of Theory and Empirical Work*, Fama defines an efficient market as "a market in which prices always "fully reflect" available information." If you were stop reading here, you'd already have a better understanding of what is meant by efficient markets than the caricatures presented on Twitter. The EMH is not a mystical claim. It's simply the view that market prices reflect available information. This is why academics often refer to them as 'informationally' efficient markets. The efficiency refers to information proliferation.

What does this actually mean? It simply means that if there is new information which is relevant to the asset being traded, this information tends to be incorporated into the price of that asset with rapidity. And if there are future events which you might reasonably imagine would affect price, they tend to be incorporated into the price *when known*. Markets don't wait for (knowable) events to happen — they anticipate them. This means, if a weather forecast predicts that a hurricane will emerge and wipe out sugarcane plantations next week, speculators will bid up the price of sugar *today*, anticipating the supply shock. Now, of course, when there are unpredictable exogenous shocks (imagine that the hurricane materialized with no warning), then price can only react in real time, as the information becomes known. The speed of information incorporation is one of the tests of efficiency.

While the EMH is a simple idea, it tells us a great deal about how markets operate. Markets are efficient if prices rapidly incorporate new information. Forecastable, market-moving events taking place in the future tend to be incorporated in price beforehand. Importantly, one consequence of the EMH is that, once all relevant information is incorporated into price, you are left with only random fluctuations, called 'noise'. What this means is that while asset prices will still jitter about, even in the presence of no new fundamental information, these fluctuations contain no information of their own.

And lastly, the difficulty of surfacing unique new information (not already included in price) tends to vary with the sophistication of market participants and the liquidity of the asset. This explains why you might be able to find an edge in an obscure micro cap stock, but probably not in predicting the price of Apple.

Since Fama's paper, and thanks to popular books on the topic like Burton Malkiel's *A Random Walk Down Wall Street*, a heated debate has raged over whether active management is worth it. Indeed, since efficient markets posit that consistent edges are very difficult to find, many investors have come to question whether actively traded vehicles like hedge and mutual funds make sense. In the last decade, trillions of dollars have flowed out of such 'active,' stock-picking strategies, and into passive vehicles, which simply seek to track the performance of the entire market, or a specific sector. This is one of the most critical debates happening in finance right now, and it's mostly due to the growing realization that markets are, indeed, generally efficient.

The EMH described

I take slight exception to the 'hypothesis' component of the EMH. If it were up to me, I'd call it the efficient markets *model*, not hypothesis. This is because it doesn't really contain a hypothesis. It doesn't really make a specific testable claim about the world. As stated, the EMH posits that **market prices reflect available information** (which, as we have noted, is the purpose of markets in the first place). Interestingly, Fama in his 1970 paper calls it the efficient market model, not hypothesis. It seems he has the same intuition.

I would also go as far as to consider EMH somewhat tautological. Recalling Hayek, we know that (free) markets measure society's net informational stance over various assets. So if we replace 'market prices' with 'concentrated information outputs' in the EMH construction bolded above, we get the following:

Concentrated information outputs reflect available information

That certainly sounds tautological. But that doesn't make the model any less useful_._ Conversely, it means that contesting the EMH is to question the nature of markets themselves. And indeed, most critiques of the EMH (I will cover a few later in this piece) generally cover instances where markets are not clearing, for some reason or other. So if you accept that EMH is tautological, 'efficient markets' also starts to sound redundant. Indeed, the default state of (free) markets is to be efficient, because this is why we have markets. Markets compensate anyone for finding relevant information. If they weren't default-efficient, then we wouldn't bother with them.

Referring to it as a model makes it very clear that it's just an abstraction of the world, a description of the way markets should (and generally do) work, but by no means an iron law. It's just a useful way to think about markets.

Let me be clear! I do not believe in the "strong form" of the EMH. No finance professional I know does. It is generally a straw man. The strong form holds that markets reflect **all** information, all the time. If this were true, no hedge funds or active managers would exist. No one would bother poring over Apple's quarterly reports, or evaluating the prospects for oil discovery in the Permian basin. Clearly, given that we

have a large active asset management industry, in which lots of very bright individuals constantly seek to surface new information about various assets, the strong form doesn't hold.

Truthfully, the EMH is not something you 'believe in,' or not. The choice is to understand markets as useful information-discovery mechanisms, or reject the usefulness of markets altogether.

There are of course conditions which lead to market inefficiency. Fama acknowledges as much in his 1970 paper, calling out transaction costs, the costs of acquiring relevant information, and disagreement among investors as potential impairments to market efficiency. I'll discuss two here: the costs of surfacing material information, and frictions inherent in actually expressing market views.

If the EMH generally holds, how are funds compensated for finding information?

So what explains the fact that there is a large (albeit shrinking) industry involved in active investing, despite the fact that markets are generally efficient? If market-relevant information is generally encoded in prices, then there is no profit from finding new information and trading against it. But clearly, many individuals and firms do actively attempt to surface new information. This presents a bit of a paradox.

This brings us to another one of my favorite papers, *On the Impossibility of Efficient Markets*, by Grossman and Stiglitz. The authors point out that gathering information is costly, not free. They then note that since EMH posits that all information is immediately expressed in prices, there would be no compensation from incurring costs to surface new information under that model. Thus markets cannot be perfectly efficient: information asymmetries must exist, as there must be a way to compensate informed traders. Their model introduces the useful variable of information cost into the standard model of market efficiency. It follows from their model that if information becomes more costly, markets become less efficient, and vice versa. So whether or not markets reflect their fundamentals is at least partially a function of the difficulty of surfacing that relevant information.

The authors conclude:

We have argued that because information is costly, prices cannot perfectly reflect the information which is available, since if it did, those who spent resources to obtain it would receive no compensation. There is a fundamental conflict between the efficiency with which markets spread information and the incentives to acquire information.

A rather delightful implication of Grossman and Stiglitz is that, to render arbitraging prices back to where they 'should' be a profitable activity, there has to be a cohort of traders who are perennially knocking prices out of whack. Fischer Black (he of the Black Scholes formula) gives us an answer, with a lovely paper pithily entitled *Noise* in the Journal of Finance. He identifies unsophisticated 'noise' traders: those who trade on noise, rather than information. Noise can be found anywhere. Just mosey on to Tradingview and see the plethora of indicators that people swear by. Black divides market players into two cohorts:

People who trade on noise are willing to trade even though from an objective point of view they would be better off not trading. Perhaps they think the noise they are trading on is information. Or perhaps they just like to trade.

With a lot of noise traders in the market, it now pays for those with information to trade. Most of the time, the noise traders as a group will lose money by trading, while information traders as a group will make money.

Noise, in Black's view, "makes financial markets possible." The existence of noise traders gives professional firms like hedge funds liquidity, and valuable counterparts to trade against. In the poker analogy, noise traders are the fish. They make the game profitable for the sharks, even in the presence of a rake. Ask any former online poker player — as the scene became more competitive, and unsophisticated players left, it stopped being as profitable to play.

The noise theory resolves the 'apparent impossibility' of efficient markets as pointed out by Grossman and Stiglitz. The existence of noise as introduced by unsophisticated traders gives sophisticated traders a considerable financial incentive to introduce information into prices. So you can thank the degens overtrading on Bitmex — they are the ones compensating funds for allocating resources to Bitcoin and surfacing relevant information quickly.

If the EMH generally holds, how do you explain instances where markets do not clear?

This is another good question. There are copious examples of situations where arbitrage opportunities were easy to identify, yet where the arbitrage could not be closed for some reason. The most famous of these examples is arguably the trade which caused the demise of Long Term Capital Management. It was a pair trade on bonds which were effectively identical but were differently priced (partially due to the Russian default in 1998). LTCM was betting that the prices of the bonds would converge. However, many other hedge funds had made that same bet with leverage, and as the bonds failed to converge in a timely manner, LPs in some of the hedge funds redeemed, the funds faced margin calls, and were thus forced to liquidate this positions. This kicked off a feedback loop causing additional squeezes: the cheaper bonds were sold off, and the pricier instruments kept rallying as shorts were covered. LTCM was betting on market efficiency and the convergence of these instruments; but because of market stress and the winding down of pent-up leverage, they weren't able to complete the trade, and the fund blew up.

This phenomenon is examined in a 1997 paper from Shleifer and Vishny entitled *The Limits of Arbitrage*. Shleifer and Vishny point out that arbitrage is not normally done by the market, generically, but rather is a task delegated to specialized institutions (funds, typically). As such, arbitrage is costly: requiring freely available capital. There's a paradox: great arbitrage opportunities come about when the market is under stress (this is when you get many stocks trading at a low price-to-book, for instance). But during times of market stress, capital is *least available*. Thus the arbitrageurs, who require capital to operate, are worst equipped to perform the required arbitrage when they are most needed. These are the limits of arbitrage. As the authors state:

When arbitrage requires capital, arbitrageurs can become most constrained when they have the best opportunities, i.e., when the mispricing they have bet against gets even worse. Moreover, the fear of this scenario would make them more cautious when they put on their initial trades, and hence less effective in bringing about market efficiency.

Take the simple example of a value-based hedge fund which has raised outside capital. They will tell LPs (investors in the hedge fund) of their intention to pursue contrarian bets — buying value stocks when they are cheap, for instance. Let's say the market declines and they buy a basket of stocks whose valuations have contracted and have low P/E ratios. However, imagine that the market subsequently declines another 40%. Their LPs are now staring at a loss and ask to redeem. This is the worst possible time: the fund has to sell the stocks at a loss, even if they have a high conviction on making money on them in the long term. They would much rather be buying the (now very discounted) stocks, whose valuations are even more attractive. To make things worse, liquidating those positions forces them down further, punishing other funds making the same trade.

Shleifer and Vishny therefore find that:

[P]erformance-based arbitrage is particularly ineffective in extreme circumstances, where prices are significantly out of line and arbitrageurs are fully invested. In these circumstances, arbitrageurs might bail out of the market when their participation is most needed.

The limits to arbitrage caveat about EMH actually explains a lot of situations where people will describe market conditions and lament that information is not being incorporated. This is often taken as a slight against the EMH. But of course we cannot expect malfunctioning markets to operate properly. So when Dentacoin's multi-billion dollar putative market cap is touted as an example of market efficiency not holding, consider that it likely had a minuscule float, ownership was extremely concentrated, and obtaining a borrow for a short was impossible. This means that market participants cannot meaningfully express their views on the asset.

A fuller conception

Mindful of these constraints (issues of market structure, costly information, limits to arbitrage), we can devise a more complete version of the EMH which includes these caveats. You might therefore devise a modified EMH that sounds a bit like this:

Free markets reflect available information to the extent that price-setting entities are willing and mechanically able to act upon it.

- *Free markets:* because state-controlled markets may not clear (for instance, markets for currencies with capital controls do not give reliable signals, since selling is effectively constrained)
- *Price-setting entities*: because minnows don't ultimately matter most of the time. A small number of well-capitalized participants can suffice to incorporate material information into price
- *To the extent that they are willing*: this covers the 'costly information' caveat. If information is more costly to obtain than it is worth to instrumentalize (for instance, in the case of discovering accounting fraud in a micro-cap stock), then it won't be included in price

- *Mechanically able:* this covers cases where limits to arbitrage exist. If there is a liquidity crisis, or the markets are not functioning properly, for whatever reason, and funds cannot operationalize their views on the market, inefficiency may occur

So when most financial professionals talk about the EMH, they generally imply a modified, slightly caveated version like the one above. Almost never do they mean the 'strong form' of the EMH.

Interestingly, by caveating the EMH, we have stumbled on an alternative conception entirely. The model I have described here somewhat resembles Andrew Lo's *adaptive market hypothesis*. Indeed, while I am very happy to maintain that most (liquid) markets are efficient, most of the time, the adaptive market model far more closely captures my views on the markets than any of the generic EMH formulations. Many active managers that I know are at least familiar with Lo's work. The theory is fully developed in his book, but you can get a condensed version in his 2004 paper.

In short, Lo attempts to harmonize findings from behavioral economics finding apparent irrationality on the part of investors, with the orthodox EMH school. He calls it the adaptive market hypothesis because he relies on an evolutionary approach to markets. Taking Black's insight further, Lo divides market participants into 'species', giving us a view of market efficiency which departs from the mainstream:

Prices reflect as much information as dictated by the combination of environmental conditions and the number and nature of "species" in the economy or, to use the appropriate biological term, the *ecology*.

Lo describes profit opportunities from information asymmetries as 'resources', leading to formulations like the following:

If multiple species (or the members of a single highly populous species) are competing for rather scarce resources within a single market, that market is likely to be highly efficient, e.g., the market for 10-Year US Treasury Notes, which reflects most relevant information very quickly indeed. If, on the other hand, a small number of species are competing for rather abundant resources in a given market, that market will be less efficient, e.g., the market for oil paintings from the Italian Renaissance.

The contextualism and pragmatism that Lo's model presents aligns it with the experience of most traders, who intuitively understand that market participants are quite heterogeneous, and understand the notion of 'table selection' (borrowed from poker). I won't dive too deep into Lo's take here, but I do recommend his book, and at the very least his paper summarizing his theory.

What this means for Bitcoin and the halving

As we have seen, most markets are efficient most of the time. This is not something markets just happen to do; this is their purpose. I have discussed a few exceptions: the limits to arbitrage situation, non-free market situations, situations where behavioral biases apply, and situations where market participants may not be sufficiently motivated to surface relevant information. The question is, do any of these conditions apply to the Bitcoin markets? Right now, this doesn't seem to be the case. We are not in a liquidity crunch. There are no apparent limits to arbitrage. In the pre-financialized era for Bitcoin (I'd say

anytime before 2015), you could have convincingly made that case. There truly was no easy way for a well-capitalized entity to express as positive view on Bitcoin. But today there is.

As for free markets, Bitcoin is clearly a very free market, one of the freest on earth (since the asset itself is highly portable and easily concealable, and traded around the globe). Unlike most currencies, it is not backed or guaranteed by a sovereign, and there are no capital controls impairing selling. Participants also have the abundant ability to place large short positions on Bitcoin, so they can express a diverse set of views. So we can check the 'functioning markets box'. Now, is Bitcoin sufficiently large for there to be a significant number of sophisticated funds devoting concerted effort to surfacing material information? At a $150b market cap, I think that's absolutely the case. The final test of market efficiency is whether or not market-moving information is incorporated into prices right away, or with a lag. An event study covering the effect of exogenous shocks like exchange hacks or sudden regulatory shifts on price would be welcome.

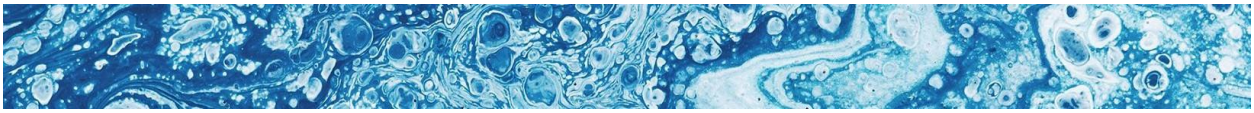
The only necessary conditions for efficiency for which Bitcoin still has question marks have to do with disagreement among market participants (i.e. the lack of a shared valuation model that price setting entities converge on), and the development of more financial plumbing. There are still a few classes of entity for which Bitcoin exposure is rather difficult to obtain. Of course, surmounting these challenges will render Bitcoin's prospects sunnier.

So is the halving "priced in" or will it be a catalyst for appreciation? If you've read this far, you will understand that I consider it patently absurd that a change in issuance would have been overlooked by the price-setting entities. Anyone with an interest in Bitcoin has been aware of the supply trajectory from inception. Supply was encoded in the very first implementation that Satoshi released to the world in January 2009. Long-scheduled changes in the rate of issuance do not constitute new information. Any presumed demand-side reactions to the 'halving catalyst' can also be anticipated by sophisticated funds who have a strong incentive to frontrun investor optimism.

Now, can Bitcoin appreciate from here onwards? Absolutely. I don't believe appreciation, if it occurs, will be due to the entirely foreseeable changes in the rate of issuance (the forthcoming halving will take us from 3.6% to 1.8% annualized issuance), but of course I feel that there are other factors which could positively affect the price, most of which are hard to predict. Is that consistent with the EMH? Very much so. EMH permits informational shocks (for instance, imagine if we suddenly had rampant inflation in a major world currency). It's also possible that the price setting entities are taking an overly conservative view of Bitcoin's future, or that they are acting on a weak fundamental model. These are consistent with weak form EMH.

I'll leave you with this parting thought. Regulated securities markets have structural barriers to efficiency in the form of prohibitions on insider trading. As Matt Levine likes to say, insider trading is a form of theft in which someone trades on information which does not belong to them. They have not discovered the information from public sources, but rather were privy to something like a merger discussion and acted on it. Since insider trading is banned, stock prices generally don't reflect pending catalysts like acquisitions until they are publicly announced. However, in a market for a virtual commodity like Bitcoin, insider standards don't typically apply. If a catastrophic bug is found, you can expect that this

information might be incorporated into price right away. So in that sense, it's quite possible that the market for Bitcoin is *more* informationally efficient than markets for U.S. equity are.



Common objections

I will consider some objections here. Odds are, your responses are covered.

I found an instance of inefficiency. This is evidence for the inefficiency of markets generally

This is a bit like throwing a baseball in the air and claiming that its temporary departure from the earth disproves gravity. Few or no finance practitioners believe that all markets are efficient all the time. If information is unevenly distributed, or information-owners lack the means to instrumentalize their views, then the prices may not reflect information. Short term instances in which markets do not apparently reflect information are just invitations to query why market participants were unable to price in relevant information. These failures aren't evidence of the weakness of the EMH, but rather reinforce its usefulness as an explanatory tool.

Behavioral biases exist, so market efficiency doesn't hold

A number of persistent behavioral biases have indeed been found by researchers, and I find it plausible that they systematically affect asset prices to an extent in the medium term. However the question here is whether they are relevant to the matter at hand — the putative effect of a change of the rate of supply on the price of the asset — and whether these purported biases can actually affect the price formation of a highly liquid $150b asset. You might respond: 'well Bitcoiners have a bias which causes them to bid up the price of assets with sharply decreasing issuance rates, even if this information is already known.' If you can prove, Kahneman and Tversky-style, that this is a universal human bias which affects asset pricing, and contradicts dominant market models, not only will you win the argument, but you will also likely collect a Nobel. In this situation I'd also refer you once again to Lo's adaptive markets.

Efficiency is impossible in Bitcoin because there are no fundamentals

Some people hold that sentiment drives everything in crypto markets, and that fundamentals do not exist. This is a convenient fallacy. There are obvious fundamentals which everyone would agree matter. Here is a short, non-exhaustive list:

- the quality of financial infrastructure enabling individuals to get exposure to and hold Bitcoin. In 2010, it was virtually impossible to buy Bitcoin, and your only option for custody was the Bitcoin QT 'Satoshi Client' or a homebrewed paper wallet. Today, you can get a billion dollars of Bitcoin

exposure, and you can self-custody it or rely on some of the world's largest asset managers and custodians. This is a fundamental change
- the quality of the Bitcoin software (compare the current version with Satoshi's first client). The protocol itself and the tooling surrounding it has been improved, refined, and made more useful
- the actual stability and functionality of the system — imagine a case where Bitcoin failed to produce blocks for a month. That would surely impair the price. If you concede this, you admit that there are 'fundamentals' beyond mere sentiment
- the number of individuals globally that are aware of and demand Bitcoin. This is 'adoption'. This not mere sentiment; this is a measure of which sources of capital, worldwide, are actively seeking exposure to Bitcoin

There are many other fundamentals which I won't cover here. Funds which trade Bitcoin seek to track the trajectory of these variables, and ascertain whether Bitcoin is too richly or modestly priced relative to their growth. This is "fundamental analysis".

Again, if you aren't persuaded, just think about the contrast between Bitcoin's state in 2010 and its state in 2020. It's many orders of magnitudes easier to use, acquire, buy, sell, and store. That is a change in fundamentals. Granted, these aren't 'fundamentals' of the sort that apply to stocks with cash flows, but Bitcoin isn't a stock. A unit of Bitcoin is a claim on ledger space which gives you access to the particular transactional utility of the network. I'll concede that the fundamentals aren't quite as explicit as those present in a stock. But, the notion of 'fundamentals' isn't just restricted to equity or instruments with cashflows. Global macro investors consider currencies based on macro variables or assessments of political risk. Commodity traders look at production rates and the ebb and flow of supply. There are analogies here.

All of this to say that funds have meaningful market-relevant information to trade against, not just sentiment or hype. It's just that it's hard to obtain a precise fundamental assessment of Bitcoin.

Efficiency is impossible in Bitcoin because it is volatile

It's entirely possible to have volatile and efficient markets. Recall that all efficiency requires is that available information is incorporated in price. Think about the value of a call option close to expiry, with the underlying fluctuating around the strike price. One minute the option is in the money, the next it is worthless. This would be both a volatile and efficient situation.

Alternatively, consider the value of Argentine government bonds in response to political turmoil. The fundamental here is the Argentine government's willingness to honor their debts. Efficiently functioning markets would continuously reevaluate the prospects for creditors being repaid. In a period of flux the fundamental is volatile, and so too consequently is the value of the bonds.

Bitcoin's volatility derives in part from market participants rapidly re-assessing its prospects growth, both in terms of pace and trajectory. Even small changes in future expectations of growth rates have significant effects on the implied present value. (Indeed, in DCF models for equity valuation, the outputs are very sensitive to long term growth rates.) Market participants revise their growth expectations frequently, and

expectations differ (because there is no single dominant model of Bitcoin's price), giving rise to the elevated volatility (especially against the backdrop of a inelastic supply). If future expectations of growth *are* the fundamental, then the rapid revaluation of those expectations creates consequent volatility in price. So volatility does not disqualify efficiency.

If the EMH were true, Bitcoin would have just started life at its current valuation

This isn't how the world works. As I explained above, Bitcoin didn't start life with mature, rock solid fundamentals like it presently has. It had to grow into its valuation. In its earliest days, there was considerable uncertainty over whether it would achieve any success whatsoever. It had to actually go through all these trials and tribulations to get to where it is today. So it wouldn't have made sense for large funds to allocate to Bitcoin on day 1 (although, it clearly makes sense in hindsight), because they didn't know it would grow, and in many cases, because they structurally couldn't invest in it. Think about how you would have acquired Bitcoin in 2012, two years into its existence. You would have had to use something like Charlie Shrem's BitInstant, or the (already insolvent) Mt Gox, which we know now was run shambolically. You could have mined Bitcoin, but this was a difficult and deeply technical task.

This returns us to the "limits to arbitrage" point. Many investors that *wanted* to buy Bitcoin from 2009 through to present day simply couldn't, due to regulatory reasons, operational risks, and a lack of functional market infrastructure. Even if they did believe that Bitcoin would be worth north of $100b at some point, they wouldn't have had the ability to instrumentalize that view. Moreover, investors didn't start out with rock solid conviction. They needed to see Bitcoin work, successfully, in the wild, without being shut down, before choosing to store wealth in it. If you believe that Bitcoin's continued success represents new information being brought to market, then you understand that the EMH does not require it emerging from the womb, fully formed, at an initial >$100b valuation.

Something which is influenced by ponzi-related buying like Plustoken cannot be efficient

I'd agree that investors in Plustoken buying (and then selling) about 200,000 BTC was a major driver of price action in 2019. However, this doesn't impair efficiency. If it had been known in the West that Plustoken had all those coins, and were just about to sell them off, and the price of Bitcoin did not move, then I agree — there would have been questions about efficiency. However, it wasn't until much later, after much of the coins had been sold off, that information percolated through the West about the Plustoken BTC. Remember, efficiency doesn't require that prices *never move*; rather, it suggests that prices move on new information.

Small cap assets pump on by hundreds of percent on dubious news. This is evidence of market inefficiency and disproves the EMH

Again, local, or temporal evidence of perceived irrationality does not invalidate the EMH. You either believe markets are good information clearing mechanisms or you do not. Granted, many of these small cap altcoin markets are very poor, from a structural perspective. These assets may trade on unregulated or illiquid exchanges. This means the prices you see do not necessarily reflect reality. Thus temporary pumps and dumps in illiquid assets don't prove much in either direction, aside from the poverty of the market environment in which they trade.

Generally speaking, most adherents to the EMH will concede that efficiency varies positively with the size of the asset and the sophistication of the participants. It will be very hard to find an edge in large, publicly traded stocks. Odds are, if you find some market-relevant information about Apple or Microsoft, someone else will have found it as well. But in smaller, less liquid asset classes, the returns from surfacing relevant information are far less, so there are less analysts actively inserting information into assets, meaning that opportunities may well exist. This is because large, multibillion dollar funds simply cannot operationalize strategies trading in microcap assets.

This is simply to say that there are scale effects with efficiency. Bitcoin is not a microcap; it's a globally traded traded asset worth over $100b. This ensures that there are high returns from surfacing relevant information and expressing it in the form of trades. Thus there is a significant disanalogy between the inefficient microcap altcoins (where returns from finding information are low, and markets are weak), and a mature asset with lots of analysts looking for an edge.

When small cap cryptoassets get 51% attacked or suffer bad news, they don't decline. This demonstrates that crypto markets are not efficient

I'll defer to Lo here (seriously — read Adaptive Markets!). The adaptive explanation would be that small cap assets are generally held by hardcore believers, or better yet, closely held by confederates of the founding team. In those conditions, cartel-like behavior can easily emerge. You have likely seen these conversations on Reddit and Telegram: coin owners urging each other not to sell, especially not in the presence of bad news, since the crypto community is briefly paying attention to the project. Renewed buying in the face of bad news is a way that issuers seek to blunt the effect of a negative catalyst. This only works in small markets were ownership is not widely distributed, though.

Also, it's worth considering that virtually no one holds these assets because they like the underlying technology or find that particular flavor of code ripped off from Bitcoin Core or Ethereum that interesting. Small cap cryptoassets are held in expectation of a possible future pumps. Thus, impairments relating to the actual protocol itself are not the *fundamental*. The fundamental is the issuing team's willingness to procure "adoption," or at the very least, feign adoption by securing favorable press releases and partnerships. As long as the underlying protocol doesn't totally dissolve, the 'fundamental' — the ability of the issuing team to create hype — can remain intact.

Since some bitcoiners mechanically buy Bitcoin on a regular basis (think: tithing) and less new supply will exist, this will mechanically cause appreciation

This is an example of first order thinking. The EMH lives on the second order. The key insight of the EMH, to me, is that any information you have, a sophisticated market participant also has. Since sophisticated market participants are strongly incentivized to find relevant information and trade against it, you can bet that they will have expressed that information the moment they acquired it. If this were indeed a plausible hypothesis (that static buying pressure would have a positive effect on price as issuance is cut in half), then these funds have already expressed this positive view in the form of a trade. This is what is meant by "priced in." If something material is discovered to be due to happen tomorrow, it will be incorporated into price today. This is one of the most tricky features of the EMH, and it genuinely takes a bit of effort to get your head around it.

The question then becomes, not "is this information which, in a vacuum, would move the price?" but rather "**do I have information which the smartest and best-resourced hedge fund analyst does not have?**" If the answer is "no," you can expect that this information is presently incorporated into price (to the extent that it is actually material information).

Why the focus on funds? The reason is that they are specialized firms which aggressively seek out information and express it in the form of trades. They are the entities which keep price in line with the "fundamental." You need to recall that you are not operating in isolation. You are operating in the digital equivalent of a jungle with predators lurking around every corner. These predators are skilled, fast, and well resourced.

In equity markets, we're talking about funds that have personal relationships with CEOs and CFOs, have dinner with them, and interpret whether they are optimistic about the next quarter. Funds that have dozens of analysts crunching datasets you weren't even aware existed. They will track corporate private jet movements to suss out whether an acquisition is likely to take place. They will run a machine learning model to assess the emotional state of Jerome Powell from his eyebrow twitches as he announces Federal reserve actions. They will take satellite data imagery from parking lots to predict whether Walmart will beat quarterly earnings guidance. Public markets are incredibly competitive. They are where some of the most talented individuals make their careers, and there's no real restriction on being able to act on information (outside of insider trading). Anyone who believes they have an edge is free to express their view in a trade.

So if you feel you have information which is market-relevant (like this expectation that a supply contraction would drive up the price), the most sophisticated participants have it too. And they've already evaluated it and acted on it.

Additionally, you need to recall that markets are not democratic. They are weighted by capital. A whale can express a far stronger opinion than a minnow. Hedge funds simply have more capital (and they tend to have access to cheaper leverage!). Then, when they develop a view on some stock, they have the means to

express that view. This is how the "pricing in" takes place. Thus it's really only price-setting entities that matter most of the time.

Plustoken amassing 200k BTC (~1% of supply) and selling it was a major driver of price action in 2019. Why wouldn't the halving (affecting 1.8% of issuance) do the same?

First of all, the rise and fall of Plustoken wasn't anticipated. It was genuinely new information — so much so that most investors only learned of the magnitude of the ponzi until **after** it was mostly done selling off. Also, as far as we can tell, the Plustoken BTC wallets were liquidated over a relatively short period; about 1-2 months far as I can tell. That's a lot of BTC for any market to absorb. The change in issuance adds up to a decline in 1.8% annualized — but that's annualized. What it means mechanically is that ~24,800 fewer BTC will be mined every month. That's a large number, but it's not the same as 200,000 BTC being liquidated in a short period. And, unlike Plustoken, the reduction is known well in advance.

The halving will affect Bitcoin from the demand side, by causing excitement among investors and getting press coverage. Thus the halving will still be a positive catalyst for Bitcoin

The same logic as found in the response directly above holds here. If you look at the Litecoin case study, the price was clearly bid up in anticipation of the halving, and then it collapsed after the halving itself. This may well have been a case of investors hoping that the halving would be a positive catalyst. You can see how investors positioning themselves (making bets on how they think other investors might react) affects price. You get into a recursive game where everyone is watching everyone else, and they all try and anticipate what the other is doing. Thus even if there is a highly-anticipated demand-side shock on the date of the halving (either through press coverage or simply investor ebullience), it will have been anticipated by a price setting entity and likely incorporated into price months prior.

If markets are efficient, there's no point investing in Bitcoin

This isn't the case at all. There are some informational facets of Bitcoin which are entirely known and transparent, like the supply schedule. However, as I mention above, a lot of the fundamental drivers of the Bitcoin price are not easily quantifiable or even knowable. No one quite knows how many Bitcoin owners there are worldwide, for instance. If you are able to forecast these factors better than others, you will be able to find an edge. Additionally, there are plenty of un-forecastable shocks which might have a positive effect on Bitcoin in the future, such as currency crises. Critics of the EMH fail to see that it only stipulates that markets express *available* information. Obviously, unknown future catalysts are not available. They haven't happened yet.

Ultimately, if you are better at forecasting Bitcoin's growth than other price-setting entities, you might want to trade on your superior knowledge. I think this is an entirely plausible prospect. So I am absolutely

not discounting Bitcoin potentially being attractive for an active allocator, even in the presence of the EMH. Indeed, I personally have a positive outlook on Bitcoin. So clearly I believe there is alpha in having specific domain expertise on Bitcoin. If I were a staunch strong-form EMH believer, I wouldn't be in active management! In fact, active managers have a very strong incentive to find ways to repudiate the EMH. So it should be rather telling that I am defending it here.

For an example of what a demand-oriented fundamental model of Bitcoin might look like, here's an attempt courtesy of Byrne Hobart:

Investing in Bitcoin: The Asset Allocator's Perspective

Off and on, friends ask me why I'm not working at or running a crypto hedge fund. I'm interested, worked in the...

medium.com

Under the presence of weak-form EMH, fundamental analysis is possible, and indeed necessary. After all, someone has to do the analysis to surface the information that ultimately is expressed in prices. This job is left to active managers. So maybe those nasty hedge fund investors are useful for something, after all.

Thanks to Allen Farrington and Leigh Cuen for their helpful review and feedback.

Lessons from the uneven distribution of capital

By Nic Carter

Posted February 8, 2020

What we can learn from distorted maps

As the crypto markets continue their transition from a retail-focused, unrestricted global altcoin casino, to a more constrained and regulated environment, it's worth zooming out and pondering what long-term allocative outcomes this market is likely to witness. Cryptocurrency purports to allow commerce and capital to flow freely, independent of artificial nation state boundaries. However, when securities are involved, the state tends to intervene.

There is a good reason for this: securities are high-stakes markets governing the allocation of productive capital, and for them to function, the state needs to enforce fairness, disclosure, and information symmetry. In fact, the best example in favor of securities laws I can think of is the anarchy and carnage exhibited in the Initial Coin Offering boom in 2017. If blockchain-lubricated capital markets mature from these early hiccups and some of these equity-like assets become viable, they will surely be indexed to their local jurisdictional rules. To the extent that tokenization and crypto-wrapped securities become investable, I'd venture that the U.S. is strongly positioned to compete for issuers — despite the globalized nature of the crypto industry.

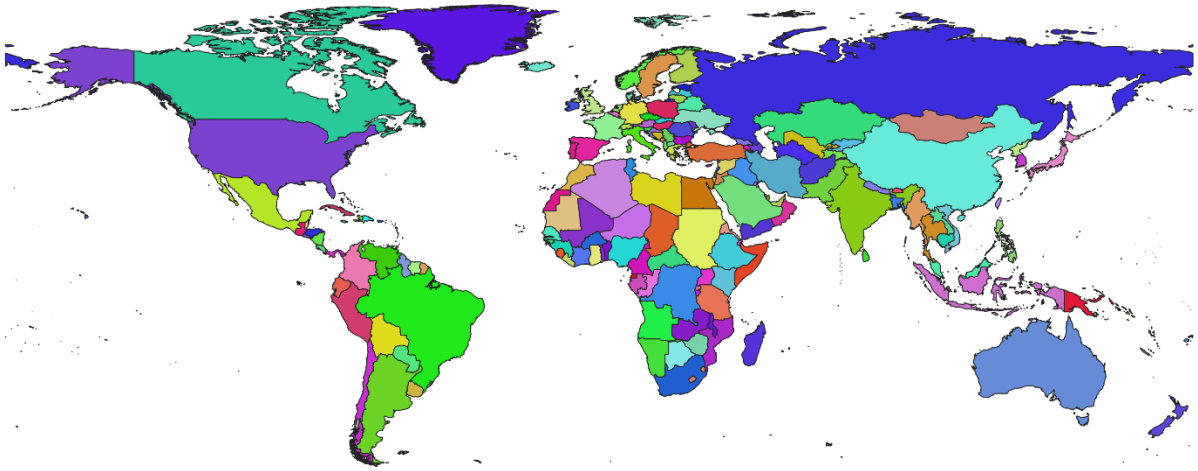
What distorted maps tell us about shareholder rights

It's often said that the SEC is "pushing innovation abroad" by cracking down on crypto projects, especially those that issue pseudo-equity in the form of a token. This may well be the case. It is also quite a reductive view. Capital clusters in jurisdictions where the rules are understood, where property rights are respected, and where legal systems appropriately apportion power between shareholders and directors. Thus, the enforcement of age-old rules which made the U.S. the most vibrant equity market on earth in a crypto context can be understood as either hostile to issuers, or accommodating to investors. The latter perspective is sorely neglected in the regulatory analysis.

In the issuance of equity, standardization is a godsend. If you work in startups, you will mostly likely have a strong understanding of the nuances of a Delaware C corp or the YC SAFE. When issuers select these instruments to raise capital, they are opting for a set of rules and a legal context which are mutually understood by founders, VCs, and law firms. This often entails cheaper diligence and less legal overhead. Indeed, some VC funds don't invest in anything other than Delaware C Corps. This is just one anecdote, but it hints at the bigger picture: investors like predictable and comprehensible structures. They like to know where they stand relative to founders, and what their recourse is if something goes wrong. At a global scale, small differences in jurisdictional predictability lead to wildly divergent outcomes.

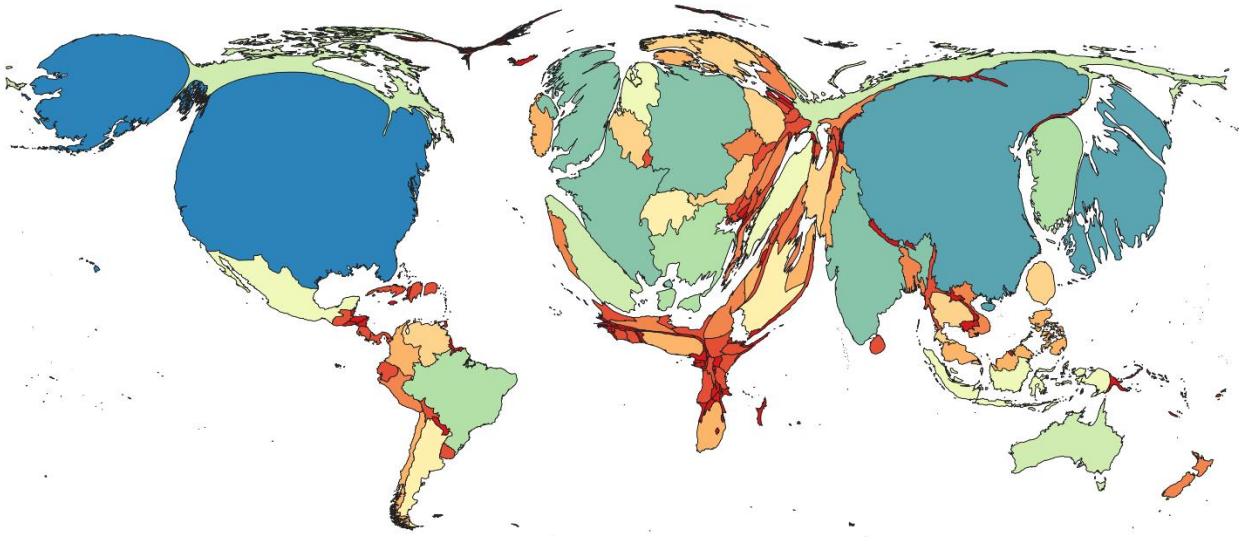
You may be surprised to learn that the U.S. accounts for 26% of global GDP, but a staggering 40% of global public equity capitalization. This point is best made visually with a chart called a cartogram. What a

cartogram does is weight land area by some variable while keeping shape intact (or at least attempting to). Let's start with a basic map projection. In this case I am using the Plate Carée projection, a variant of the equirectangular projection. This is what it looks like:



World countries shapefile courtesy of ArcGIS Hub (source)

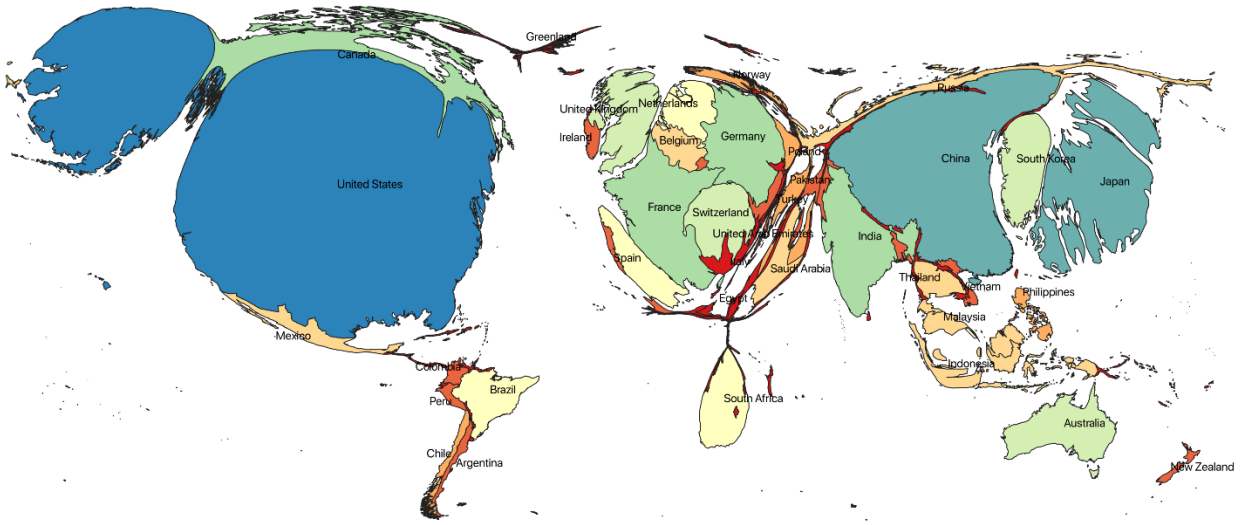
Now let's **weight countries by GDP** (2018) so you can get a general sense of the global income distribution. This means that certain more developed countries will swell up and less developed countries will shrink. But I'll do my best to retain the general shapes of the countries so the map is still intelligible.



Cartogram made with Scapetoad and visualized in QGIS3.4. Data is 2018 GDP in USD terms from the World Bank

I've bucketed countries into a few color coded categories so you can compare similar countries by GDP. For instance, with this chart, you can tell that France ($2.5T), Germany ($3.6T), and India ($2.9T) are in a similar range. Same with South Korea ($2T), Brazil ($2T), and Italy ($1.9T). You can also tell that Australia, Spain, Canada, and Russia have similar GDP — between $1.3 and $1.6 trillion. You get the point.

Now if I were to ask you what the same map with **domestic public equity capitalization** as the key variable might look like, you might imagine it would resemble the above. More GDP, more money to invest in the stock market, after all. Interestingly, this isn't quite the case. Here's the map weighted by the size of domestically listed equity markets:

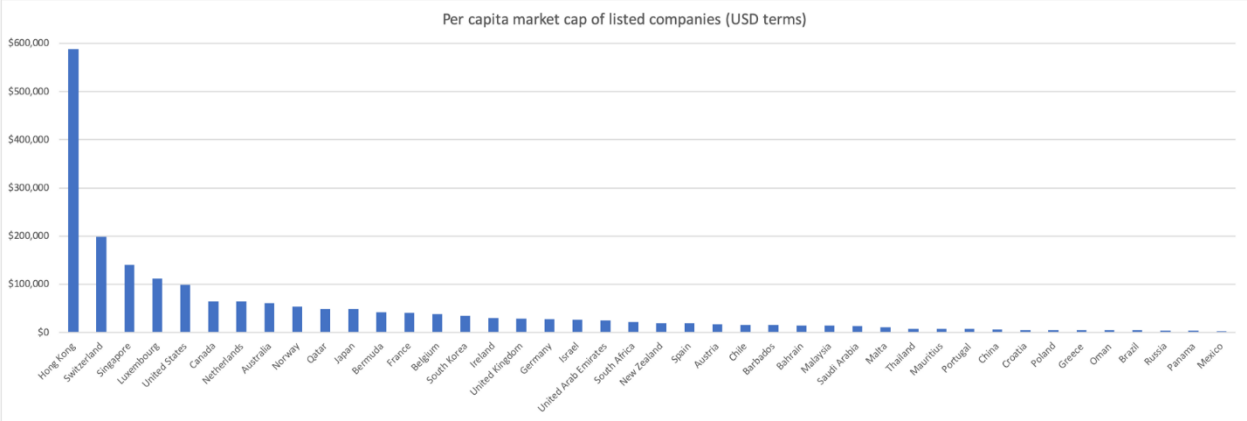


Cartogram weighted by market capitalization of domestically listed companies, 2018 data courtesy of the World Bank

Please note that Hong Kong isn't present on this map because it sadly wasn't included in the open source vector file I used to build the country shapes. Hong Kong would be about 50% the size of China on this map. Compare the Public Equity cartogram with the GDP cartogram and you notice a few things immediately:

- the U.S., even though generates a big chunk of global GDP, still punches above its weight in terms of domestically listed equity
- South America and Africa have under-developed capital markets, even relative to GDP
- Chinese equity markets are prominent, but small relative to their share of global GDP
- niche/haven jurisdictions like Hong Kong (not depicted), Luxembourg, Singapore, Switzerland, are overweighted
- Europe represents a significant fraction of equity markets but less than you might expect from their share of global GDP

Let's dig in to the data a bit more to find the biggest outliers when it comes to countries that punch above their weight from an equity market perspective.



Market capitalization of listed domestic companies (USD) divided by population, World Bank data

Amazingly, the per capita market cap of domestic equity in Hong Kong is US$588k. This is a bit of an exception, as many Chinese companies choose to list on the HKEX rather than in Shanghai or Shenzhen. This is partially a function of less onerous listing requirements in Hong Kong, partly a function of Hong Kong's financial hub status, and tighter relationships with western capital markets, and partially a function of the fact that Hong Kong's legislature, judiciary, and attitude towards property rights are influenced by its former status as a British colony.

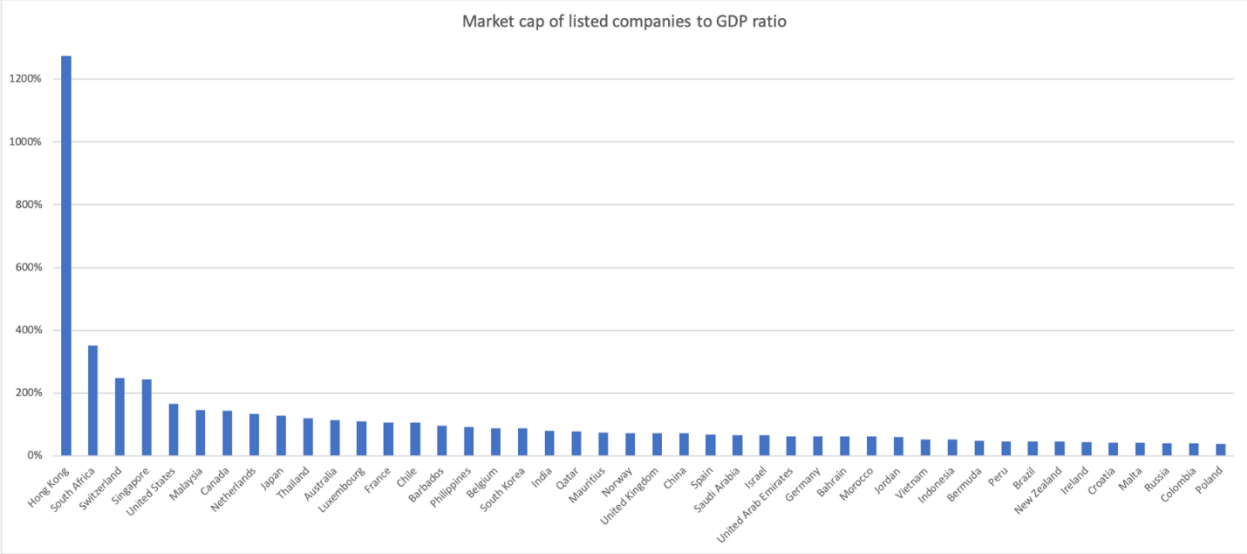
For a more detailed take on why Chinese firms are so fond of listing in Hong Kong, Fanpeng Meng's *A History of Chinese Companies Listing in Hong Kong and Its Implications for the Future* provides additional context:

Specifically, there are some fundamental elements [present in Hong Kong]: a stable and sound legal system with strong respect of private property ownership, an absence of exchange rate control with the linked exchange rate, an efficient and sophisticated banking sector populated by some of the world's top banks, a simple and low-rate taxation regime in which there are no capital gains taxes and whereby income taxes are charged on a territoriality basis, and a relatively clean and transparent business environment intensively monitored by the government.

Listings in Hong Kong are quite significant relative to China, totaling about US$4.3T compared with China's US$8.7T.

Other states scoring highly on the per capita equity market cap figures include a smattering of haven states like Switzerland, Singapore, Bermuda, and Luxembourg, and developed nations like the U.S., Canada, the Netherlands, Norway, and Japan. Regional financial hubs like Qatar, the UAE, and South Africa also score well by this measure.

Another similar measure is the aggregate market cap to GDP ratio. This synthesizes the two cartograms depicted above, so you can find the biggest outliers without having to visually inspect the charts.



The ratio of the market capitalization of listed domestic companies (USD) to 2018 GDP, World Bank data

Compared with the per-capita metric, this one better selects for nations which have a lower overall standard of development but still have large equity markets relative to their economies. Again, Hong Kong is the stark outlier here. But it's joined in the list of unexpectedly large equity markets by places like South Africa, Malaysia, Thailand, and Chile.

South Africa is an interesting case study. In Africa, there are only three meaningfully developed local equity markets — Nigeria, South Africa, and Egypt. South Africa, a historically prosperous former British colony with the lingering presence of British institutions, is the largest of the three. Literature on equity development in Sub-Saharan Africa is sparse.

POLITICAL RISK COMPONENTS		
Sequence	**Component**	**Points *(max.)***
* A	Government Stability	12
* B	Socioeconomic Conditions	12
* C	Investment Profile	12
* D	Internal Conflict	12
* E	External Conflict	12
F	Corruption	6
G	Military in Politics	6
H	Religious Tensions	6
I	Law and Order	6
J	Ethnic Tensions	6
K	Democratic Accountability	6
L	Bureaucracy Quality	4
Total		100

Political risk determinants from the International Country Risk Guide Methodology

Some answers can be found in an IMF working paper on the topic (Andrianaivo and Yartey 2009). The authors conclude from a cross sectional regression that the most important determinant of equity market development in Africa, aside from straightforward variables like domestic savings and per capita GDP, is political risk. This stands to reason: if a military junta takes over, or parliament is dissolved, or the country experiences armed insurrection, equity markets will not develop. I've inserted the political risk rubric that the authors used to give you an idea of the relevant criteria. Historically, South Africa has been relatively conflict free (their main post-independence conflicts were minor excursions in Namibia and Angola) and has benefited from stable rule under the ANC, although political conditions have deteriorated in recent years.

My main reaction from the data is to observe that the development of a vibrant equity market is somewhat of an aberration. There are a huge number of disqualifying features — and indeed, your typical state does *not* in fact have a liquid domestic equity market. So what explains the uneven development of public equity markets around the world?

Rules Make the Market

So why do some jurisdictions dominate when it comes to the issuance of public equity? As it turns out, there's an incredibly vibrant literature motivated by this specific question. The foundational, field-defining paper is **Law and Finance** by La Porta, Lopez-de-Silane, Shleifer, and Vishny.

Law and Finance NBER Working Paper №5661 Issued in July 1996 NBER Program(s):Corporate Finance Program This paper examines legal... www.nber.org

If you haven't read it, I strongly recommend a read. It's one of my favorite economics papers, because the methodology really is dead simple: the authors simply look at the variance in investor protections across a broad array of countries, and realize that legal traditions in those countries explain a significant fraction of that variance. In other words, the legal tradition employed on a country-by-country basis, which informs_ what it means to be a shareholder._

Specifically, the authors divide commercial legal traditions in 49 jurisdictions into civil law and common law, further subdividing civil law into German, French, and Scandinavian variants. Common law refers to the British tradition of allowing judges to shape the law through precedent, whereas in civil law, inherited from the Roman tradition, the law is generally created by the legislature, with case law (precedent-setting through court cases) being secondary.

As the authors (henceforth LLSV) note,

[Civil law] originates in Roman law, uses statutes and comprehensive codes as a primary means of ordering legal material, and relies heavily on legal scholars to ascertain and formulate its rules

More abstractly, you can think of common law as a bottom-up, adaptive approach, and civil law as a top-down, more rigid approach. The consequential differences between jurisdictions with diverging legal traditions are significant; indeed, it has been compellingly argued that Brexit primarily boils down to a dispute between legal traditions (in which the EU attempted to impose a civil law tradition on the common law UK, causing frictions). In the words of the Economist, "English lawyers take pride in the

flexibility of their [common law] system, because it can quickly adapt to circumstance without the need for Parliament to enact legislation." In short, common law is considered to be faster moving and more adaptable — ideal for fast-changing capital markets.

A full 21 countries in the sample inherit France's civil law tradition, many of which were conquered by Napoleon. Others were added as part of France's colonial holdings in Africa and the Pacific. And French jurisprudence informed the structure of post-colonial regimes in the wake of Spanish and Portuguese empires in Latin America.

The British Empire led to the proliferation of English jurisprudence throughout the commonwealth. Strikingly, these colonial origins seem to have had long term effects on the future development of shareholder rights, hundreds of years later. As LLSV note:

[L]aws differ a great deal across countries: an investor in France has very different legal rights than she does in Britain or Taiwan. Moreover, a large part of this variation is accounted for by differences in legal origin. Civil laws give investors weaker legal rights than common laws do. The most striking difference is between common law countries, which give both shareholders and creditors the — relatively speaking — strongest protections, and French civil law countries, which protect investors the least.

Mechanically, LLSV enumerate specific shareholder rights which speak to the extent to which shareholders are protected against directors. A selection are listed below:

- **One share one vote**: whether laws exist to tie shares to votes, as opposed to dual classes or nonvoting tranches of equity. The authors consider jurisdictions with these laws as more shareholder friendly
- **Proxy by mail**: whether or not shareholders are allowed to vote by mail (more hindrance in shareholder votes disempowers shareholders, especially smaller ones)
- **Oppressed minorities mechanism**: whether or not minority shareholders (owning 10% or less of share capital) have the ability to challenge the decisions of management or force a buyout of their shares in the case of certain changes like M&A activity
- **Preemptive rights:** whether shareholders have the right of first refusal over new equity issuance
- **Percent of capital required to call a shareholder's meeting:** the higher the required fraction, the less friendly the jurisdiction is to minority shareholders

Their conclusions, while simple from a statistical perspective, were revelatory in the corporate governance literature. LLSV found that:

[A]long a variety of dimensions, common-law countries afford the best legal protections to shareholders. They most frequently (39 percent) allow shareholders to vote by mail, they never block shares for shareholder meetings, they have the highest (94 percent) incidence of laws protecting oppressed minorities, and they generally require relatively little share capital (9 percent) to call an extraordinary shareholder meeting. The only dimension on which common-law countries are not especially protective is the preemptive right to new share issues (44 percent). Still, the common-law countries have the highest average antidirector rights score (4.00) of all legal families. Many of the differences between common-law

and civil-law countries are statistically significant. **In short, relative to the rest of the world, common-law countries have a package of laws most protective of shareholders.**

Taking the analysis further, the same four authors followed their seminal paper with the 1997 Legal Determinants of External Finance, demonstrating that not only do common law countries systematically offer better shareholder protections, but that these investor protections empirically manifest in larger and more robust capital markets.

The authors summarize the key finding:

[T]he legal environment — as described by both legal rules and their enforcement — matters for the size and extent of a country's capital markets. Because a good legal environment protects the potential financiers against expropriation by entrepreneurs, it raises their willingness to surrender funds in exchange for securities, and hence expands the scope of capital markets.

This might seem like a simple point — more investor assurances yield more capital deployed, but when you reflect on the fact that these assurances trace back to the legal philosophy undergirding the financial system, one becomes starkly aware of the path dependence in capital market outcomes. Put simply: institutional quality dictates allocative outcomes. The U.S. isn't just the largest hub of capital formation on earth, it's disproportionately large. This system creates extreme outliers like Hong Kong, Singapore, or Luxembourg.

A related conclusion can be found in Hernando de Soto's book, *The Mystery of Capital*. De Soto evaluates the relationship between property rights and capitalism in a large number of countries worldwide, and concludes that for capitalism to function properly, it must rest atop the bedrock of strongly codified property rights. His reasoning is as follows: the main form of savings for individuals worldwide is through property (in particular, real estate). The main way that capital formation occurs on a small scale is through the monetization of that property, turning it from a purely instrumental asset (somewhere to live) into a capital asset. One example of this would be an individual borrowing against their house in order to set up a small business. If lots of savers can mobilize the capital that they naturally accumulate, capitalism can flourish.

However, as de Soto finds, a significant chunk of property, especially in the developing world, is poorly codified. That is to say, homeowners cannot prove that they hold the deed to their home (a deed may not exist), and they may not have a plausible path to formalizing their ownership. This inhibits their ability to monetize their property at all. Typically, this is due to a dysfunctional bureaucracy or a state apparatus which does not provide a means for incorporating black/grey markets into the formal economy. My takeaway from this remarkable book is that free market economies alone are not enough; they must be accompanied by a legal and bureaucratic apparatus which is flexible enough to enable property owners to make transition from *de facto* to *de jure*, and these rights must be consistently respected. For a longer take on De Soto's conclusions as applied to Bitcoin, see Allen Farrington's essay on the topic.

Cryptocurrencies, perhaps more so than any asset, mitigate these institutional constraints. It's trivial to prove to a third party that you own some Bitcoin; it's trivial to self-custody this claim, and settlement is physical and almost immediately final. Cryptocurrencies are *monetary institutions* — the protocol lays out a

set of rules for permitted behavior, and all participants must adhere to them. This is what gives cryptocurrencies such remarkable global penetration: users mutually understand where they stand relative to the system and the established ruleset, and trust that no well-connected lobbyists are able to exert local policy on system. This is what Nick Szabo refers to as social scalability – the idea that a system can only scale to serve millions of disparate users if it standardizes behavior in a narrow domain (say, rules for what transactions are valid) while minimizing idiosyncrasy and obscurity (which undermine the system's credibility).

Don't Count the U.S. Out

Within the crypto industry, the U.S. has a reputation for being extremely restrictive with regards to the issuance of new cryptoassets. Since 2017 with the infamous DAO report, the SEC has made it quite clear that ICOs are more often than not unregistered securities issuances, and that issuers should be held to the same standard as conventional issuers of securities. In the U.S., if you want to sell equity to the general public, this entails significant legal costs and a high standard of transparency.

In the crypto markets so far, virtually no issuers have met this conventional standard (one exception is Blockstack). Moreover, it's not even clear what information would be considered material for the issuance of a novel protocol or token. In their paper _What Should Be Disclosed in an Initial Coin Offering?, _Brummer, Kiviat, and Massari convincingly make the case that the various disclosure frameworks in the U.S. poorly fit the reality of token issuance, calling for a more appropriate model to be devised.

The significant amount of teeth-gnashing within the crypto industry belies the reality of these markets: the vast majority of tokens sold to the public were entirely meritless, and carried no investor protections whatsoever. Even in cases where tokens purportedly held benefits relative to conventional issuance, with touted features like algorithmically enforced vesting schedules, much of the time these soft provisions were not actually enforced. Hoffman's _Regulating Initial Coin Offerings _takes a careful look at the promises made by promoters which could have been algorithmically enforced. In a survey of the top 50 ICOs that raised significant capital in 2017, Hoffman evaluates the actual implementation in code of promises made to investors. These fall into three categories:

- Promises made about the restriction of supply
- Promises made about vesting schedules that team members were subject to and restrictions on transfers
- Promises about surrendering power to modify smart contracts once deployed (many issuers claimed they would ultimately give up this power)

Unsurprisingly, the authors, by examining the actual code written by issuers, find overwhelming noncompliance with these relatively weak restrictions. So not only were issuers providing extremely limited assurances to buyers; ***those issuers could not even adhere to their own, self-imposed standards***!

So we have a situation where the vast, vast majority of token offerings openly flouted the law. And _lex cryptographia _was an inferior substitute for the law: the few assurances which could indeed be encoded into a smart contract were only spottily upheld. In this context, U.S. policy towards token issuance seems downright reasonable. Assuming that the predominant legal analysis of token launches (in which a single issuer sells tokens to the public) as unregistered securities is correct, the fact that this issuance was happening through a new technological medium is irrelevant.

If you strip away the technobabble and the (generally spurious) claims of "decentralization" and "unstoppable applications," you are left with the straightforward issuance of pseudo-equity to the general public. That anyone, even the most devoted crypto stalwarts, imagined securities regulators would turn a blind eye to this practice in perpetuity is baffling. And gradually, the SEC has come to reckon with this market niche. By being relatively (but not overly) stern, U.S. regulators are positioning themselves for a middle path. Far from outright banning tokens and the industry surrounding them, regulators have meted out a mixture of punishments. The SEC has prosecuted the very worst ICOs and given amnesty to others. Some academics have even praised the much-maligned SEC strategy of selectively enforcing the law.

Reminding ourselves that the U.S. has a 40% share of public equity markets for a reason, the professed strategy of many industry participants to seek greener pastures elsewhere seems short-sighted. The fact that an inferior instrument (the public ICO) did not get a regulatory blessing does not mean that the U.S. is destined to lose its crown as the premier locale for capital formation. Indeed, many high profile securities regulators in other capital-friendly jurisdictions are falling into step with the U.S., as is customary. If crypto issuance is to evolve into something friendlier to buyers, with functional, germane disclosures, genuine algorithmically-enforced vesting and lockups, and perhaps other strongly codified investor protections, there's no reason that regulators wouldn't acknowledge this reality. That they haven't given carte blanche to these issuances is a reflection on the poverty of the implementations we've seen so far, not the weakness of the idea.

Recall, given the above, why the U.S. hosts a disproportionate share of public equity capital. Not only has the U.S. been a hegemonic power for most of the last century, but it has been politically stable, has not seen violent conflicts on its shores, and it boasts an accommodating common law regime which has manifested in strong shareholder protections. Additionally, it has a large middle class for which investing in equities is as much as pastime as it is a necessity. This affinity for active consumer participation in capital markets has unsurprisingly spilled over into crypto as well. Coinbase, the largest crypto exchange/custodian in the world (by far!), is an American company. The largest financialized Bitcoin product is the Bitcoin Investment Trust, issued by the NY-based Grayscale. The first established global financial institution to take Bitcoin and digital assets seriously was the Boston-based Fidelity. To the extent that this industry is an *asset class* (to be clear, the jury is still out on this!)_, _jurisdictions with the financial plumbing and the consumer demand for exposure will naturally be the first to service it.

This perspective may strike you as anglocentric. However, consider it in context. Within the crypto industry, the U.S. is considered a pariah simply for enforcing its local laws (and even then, extremely permissively — see the Block.one settlement). The token frenzy has been chased overseas for now, but it's unlikely to develop into a functional securities market if it operates in an anarchic mode, dependent on

the goodwill of marginal jurisdictions. The industry's best hope is to acknowledge that market oversight is what makes them function and embrace a regime which takes a commonsense view about shareholder/tokenholder protection.

When and if these markets do mature, and security tokens, or on-chain cashflow-wrapped instruments, or highly automated smart-contract-mediated equity do emerge as a meaningful segment of the securities industry, I would fully expect U.S. regulators to engage productively. At that time, issuers and market participants will benefit from taking part in the most dynamic capital markets on earth.

The Last Word on Bitcoin's Energy Consumption

By Nic Carter on Coindesk

Posted May 19, 2020

CoinDesk columnist Nic Carter is partner at Castle Island Ventures, a public blockchain-focused venture fund based in Cambridge, Mass. He is also the cofounder of Coin Metrics, a blockchain analytics startup.

Much ink has been spilled on the question of Bitcoin's energy footprint. But amid the clarifying details and the energy mix calculations we have lost sight of the most important questions. Anyone who wades into this muddy debate must consider the fundamentals before making a final assessment.

Energy: a local phenomenon

Let's start with the basics. Many people, when decrying Bitcoin's energy footprint, point out its energy consumption and presume that someone, somewhere is being deprived of electricity because of this rapacious asset. Not only is this not the case, but Bitcoin's presence in many jurisdictions doesn't affect the price of energy at all because the energy there isn't actually being used. How could this be?

The first thing to understand is that energy is not globally fungible. Electricity decays as it leaves its point of origin; it's expensive to transport. Globally, about 8 percent of electricity is lost in transit. Even high-voltage transmission lines suffer "line losses," making it impractical to transport electricity over very long distances. This is why we talk about an energy grid — you have to produce it virtually everywhere, especially near to population centers.

When you consider Bitcoin's energy intake, interesting patterns emerge. New data from the Cambridge Center for Alternative Finance has confirmed what we effectively already knew: China is the epicenter of Bitcoin mining, with specific regions like Xinjiang, Sichuan and Inner Mongolia dominating. With the cooperation of mining pools, the Cambridge researchers were able to geolocate the IPs of a sizable fraction of active miners, creating a novel dataset giving us new insight into Bitcoin's energy mix.

And the results are revealing: Sichuan, second only in the hashpower rankings to Xinjiang, is a province characterized by a massive overbuild of hydroelectric power in the last decade. Sichuan's installed hydro capacity is double what its power grid can support, leading to lots of "curtailment" (or waste). Dams can only store so much potential energy in the form of water before they must let it out. It's an open secret that this otherwise-wasted energy has been put to use mining Bitcoin. If your local energy cost is effectively zero but you cannot sell your energy anywhere, the existence of a global buyer for energy is a godsend.

There is historical precedent for this phenomenon. Other commodities have been employed to export energy, effectively smoothing out ripples in the global energy market. Before Bitcoin, aluminium served this purpose. A huge fraction of aluminum's embodied cost is the cost of electricity involved in smelting bauxite ore. Because Iceland boasts cheap and abundant energy, in particular in the form of hydro and

geothermal, smelting bauxite was a natural move. The ore was shipped from Australia or China, smelted in Iceland and shipped back to places like China for construction.

See also: Bitcoin Miners, US Energy Producers and Moore's Law

This led to an Icelandic economist famously stating that Iceland "export[s] energy in the form of aluminum." Today, Iceland is hoping it can replicate this model with the export of energy via data storage. This is why smelters are located in places where electricity is abundant, and where the local consumers may not be able to absorb all that capacity. Today, many of these smelters have been converted into Bitcoin mines – including an old Alcoa plant in upstate New York. The historical parallels are exquisite in their aptness.

ULTIMATELY IT'S JUST A MATTER OF OPINION AS TO WHETHER THE EXISTENCE OF A NON-STATE, SYNTHETIC MONETARY COMMODITY IS A GOOD IDEA.

So to sum up, part of the reason Bitcoin consumes so much electricity is because China lowered the clearing price of energy by overbuilding hydro capacity due to sloppy central planning. In a non-Bitcoin world, this excess energy would either have been used to smelt aluminum or would simply have been wasted.

My favorite way to think about it is as follows. Imagine a topographic map of the world, but with local electricity costs as the variable determining the peaks and troughs. Adding Bitcoin to the mix is like pouring a glass of water over the 3D map – it settles in the troughs, smoothing them out. As Bitcoin is a global buyer of energy at a fixed price, it makes sense for miners with very cheap energy to sell some to the protocol. This is why so many oil miners (whose business results in the production of lots of waste methane) have developed an enthusiasm for mining Bitcoin. From a climate perspective, this is actually a net positive. Bitcoin thrives on the margins, where energy is lost or curtailed.

It's about the energy mix

Another common mistake energy detractors make is to naively extrapolate Bitcoin's energy consumption to the equivalent CO2 emissions. What matters is the type of energy source being used to generate electricity, as they are not homogenous from a carbon footprint perspective. The academic efforts that get breathlessly reported in the press tend to assume either an energy mix which is invariant at the global or country level. Both Mora et al and Krause and Tolaymat generated flashy headlines for their calculations of Bitcoin's footprint, but rely on naive extrapolations of energy consumption to CO2 emissions.

Even though lots of Bitcoin is mined in China, it's not appropriate to map China's generic CO2 footprint to Bitcoin mining. As discussed, Bitcoin seeks out otherwise-curtailed energy, like hydropower in Sichuan, which is relatively green. Any reliable estimate must take this into account.

Silver linings

The prospects look even sunnier when you consider the changing nature of Bitcoin security spend. Eighty-seven percent of Bitcoin's terminal supply has been issued already. Due to the path Bitcoin's price took during the heavy-issuance phase, miners will have been collectively rewarded just over $17 billion in

exchange for finding those coins (assuming simply that they sold their coins when they mined them), even though the coins are worth $160 billion today. This is because most of those coins were issued at cheaper price points.

If Bitcoin ends up being worth substantially more in the future than it is worth today (say, by an order of magnitude), then the world will actually have received a discount on its issuance. The energy-externality of pulling those Bitcoins out of the mathematical ether will actually have been very low, due to the historical contingency of when, price-wise, those Bitcoins were actually mined. In other words: Bitcoin's energy expenditure may end up looking rather cheap in the final analysis. Coins only need to be issued once. And it's better for the planet that they be issued when the coin price was low, and the electricity expended to extract them was commensurately low.

See also: Bitcoin Halving 2020: How the World's Largest Mining Pool Is Helping Miners 'De-Risk'

As any Bitcoin observer knows, issuance as a driver of miner revenue will decline with time. Last week's halving cut the issuance side of miner revenue by half. If I had to make a guess, Bitcoin's periodic halvings will at least offset its appreciation long term, making runaway growth in security spend unlikely. Fees will necessarily grow to account for a much larger fraction of miner income. Fees have a natural ceiling to them, as transactors must actively pay them on a per-transaction basis. If they become too onerous, users will look elsewhere, or economize on fees with other layers that periodically settle to the base chain.

Thus it's unlikely that security spend results in the world-eating feedback loop that has been posited in the popular press. In the long term, Bitcoin's energy consumption is a linear function of its security spend. Like any other utility, the public's willingness to pay for block-space will determine the resources that are allocated to providing the service in question.

Is it worth it?

Now, despite all the caveats listed above, it's undeniable that Bitcoin not only consumes a lot of energy but produces externalities in the form of CO2 emissions. This is not under debate. What Bitcoiners are often confronted about is whether Bitcoin has a legitimate claim on _any _of society's resources. This question relies on a kind of utilitarian logic about which industries should be entitled to consume energy. In practice, no one actually reasons like this. The Bitcoin-energy supplicants are mum when it comes to the energy used to illuminate Christmas lights, to power the data centers behind Netflix or to distribute untold millions of single-serve meal kits. It's clear that because Bitcoin's footprint is so easy to quantify — and an object of revulsion among the chattering classes — it is singled out for special treatment.

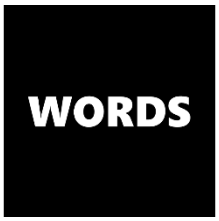
Ultimately it's just a matter of opinion as to whether the existence of a non-state, synthetic monetary commodity is a good idea. The truth is that blockspace is a service which is paid for, and that's where its resource cost is derived. Something duly purchased cannot, by definition, be a waste. Its buyer derives benefit from its existence, regardless of anyone else's subjective opinion of the merit of the transaction. These same arguments have been made countless times about perceived "costs" of the gold standard, and rebutted on similar grounds before. Fundamentally, millions of individuals the world over still value

physical, bank-independent savings, so it still gets pulled out of the ground with regularity. As long as people value Bitcoin, so, too, will the block-space auction continue in perpetuity.

The Bitcoin-energy worriers need not despair, however. There is a solution. All they must do is persuade Bitcoin fans to use and value an alternative settlement medium. Their best bet will be to devise a system that is even more secure, offers stronger assurances, settles faster, is more privacy preserving and is more censor resistant – all without using Proof-of-Work. Such a system would be miraculous. I'm waiting with bated breath.

NOTE: The paragraph beginning "Now, despite all the caveats listed above.." has been updated.

Disclaimer:



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

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

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

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

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

DYOR | BTFD | HODL

I hope you enjoy this project. I'm on a mission to archive the great works of Bitcoin thinkers. Onward!

Read **WORDS**

- @_joerodgers