CRYPTO WORDS

CY19 August

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

Contents

Goals and Scope

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

History

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

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

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

Support Crypto Words

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

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

Spread the word

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

Follow us on social media

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

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

Twitter

Subscribe to our newsletter

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

Our pledge

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

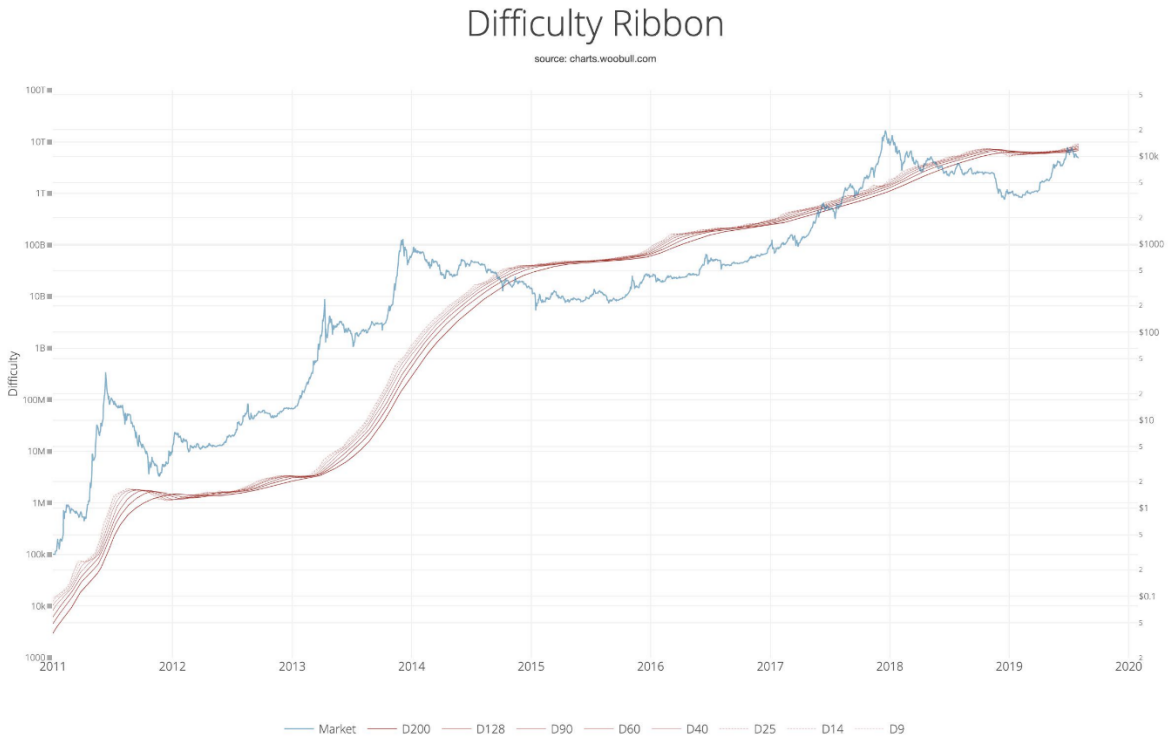
Subscribe

Introducing the Difficulty Ribbon, signaling the best times to buy Bitcoin

By Willy Woo

Posted August 1, 2019

Introducing the Bitcoin Difficulty Ribbon. When the ribbon compresses, or flips negative, these are the best times to buy Bitcoin. The ribbon consists of simple moving averages on mining difficulty so we can easily see the rate of change in difficulty.



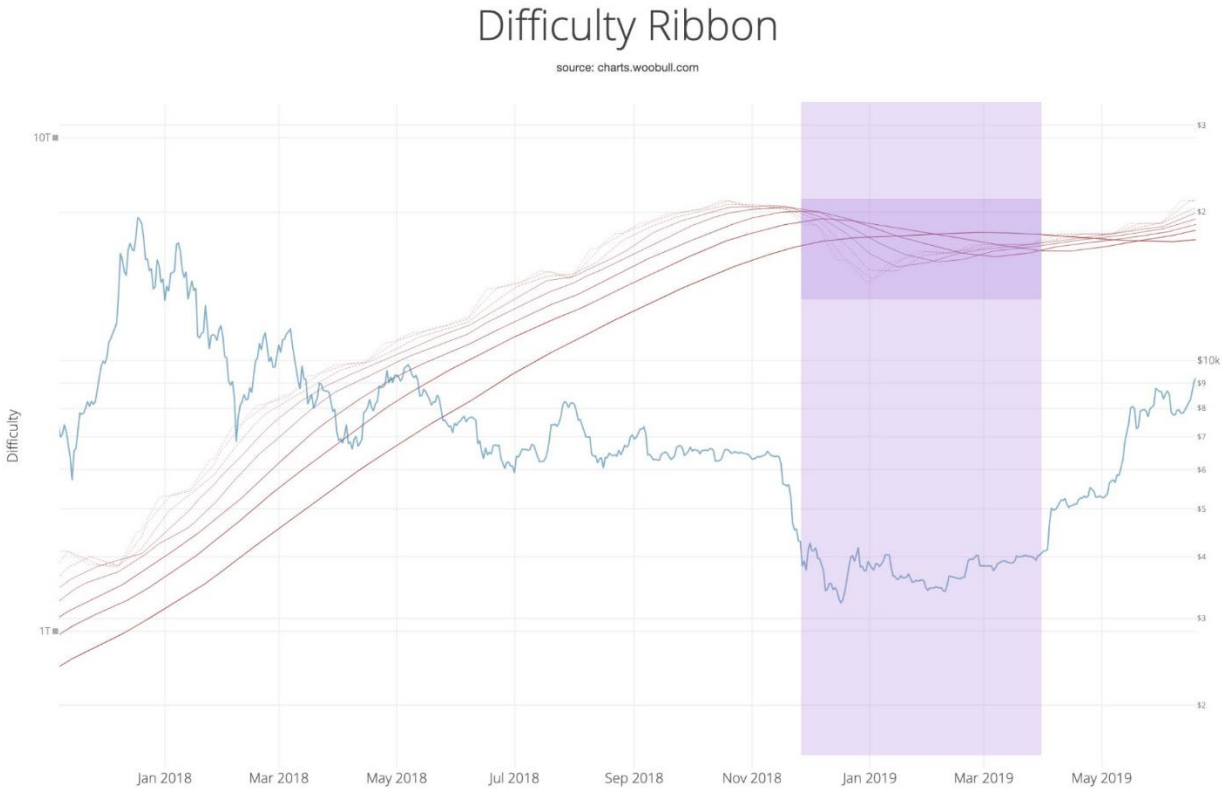
How it the Difficulty Ribbon works

This visualisation of network mining difficulty speaks to the impact of mining on Bitcoin's price. As new coins are mined into existence, miners sell some of their mined coins to pay for production costs. This produces bearish price pressure.

The weakest miners sell more of their coins to remain operational. When it becomes unsustainable, they capitulate, hashing power and network difficulty

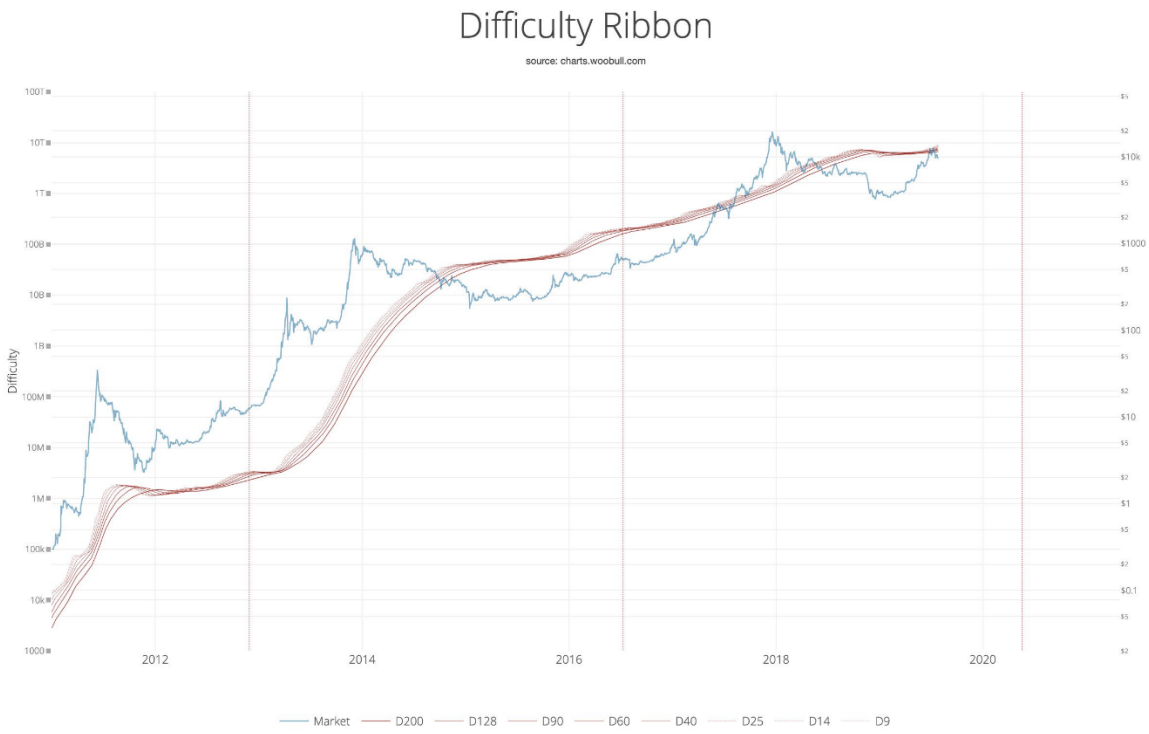
reduces (ribbon compression), leaving only the strong, who sell less leaving more room for more bullish price action.

Typically we see this at the end of bear cycles, after miners capitulate, the lack of miner selling pressure allows the price to stabilise and then climb; the classic accumulation bottom.

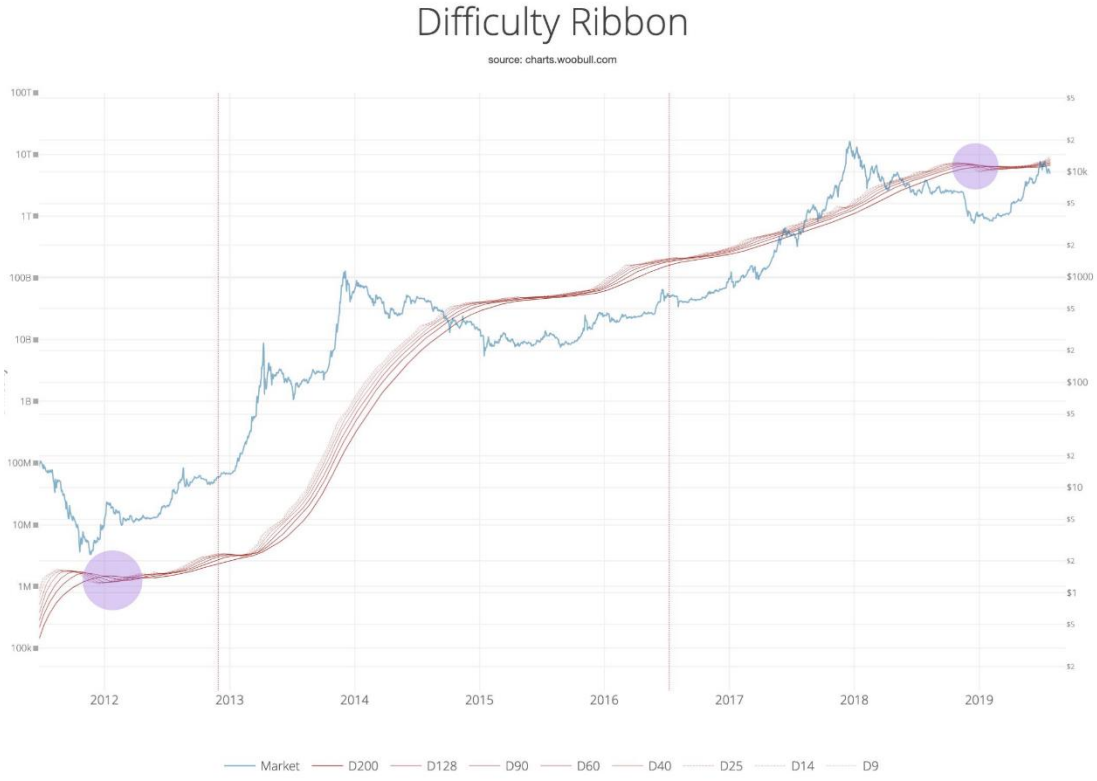


Credit goes to Vinny Lingham who was the first as far as I know to spot this dynamic in his April 2014 article on how Bitcoin finds its price equilibrium . We now have 5 more years of data to back it up.

Miners capitulate in bears, but also during block reward halvening events when suddenly only half the coins are mined for the same costs and the market price has yet to catch up to pay for it. We can easily see the compression after each halvening (marked as vertical lines) as miners die off.



As a final note, notice how the 2019 the 2012 bull market have the same structure, we saw severe mining capitulation (i.e. the ribbon flipped negative), the resulting vacuum in selling pressure lead to a shorter accumulation band before price breakout. Thus this bull market has resembles 2012 more than 2016 structurally.



Tweet: Bitcoin's Power Balance

By Nic Carter

Posted August 1, 2019

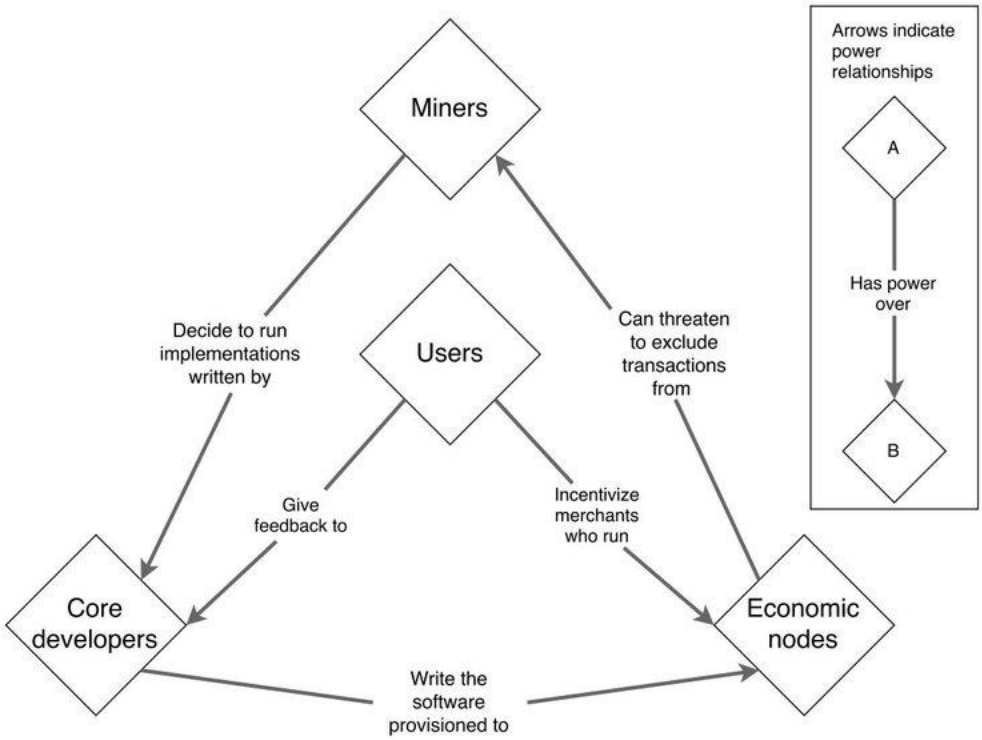
Happy UASF day*

*nothing actually happened on this day in 2017 but it was decreed as Segwit lock in day so we're going to celebrate it anyway

UASF is the most important event in bitcoin's history (in my opinion) and it is absolutely critical to understand bitcoins "governance" (call it what you will)

I modeled bitcoin's power balance like this after the event, I'm fairly pleased at how it has held up.

Bitcoin's governance is set out in De Philippi and Loveluck (2016) as an intensely technocratic and closed process among core developers. However recent events challenge this model. Alternative implementations, starting with Bitcoin Cash, were released, invoking market-based arbitration. Prior to this, miners held provably large power relative to developers by blocking the SegWit implementation. This 'veto' was subsequently overruled by the community in the form of the User Activated Soft Fork rebellion, which escalated the debate and saw miners implement SegWit. Protocol-level actions by miners affect extra-protocol decisions by developers, although not exclusively. Thus a tripartite model is set out here, detailed in the figure below.



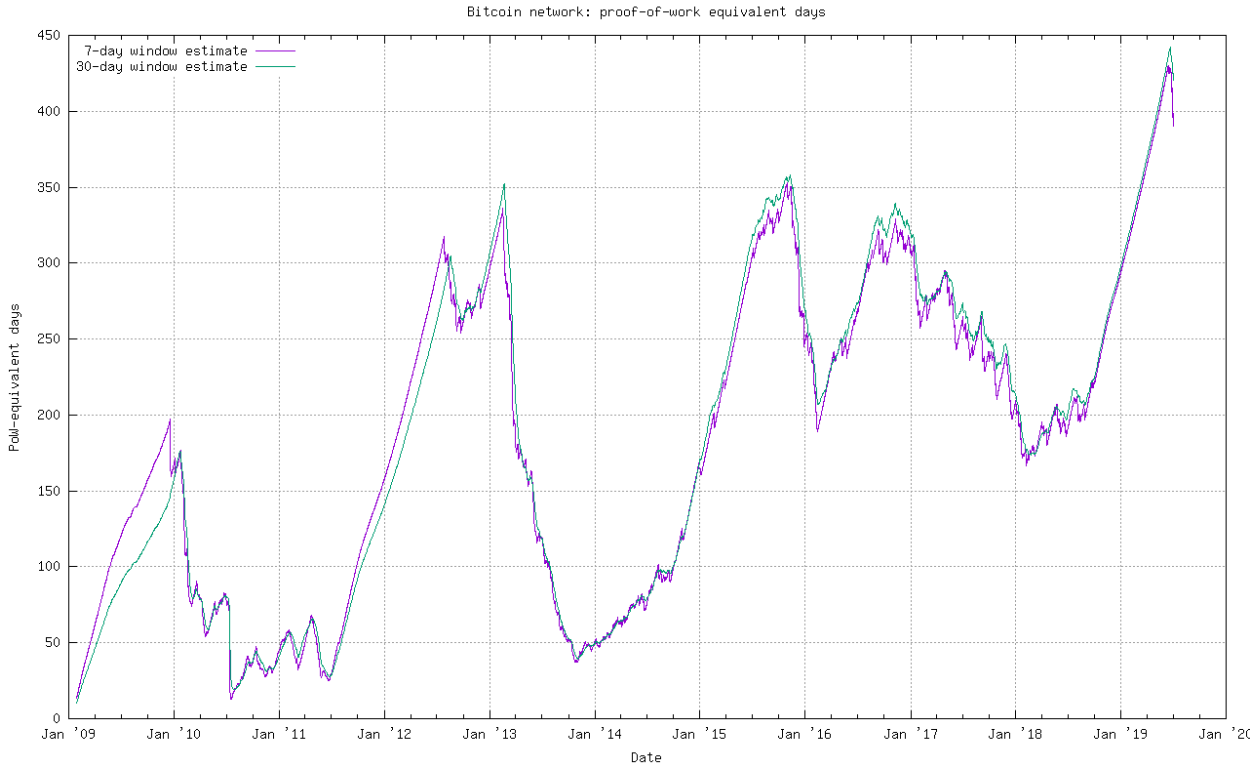
Tweet: Proof of Work Equivalent Days

By Nic Carter

Posted August 1, 2019

So Bitcoin just peaked at an ATH of ~430 “proof of work equivalent days”. That refers to the time required to rewrite Bitcoin’s entire history if you had 100% of hashpower.

Chart here: http://bitcoin.sipa.be



We need Bitcoin full nodes. Economic ones.

By Stadicus

Posted August 1, 2019

Why is it important to run your own Bitcoin full node to have a say regarding Bitcoin consensus and verify your own transactions?

Bitcoin is about financial sovereignty. It's about holding a scarce bearer asset that cannot be counterfeited, seized or frozen. It' s about being part of a peer-to-peer network that does not employ middlemen to facilitate financial transactions. It is free speech money.

As a bearer asset that you truly own, private keys need to be in your possession, managed by a modern Bitcoin wallet application. It's hard to store digital secrets securely on potentially malware-riddled computers, so hardware wallets are a good way to keep your private keys out of the hands of hackers.

But who guarantees that my bitcoin are really there?

A hardware wallet stores your private keys, but not your actual bitcoin. The wallet usually comes with a software companion app that allows you to manage your funds. But this software wallet is not downloading and verifying blocks from the Bitcoin network, so how can it know what your Bitcoin balance is?

Can it guarantee that your hard-earned bitcoin are really there? That an incoming transaction really confirmed on the blockchain?

The answer is that by default you are putting all your trust in a single party: your wallet provider. Lightweight software wallets are mostly nice interfaces to some Bitcoin application backend. Whoever runs this backend controls what you see in your wallet. Your provider tells you how much bitcoin you own. Your provider broadcasts all of your transactions and suggests what fees you have to pay. Your provider runs your access gateway to Bitcoin, assures you that this one big incoming transaction really happened and decides whether it is valid or not. Your provider enforces consensus rules for you and all other customers.

A pretty good vantage point

Your access gateway to the Bitcoin network potentially knows everything. For example, it could easily correlate all your transactions, addresses and balances. As your network address is known, so is your approximate geographical location. Connecting many pseudonymous address clusters through their peer-to-peer transactions, connecting them to well known addresses of

exchanges and merchants could give a very detailed account of the whole Bitcoin ecosystem.

As a wallet provider ourselves, we haven't chosen to run these backend systems, it's simply necessary to provide a good user experience. Most providers probably don't even want to take this role and the power this gives us. Of course, we and other providers promise not to misuse this power. We don't analyze transactions, nor keep logs on our Bitcoin servers. There's nothing to gain by betraying the trust of our customers.

But what about legal coercion through a court order? A rogue employee bribed by a malicious actor? Or a hacker gaining access to the backend applications, altering them just so slightly?

In the not so distant future, when big business and central banks realise that Bitcoin is challenging their financial monopolies, the fight will be on. Once we leave the honeymoon phase, Bitcoin cannot afford such centralized choke points.

It is dangerous for Bitcoin users to outsource their direct network participation to a centralized node. There are a few really big nodes in the network, processing a lot of economic activity. They are actively validating blocks, processing transactions and updating balances. They verify how many bitcoin belong to which address and can judge whether miners behave according to the desired consensus rules. Some lightweight Bitcoin wallets (like our own BitBox App) independently check at least proof-of-work requirements and verify if a transaction has been mined using Merkle branch proofs, but these checks cannot provide definitve proof.

The good news is that it's not that hard to run a Bitcoin full node yourself. After all, that's what the Bitcoin Core application is all about. Run it on your regular computer, an old laptop or as an always-on network appliance like a Raspberry Pi. Run a node and support the network! But unless you are using your node to verify your transactions, just running an idle full node is not really achieving anything.

A harsh truth: only economic nodes matter

Propagating transactions and serving blocks to other peers is nice, but the network doesn't really need additional nodes to do that. In an ad-hoc network like Bitcoin, more nodes do not make it faster or more efficient. What the Bitcoin network really needs are more nodes that enforce the Nakamoto consensus: rules each node follows and applies to decide whether a block or a transaction is valid.

Enforcing consensus: but against whom? Well, anyone that likes to profit just that little bit more. So pretty much everyone. Miners might give themselves a

bigger block reward, regular users spend the same bitcoin twice or a business tries to spend a multi-signature contract unilaterally. Why not cheat on the Lightning Network and create a transaction that ignores a timelock?

But ultimately, it comes down to the miners. While I can create and broadcast as many fake transactions as I'd like for free, a miner that includes it in a block will lose the whole block reward while bearing the full operational costs of producing that invalid block.

Dystopia: let's think it through

Imagine a worst-case scenario, where there are only two big economic nodes, some miners and a hundred idle nodes. What happens if there is business- or miner-driven desire to change the consensus rules, for example to allow bigger blocks? Let's take a look:

1. Some big miners decide that it's time for bigger blocks, because more transactions mean more fees in total.
2. The two big economic nodes think that this is a good idea, as cheap transactions are good for business.
3. The idle nodes don't like that and threaten to not accept bigger blocks.
4. But the miners don't care. All they want is to sell their newly minted bitcoins, which will be accepted by the economic nodes. So they start producing bigger blocks.
5. The economic nodes accept these blocks, bringing them into the Bitcoin ecosystem and giving them value.
6. The hundred idle nodes reject these blocks and the Bitcoin network silently undergoes a hardfork. Unfortunately for the idle nodes, their side of the fork does not have any economic activity, so nobody even notices.
7. As the owners of the idle nodes also use the two economic nodes to send and receive Bitcoin, they are forced to accept the new consensus rules.

That was quick!

Of course it's not as clear cut. For example, customers of the big economic nodes would complain. But without running their own economic nodes, they don't really have a say. This extreme example demonstrates that idle nodes don't really count. Now the good news: in aggregate, many small nodes with just a little economic activity have a huge say when it comes to consensus rules. In the end, it's about threatening to reject transactions which you cannot do if your incoming transactions are processed by someone else.

Relationship status: it's complicated

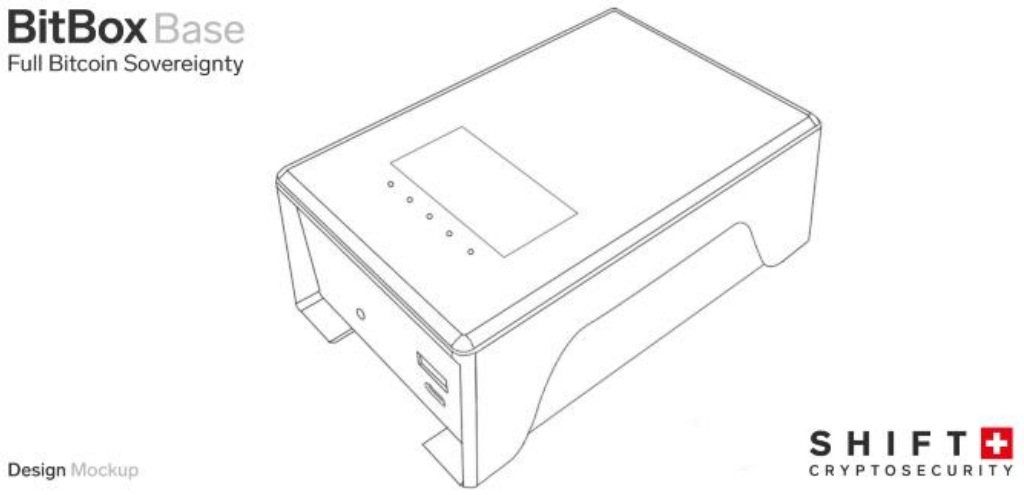
It's important that we learn to be direct participants in the Bitcoin network. There are different ways to do that, but unfortunately Bitcoin Core is not yet sufficiently in love with hardware wallets.

Run Bitcoin Core as your wallet. The Bitcoin reference client is the most popular implementation of the Bitcoin protocol: a full node that validates the whole blockchain on your regular computer and is best used with it's own included software wallet. It's not made with hardware wallets in mind, and while support for them is coming, it's not yet ready for non-techies.

Run an Electrum server. As Bitcoin Core is not made to serve other wallets, the traditional way is to run Bitcoin Core plus an Electrum server. This way, you can use the Electrum desktop application that works seamlessly with most hardware wallets. Our BitBox Applets you specify your own Electrum server, so you can easily use the BitBox hardware wallet in private.

There are several server implementations: electrs, ElectrumX or Electrum Personal Server.

Buy a Full Node appliance (or build it yourself) The most convenient way to run a full node is to buy a ready-made Bitcoin and Lightning Network appliance, or you can build your own (that's how we started). But hardware wallet integration is not quite as seamless as it could be which is why are working on our BitBox Base appliance. The BitBox Base integrates directly into the BitBox App so you are truly sovereign. You can use other wallets too as this is about providing the appropriate privacy for all of us.



If you want to learn and grow, then my RaspiBolt guide as well as the more feature-rich RaspiBlitz project are well worth your time investment.

Mass adoption? Only with better solutions.

While the Lightning Network gave a boost to the number of Bitcoin full nodes, many are not used to verify economic transactions and secure the Bitcoin network. In my experience, many users are not aware that this is an absolute necessity. I believe that better solutions need to be built, especially for usage with hardware wallets. This is the main reason why I'm dedicating all of my time to the BitBox Base.

Bitcoin Can't Be Copied

By Parker Lewis

Posted August 2, 2019

Gradually, Then Suddenly

As kids, we all learn that money doesn't grow on trees. As a society on the other hand, we have become conditioned to believe that it's not only possible but that it's a normal, necessary and productive function of our economy. Before bitcoin, this privilege was reserved to global central banks (see here for example). Post bitcoin, every Tom, Dick & Harry seems to think that they can create money too. At a root level, this is the audacity of everyone that attempts to create a copy of bitcoin. Whether by hard-forking out of consensus (bitcoin cash), cloning bitcoin (litecoin) or creating a new protocol with "better" features (ethereum), each is an attempt to create a new form of money. If bitcoin could do it, why can't we?

We sit here, in 2019, witnessing the monetization event of an economic good (bitcoin) on the free market for the first time in thousands of years (h/t gold). Rather than stopping to contemplate the weight of that reality or to understand how or why that is possible, many people skip right past it to focus on some derivative or some way to improve upon a problem they didn't see in the first place. Everyone wants to get rich quick, and so long as there is money, there will also be alchemists. Those that attempt to copy bitcoin are our modern day alchemists.

"Everyone wants to get rich quick, and so long as there is money, there will also be alchemists."

They tell us that bitcoin is too slow so they create a copy that is "faster". Or they tell us that bitcoin does not have the capacity to handle the number of transactions required by the global economy so they create a copy that has "greater" scale. Then they tell us that bitcoin is too volatile to be a currency so they create a "more stable" version. It goes on and on. Next its that bitcoin is too rigid and that it needs to be more programmable so they create a copy that is "more flexible". They often even tell us that their creation is not money but instead, it's a vehicle for "payments" or a "utility" or maybe a "global computer fueled by gas". They also try to convince us of a world that has hundreds, if not thousands, of currencies. But make no mistake, in each case, it is their own attempt to create money.

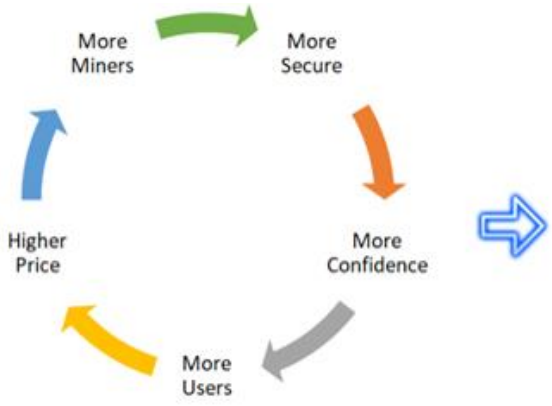
Bitcoin's Value Function

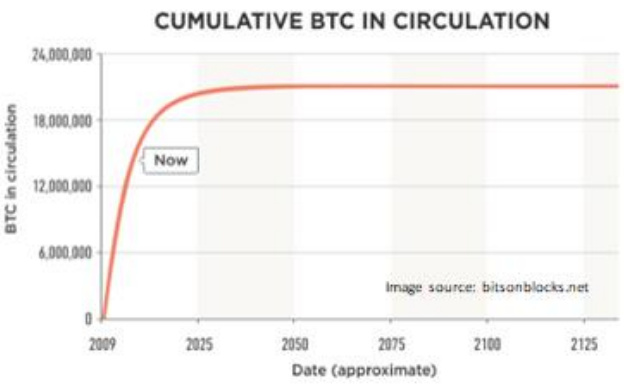
If an asset's primary (if not sole) utility is the exchange for other goods and services and if it does not have a claim on the income stream of a productive asset (such as a stock or bond), it must compete as a form of money and will only store value if it possesses credible monetary properties. With each "feature" change, those that attempt to copy bitcoin signal a failure to understand the properties that make bitcoin valuable or viable as money. When bitcoin's software code was released, it wasn't money. To this day, **bitcoin's software code is not money**. You can copy the code tomorrow or create your own variant with a new feature and no one that has adopted bitcoin as money will treat it as such. Bitcoin has become money over time only as the bitcoin network developed emergent properties that did not exist at inception and which are next to impossible to replicate now that bitcoin exists.

"Those that attempt to copy bitcoin signal a failure to understand the properties that make bitcoin valuable or viable as money."

These properties emerged organically and spontaneously as individual economic actors all over the world evaluated bitcoin and determined to store a portion of their wealth in it. As bitcoin's value increased, it became decentralized and as it became decentralized, it also became increasingly difficult to alter the network's consensus rules or to invalidate, or prevent, otherwise valid transactions (often referred to as censorship-resistance). There remains reasonable debate as to whether bitcoin is sufficiently decentralized or sufficiently censorship-resistant, but while this may be the case, there are other considerations less subject to debate:

1. Bitcoin represents, by far, the most decentralized and most censorship-resistant monetary system in the world today, whether compared to traditional currencies, other digital currencies or commodity monies like gold.
2. Bitcoin derives its value because it is decentralized and because it is censorship-resistant; it is these properties which secure and reinforce the credibility of bitcoin's fixed 21 million supply (i.e. why it is an effective store of value).
3. Bitcoin becomes increasingly decentralized and increasingly censorship-resistant as its value increases and as it scales at all levels of the network.
4. Repeat.





Monetary Systems Tend to One

Every other fiat currency, commodity money or cryptocurrency is competing for the exact same use case as bitcoin whether it is understood or not and monetary systems tend to a single medium because their utility is liquidity rather than consumption or production. When evaluating monetary networks, it would be irrational to store value in a smaller, less liquid and less secure network if a larger, more liquid and more secure network existed as an attainable option.

Apply a common sense test. If you worked for two weeks and your employer offered to pay you in a form of currency accepted by 1 billion people all over the world or a currency accepted by 1 million people, which would you take? Would you request 99.9% of one and 0.1% of the other, or would you take your chances with your billion friends? If you are a U.S. resident but travel to Europe one week a year, do you request your employer pay you 1/52nd in euros each week or do you take your chances with dollars? The practical reality is that almost all individuals store value in a single monetary asset, not because others do not exist but rather because it is the most liquid asset within their market economy.

Anyone with Venezuelan bolivars or Argentine pesos would opt into the dollar system if they could. And similarly, anyone choosing to speculate in a copy of bitcoin is making the irrational decision to voluntarily opt-in to a less liquid, less secure monetary network. While certain monetary networks are larger and more liquid than bitcoin today (e.g. the dollar, euro, yen), individuals choosing to store a percentage of their wealth in bitcoin are doing so, on average, because of the belief that it is more secure (decentralized → censorship-resistant → fixed supply → store of value). And, because of the expectation that others (e.g. a billion soon-to-be friends) will also opt-in, increasing liquidity and trading partners.

"Anyone choosing to speculate in a copy of bitcoin is making the irrational decision to voluntarily opt-in to a less liquid, less secure monetary network."

Why Bitcoin Can't Be Copied

Many individuals creating digital currencies neither accept or admit that what they are creating has to be money to succeed; others that are speculating in these assets fail to understand that monetary systems tend to one medium or naively believe that their currency can out-compete bitcoin. None of them can explain how their digital currency of choice becomes more decentralized, more censorship-resistant or develops more liquidity than bitcoin. To take that further, no other digital currency will likely ever achieve the minimum level of decentralization or censorship-resistance required to have a credibly enforced monetary policy. And to literally steal a page from The Bitcoin Standard:

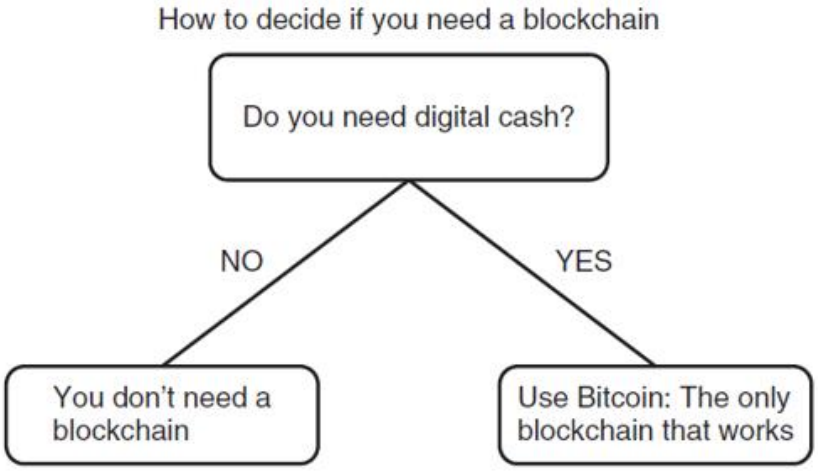


Figure 22 Blockchain decision chart.

Bitcoin is valuable, not because of a particular feature, but instead, because it achieved finite, digital scarcity, through which it derives its store of value property. The credibility of bitcoin's scarcity (and monetary policy) only exists because it is decentralized and censorship-resistant, which in itself has very little to do with software. In aggregate, this drives incremental adoption and liquidity which reinforces and strengthens the value of the bitcoin network. As part of this process, individuals are, at the same time, opting out of inferior monetary networks. This is fundamentally why the emergent properties in bitcoin are next to impossible to replicate and why bitcoin cannot be copied or out-competed: because bitcoin already exists as an option and its monetary properties become stronger over time (and with greater scale), while also at the direct expense of inferior monetary networks.

One would likely never come to this conclusion without first developing their own understanding of the following: i) that bitcoin is finitely scarce (how/why); ii) that bitcoin is valuable because it is scarce; and iii) that monetary networks tend to one medium. You may come to different conclusions, but this is the appropriate framework to consider when contemplating whether it is possible to copy (or out-compete) bitcoin rather than a framework based on any particular feature set. It's also important to recognize that any individual's conclusions, including your own or my own, has very little bearing in the equation. Instead, what matters is what the market consensus believes and what it converges on as the most credible long-term store of value.

The empirical evidence (price mechanism & value) demonstrates that the market continues to determine why bitcoin is different, despite a significant amount of noise. Before speculating, try to understand why bitcoin works and why it's unique. When someone inevitably tells you about a better bitcoin or some differentiating feature, remember that the market, which has come to this same crossroad over the last decade before you, has considered those trade-offs and chosen bitcoin over the field for very rational reasons.

The Minority Rule

Nassim Taleb writes about how a very small intransigent minority can force its preference on the majority, referring to it as the minority rule and explaining why The Most Intolerant Wins. Bitcoin (and monetary systems) are a perfect example of this phenomenon. If a very small minority converges on the belief that bitcoin has superior monetary properties and will not accept your form of digital (or traditional) currency as money, while less convicted market participants accept both bitcoin and other currencies, the intolerant minority wins. This is exactly what is happening in the global competition for digital currency supremacy. A small minority of market participants has determined that only bitcoin is viable, rejecting the monetary properties of all other digital currencies, while the majority is willing to accept bitcoin along with the field. Because of its intransigence, the minority is slowly forcing its preference on the majority. In the world of digital currencies, diversifying by picking the field is the equivalent of letting the crowd (or the intolerant minority) choose what your future money will be, while resigning yourself to only a fraction of what you otherwise would have saved. Evaluate the trade-offs and consider the minority rule before trading in your hard-earned value for a flyer. Money doesn't grow on trees.

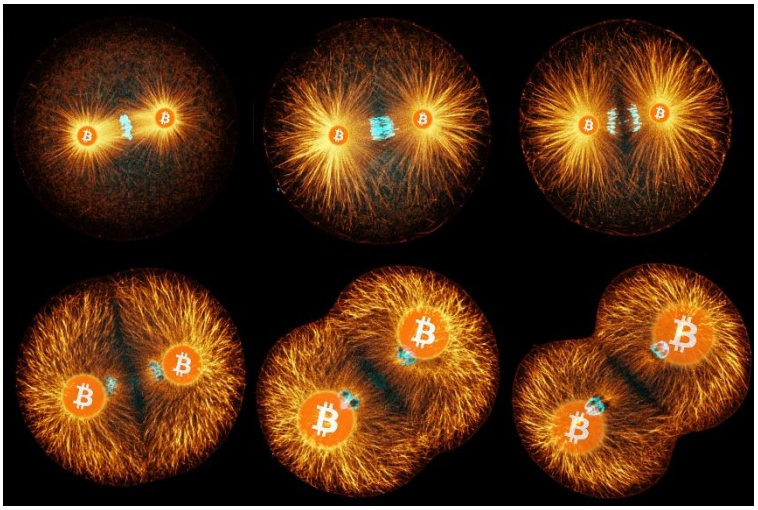
"Bitcoin is a remarkable cryptographic achievement, and the ability to create something that is not duplicable in the digital world has enormous value." – Eric Schmidt (Former Google CEO).

Proof of Life

Why Bitcoin is a Living Organism

By Gigi

Posted August 7, 2019



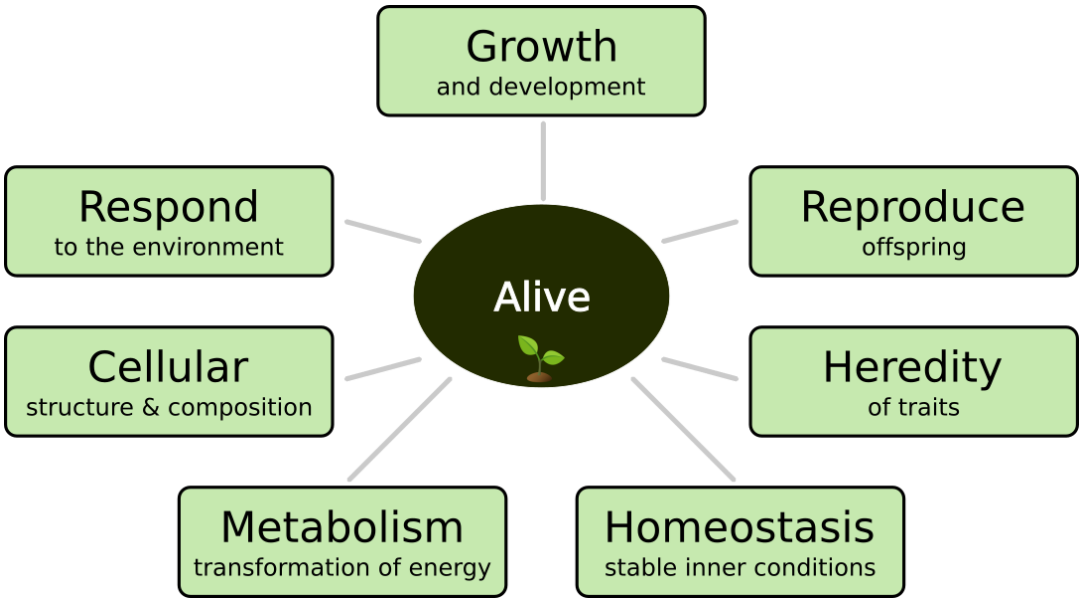
The definition of life has been a challenge for scientists and philosophers alike. While many definitions have been put forward, what precisely differentiates the living from the non-living remains elusive. Are viruses alive? DNA molecules? Computer viruses? Biologically produced minerals? Ralph Merkle, inventor of cryptographic hashing and namesake of the Merkle tree, made the argument that Bitcoin is the first example of a new form of life. In this article series, I intend to take this claim seriously, explore it further, and see what can be gleaned from viewing Bitcoin as a living organism.

The first part will establish that Bitcoin is indeed a living organism. The second part will take a closer look at Bitcoin's various habitats, and how changes in these habitats might affect the organism. In the third part we will dissect the Bitcoin organism, trying to understand some of its parts in more detail. Finally, we will perform the thought experiment of trying to kill Bitcoin, to illustrate the remarkable resilience of this strange, decentralized organism.

What is Life?

The question of whether something is alive or not obviously hinges on one's definition of life. Life is endlessly complex, so it is no surprise that answering the question "What is Life?" leads to a multitude of answers. New-age speculations aside, it seems that life is a process, not a substance.

We can try to describe this process by looking at things which are alive, and looking at what they do: they tend to grow, reproduce, and respond. They inherit traits, are made up of smaller units (cells), and use energy to maintain their internal structure in the face of entropy.



Based on Chris Packard's Characteristics of Life, cc-by-sa 4.0

From a physics perspective, living things are thermodynamic systems: they utilize the energy-differences in their surroundings to maintain a specific molecular organization and create copies of themselves. Thermodynamically speaking, living systems are able to decrease their internal entropy at the expense of "free" energy taken in from the environment. In short, living things create order out of chaos.

Bitcoin is doing exactly that: it takes energy from the environment and puts things in order, i.e. it decreases its internal entropy. It does so by appending blocks to a well-ordered structure. Some call this structure the blockchain, others call it a distributed ledger. I will refrain from using either name, since the name of this particular structure isn't important, and doesn't help to convey a deeper truth: that this structure is just one part of a large and complex system, just like the backbone in vertebrates. It is important, no doubt. But distributed or not, a ledger on its own is as useful and as alive as a bag of bones.

To understand why Bitcoin behaves animatedly we will have to look beyond the buzzwords and ask ourselves what Bitcoin actually is, what it is made of, and what its boundaries are.

What is Bitcoin?

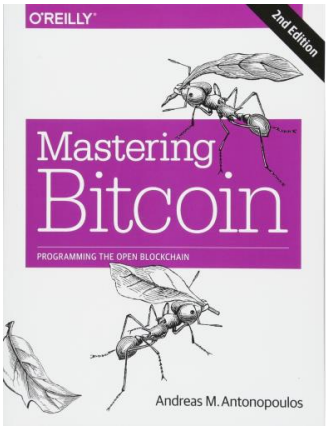
Compared to biological life, Bitcoin is quite simple. Nevertheless, finding a succinct answer to "What is Bitcoin?" is not.

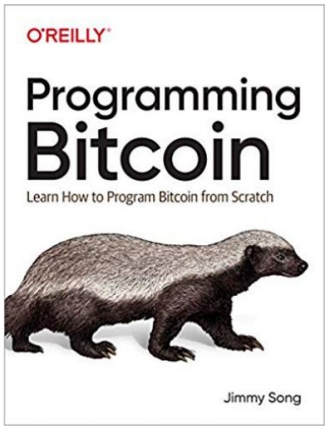
Depending on your background it might be a computer network, a financial revolution, a way to protect your wealth, a payment system, a global

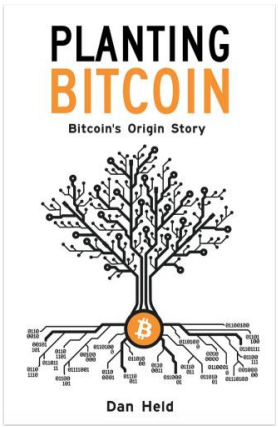
settlement layer, an alternative to central banking, sound money, a parallel economy, an exercise in free speech, a bubble, a pyramid scheme, a messaging system, a communications protocol, an inefficient database, internet money, or all of the above. In short, Bitcoin is different things to different people.

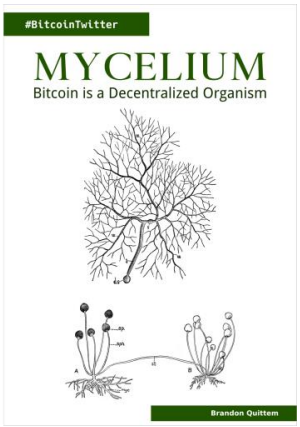
Whatever Bitcoin might be, it undoubtedly is a force to be reckoned with. It has a life of its own, and thus arguably, it is best described as a living thing.

Many people seem to have come to this conclusion independently. Bitcoin is described as an army of leaf-cutter ants in Andreas M. Antonopoulos' Mastering Bitcoin — a biological system which is working in concert without a central coordinator. The honey badger, an animal which is commonly used to refer to Bitcoin (since it doesn't care and isn't afraid of anything) is on the cover of Jimmy Song's Programming Bitcoin. Dan Held compared the invention of Bitcoin to planting a tree, examining the species (code), season (timing), soil (distribution), and gardening (community) that were essential to its success. Brandon Quittem postulates that Bitcoin is most similar to mycelium, the underground network which powers the fungi kingdom, and can thus be best understood as a decentralized organism.









The snake of regulation and central banking is biting you while you are eating it alive? *Honey badger don't care!* And just like an army of ants doesn't care if half of the workers are washed away by a flood, the Bitcoin network doesn't care if half of the nodes are offline tomorrow.

"Honey badger don't care, honey badger don't give a fuck." — Randall

Memes like these, especially if they survive and continue to be popular over a long period of time, tend to be right, conceptually. What people seem to be saying when they refer to Bitcoin as the honey badger is that, in essence, Bitcoin behaves like an animal which can't be controlled, can't be tamed, and doesn't care too much about externalities.

Which particular organism Bitcoin resembles most closely will be left as an exercise for the reader. The above examples should merely illustrate that

multiple authors made the intellectual leap of classifying Bitcoin as a living organism - a leap which I believe to be fascinating, useful, and ultimately, correct.

Bitcoin is a living organism, and we should try to understand it as such if we want to live in harmony with it.

The Bitcoin Organism

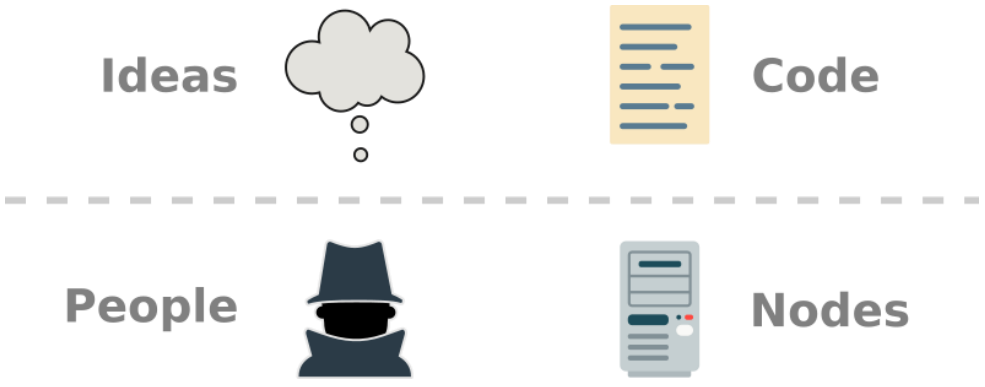
As mentioned above, Ralph Merkle was the first to point out that Bitcoin can be seen as a living entity. He remarked that Bitcoin has spawned an incredible amount of excitement in the technical community, and tried to translate this excitement into something which can be understood by everybody: a new form of life.

“Briefly, and non-technically, Bitcoin is the first example of a new form of life. It lives and breathes on the internet. It lives because it can pay people to keep it alive. It lives because it performs a useful service that people will pay it to perform. It lives because anyone, anywhere, can run a copy of its code. It lives because all the running copies are constantly talking to each other. It lives because if any one copy is corrupted it is discarded, quickly and without any fuss or muss. It lives because it is radically transparent: anyone can see its code and see exactly what it does.” — Ralph Merkle

While Bitcoin is indeed radically transparent, it is not perfectly obvious where Bitcoin begins and where it ends. Like all living things, Bitcoin isn’t just a uniform blob of matter. It is a dynamic, *living* thing, consisting of many different parts, all of which communicate with and influence each other, as well as other living things and the environment as a whole.

The Bitcoin organism is made up of many interlocking parts which work together to ensure the survival of the whole. As with biological organisms, as soon as one crucial part is missing, the whole organism is bound to die.

Bitcoin, however, is a strange beast. It lives across domains, with one foot in the purely informational realm (ideas and code) and one foot in the physical realm (people and nodes).



The Bitcoin organism manifests itself through the interplay of ideas, code, people, and nodes. All four of these conceptual pieces react to and influence each other in a value-generating feedback loop which keeps Bitcoin alive.

Whether people are part of the Bitcoin organism, or merely living in symbiosis with it, depends on your point of view. For now, let's take an all-encompassing view of the Bitcoin organism, including people as one part of the whole. After all, just like we can't live without a multitude of bacteria, fungi, viruses and other creepy-crawlies which make up the human microbiome, Bitcoin can't live without us: the tiny beings in meatspace which keep it alive.

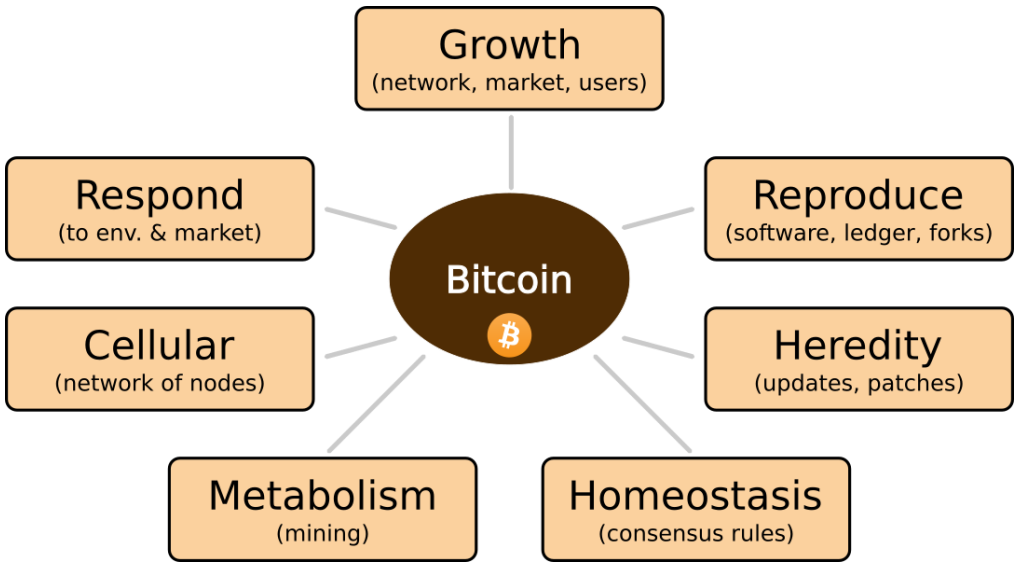
In any case, nodes and their operators are tangible things which are manifest in the physical world. Like the cells in your body, all physical components of the Bitcoin organism can and will be replaced over time. Node operators come and go, node and mining hardware is replaced periodically, and even whole mining farms go offline and are replaced by more cost-efficient facilities.

Ideas and code are more ethereal. They can't be grasped or pointed to in the same fashion. However, Bitcoin has an *essence*, the *soul* of the organism, if you like. Note that this essence could, in theory, breathe life into a new host if the current incarnation of the organism dies. The ghost of Bitcoin is independent of its physical body, to borrow a metaphor from Shirow's *Ghost in the Shell.*

As long as something is compatible with this essence, it will be treated as part of the whole. If something is incompatible, however, it will be rejected — just like biological organisms reject foreign objects inside their bodies.

Part of this essence is made explicit by Bitcoin's consensus rules, other parts are repeated as mantras: " *not your keys, not your bitcoin*" and " *run your own node*" are gentle reminders of lessons learned, as well as shortcuts to a deeper understanding of what Bitcoin is and should be.

With a basic idea of the constituents and the extent of the Bitcoin organism in mind, let's return to the descriptive definition of life above and see how Bitcoin maps onto each trait.



- **Growth:** Bitcoin grows in multiple ways. The network grows, the value of each bitcoin grows, the market grows, its user base grows, and the ecosystem as a whole grows as well.
- **Reproduction:** Paradoxically, Bitcoin uses replication to create absolute scarcity. It reproduces itself in multiple ways, and on multiple levels: the source code is replicated across repositories, the software is copying itself upon installation, the ledger reproduces itself on every node, blocks propagate across the network by replication, and even UTXOs can be understood as reproductive entities, dividing and merging during the transaction process. Mutations exist on every level as well: invalid transactions, invalid blocks, hundreds of forks, and thousands of imperfect copies have been spawned by Bitcoin in the last couple of years.
- **Heredity:** Bitcoin inherits several traits from its predecessors: public-key cryptography, digital signatures, peer-to-peer networking, digital timestamping, and unforgeable costliness — just to name a few. Further, Bitcoin's open nature enables both vertical and horizontal gene transfer: some traits develop by gradual mutations of previous versions, others find their way into the codebase by incorporating ideas from other projects.
- **Homeostasis:** Above all else, Bitcoin's consensus rules are responsible for its stable inner conditions. If blocks do not adhere to the current consensus rules, they will be rejected mercilessly and quickly. The Bitcoin network will rid itself of these blocks just like we shed the dead cells of our skin.
- **Metabolism:** Mining rigs around the world keep the organism alive, erecting virtually impenetrable walls in the process. Energy is transformed into digital amber, ensuring that the shield around past transactions is growing and Bitcoin's heart keeps beating.

- **Cellular:** Multiple parts of Bitcoin are cellular: the Bitcoin network consists of nodes, each of which a self-sustaining, functional entity. The ledger itself is cellular since blocks (and transactions) are basically cells in a large, append-only spreadsheet.
- **Responsive:** Bitcoin is a highly responsive organism. It responds to changes in price, political changes, economic changes, environmental changes (e.g. if parts of the internet are cut off), technological changes (e.g. breakthroughs in chip manufacturing), and changes in our scientific understanding (e.g. breakthroughs in computer science, mathematics, or cryptography). It reacts on its own, without any person, company, or nation-state in charge.

As mentioned above, life is a process, not a substance. A delicate dance of innumerable parts, all signaling and communicating in an intricate way to self-sustain each organism, and the phenomenon which we call life as a whole.

"Life is like fire, not water; it is a process, not a pure substance. [...] The simplest, but not the only, proof of life is to find something that is alive." — Christopher McKay

In the words of astrobiologist Chris McKay, the simplest proof of life is to find something that is alive. I have found Bitcoin, and as far as I can tell, it is alive — for all the reasons outlined above.

Conclusion

Bitcoin checks all the boxes when it comes to the characteristics of living things: it grows, reproduces, inherits and passes on traits, uses energy to maintain a stable inner structure, is cellular in nature, and responds to the various environments it lives in.

In the next part of this series we will take a closer look at these environments, and how Bitcoin responds to changes in them. Bitcoin lives and breathes on the internet, as Ralph Merkle beautifully said. But arguably, the internet isn't the only environment it is living in.

For now, I hope to have convinced you that Bitcoin can be seen as a living organism — alien as it may be.

Further Reading

- Bitcoin is a Decentralized Organism by Brandon Quittem
- Planting Bitcoin by Dan Held
- DAOs, Democracy and Governance by Ralph C. Merkle

- Bitcoin's Gravity by Gigi

Acknowledgements

Thanks to Dan Held,Brandon Quittem, and Raph for their feedback on earlier drafts of this article.

I hope you have enjoyed this excursion into the world of the Bitcoin organism. If you like to accelerate the growth of both Bitcoin and this article series feel free to drop me a line, some applause on medium, or even some sats via the beast which is Bitcoin. Thanks for all the encouragement, and thank you for reading.

Thanks to Brandon Quittem and Dan Held.

Bitcoin Layers

By Joe Rodgers

Posted August 8, 2019

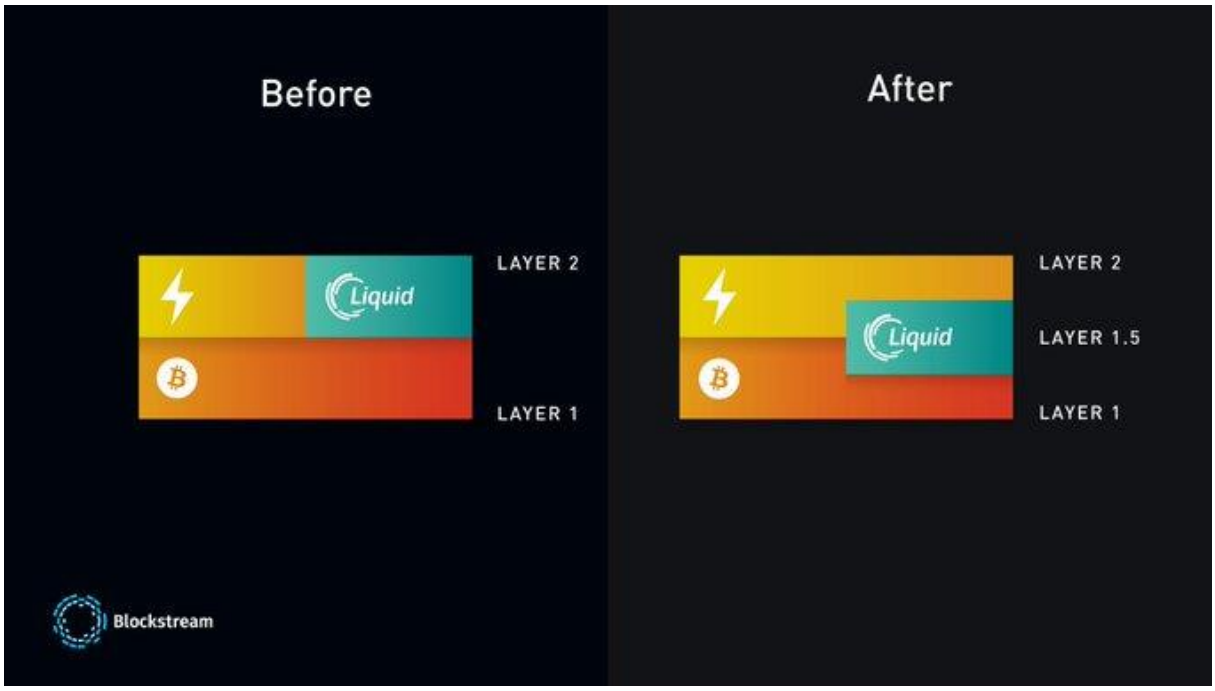
The past few weeks there have been several good threads about Bitcoin's scaling layers. Two camps have emerged as they try to define the stack. While this has no real implications and the market will ultimately decide on the best way to define layers, I wanted to put a post together to show the two camps.

Any Tech Stack

Any technology that allows you to move Bitcoin around without making a Bitcoin L1 transaction, and settles directly on L1.

link to tweet

This is consistent with our friends at Blockstream, they have put out a simple graphic with their view on things.



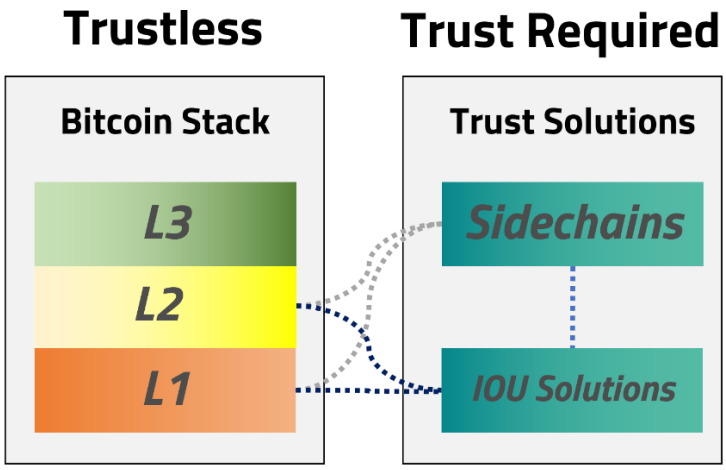
link to tweet

As you can see in this image, the “Any Tech Stack” approach shows Lightning Network and Liquid as Layer 2 solutions. With the recent update to Liquid where you can bring Lightning on top of Liquid, they are socializing the idea that Liquid is closer to Bitcoin L1 than Lightning, calling Liquid Layer 1.5.

Bitcoin Stack

On the other side of the spectrum is the camp of folks who believe Bitcoin scaling layers are trustless. These trustless scaling layers allow the transfer and control of Bitcoin. Products and services can be built upon these layers where no permission or trust is required.

Lightning Network is a Bitcoin L2 solution because it is trustless, that is you can retrieve your funds at any time and no one holds them for you.



- Bitcoin L1 (Layer 1) - The Bitcoin chain, upon which additional layers and trust solutions are built.
- Bitcoin L2 (Layer 2) - Allows you to move Bitcoin without making a L1 transaction.
- Bitcoin L3 (Layer 3) - Allows you to move Bitcoin without making a L1 or L2 transaction. Settles on L2.
- Sidechains – trusted solutions where users exchange Bitcoin for a product or service. These solutions have a cryptographic link to Bitcoin layers, which adds additional security. These products and services will help Bitcoin scale, however there are certain tradeoffs such as required trust. Examples: Liquid
- IOU Solutions – trusted solutions where entities hold Bitcoin for you. These solutions offer scalability to Bitcoin; however trust is required as they hold the Bitcoin for you. Examples: Exchanges, Custodial Wallets

The Bitcoin Stack is one piece of the Bitcoin scaling solution and can work with fantastic emerging Trust Solutions such as Sidechains and IOU Solutions.

Conclusion

I believe trust is a fundamental part of defining Bitcoin scaling technology. It's my belief that it's only Bitcoin L2 if the technology retains Bitcoin's trustless nature. For this reason, I believe Sidechains and IOU Solutions should be defined as trust solutions in the trust stack for Bitcoin, rather than L2 scaling technology.

There is no doubt that Sidechains and IOU Solutions will play a vital role in the scalability of Bitcoin, but let's not call them L2.

Markets clear.

Thanks to 6102 for helping me think through this.

Bitcoin Is Not Too Volatile

By Parker Lewis

Posted August 9, 2019

Has anyone you respect ever told you that bitcoin doesn't make any sense? Maybe you've seen the price of bitcoin rise exponentially and then seen it crash. You write it off, believe your friend was right, don't hear about it for a while and think bitcoin must have died. But then you wake up a few years later, bitcoin hasn't died and somehow its value is a lot higher again. And you start thinking maybe your skeptical friend wasn't right?

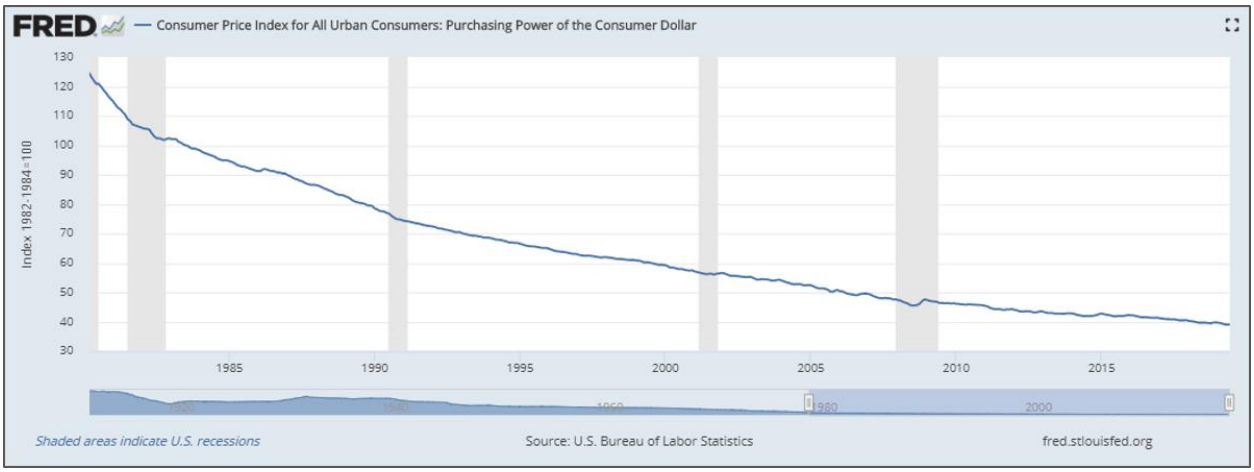
The list of bitcoin skeptics is long and distinguished (see here), but the noise contributes directly to the antifragile nature of bitcoin. People that store wealth in bitcoin are forced to think through first principles in order to understand characteristics of bitcoin which otherwise seem, on the surface, to contradict an establishment view of money, which ultimately hardens convictions. Bitcoin volatility is one of these oft-criticized characteristics. A common refrain among skeptics, including central bankers, is that bitcoin is too volatile to be a store of value, medium of exchange or unit of account. Given its volatility, why would anyone hold bitcoin as a savings mechanism? And, how could bitcoin be effective as a transactional currency for payments if its value could reasonably drop tomorrow?

The principal use case for bitcoin today is not as a payments rail but instead as a store of value, and the time horizon for those that store wealth in bitcoin is not a day, week, quarter or even a year. Bitcoin is a long-term savings mechanism and stability in the value of bitcoin will only be realized over time as mass adoption occurs. In the interim, volatility is the natural function of price discovery as bitcoin advances down the path of its monetization event and toward full adoption. Separately, bitcoin does not exist in a vacuum; most individuals or businesses are not singularly exposed to bitcoin and exposure to multiple assets, like any portfolio, mutes volatility of any single asset.

Not Volatile ≠ Store of Value

It is fair to say that volatility and store of value are often confused as mutually exclusive. However, they most certainly are not. If an asset is volatile, it does not mean that asset will be an ineffective store of value. The opposite is also true; if an asset is not volatile, it will not necessarily be an effective store of value. The dollar is a prime example: not volatile (today at least), bad store of value.

"Volatile things are not necessarily risky, and the reverse is also true." Nassim Taleb (Skin in the Game)



The Fed has been highly effective in very slowly devaluing the dollar, but always remember, *gradually, then suddenly.* And, not volatile ≠ store of value. This is a critical mental block that many people experience when thinking about bitcoin as a currency, and it is largely a function of time horizon. While central bankers all over the world point to bitcoin as a poor store of value and not functional as a currency because of volatility, they think in days, weeks, months and quarters while the rest of us plan for the long-term: years, decades and generations.

Despite the logical explanations, volatility is one area that particularly confounds the experts. Bank of England Governor, Mark Carney recently commented that bitcoin "has pretty much failed thus far on [...] the traditional aspects of money. It is not a store of value because it is all over the map. Nobody uses it as a medium of exchange," (see here). The European Central Bank (ECB) has also mused on Twitter that bitcoin is "not a currency", noting that it is "very volatile" while at the same time reassuring everyone that it can "create" money to buy assets, the very function by which its currency actually loses value and why it's a poor store of value.

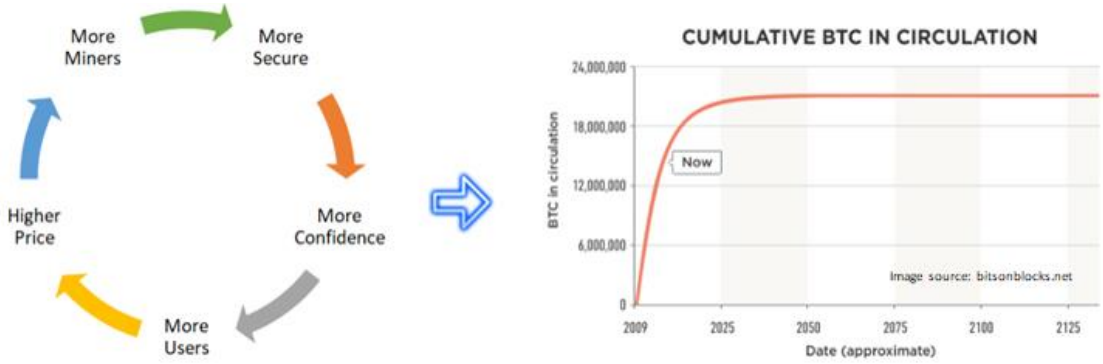
The lack of self-awareness is not lost on anyone here but Mark Carney and the ECB are not alone. From former Fed Chairs, Bernanke and Yellen, to current

Treasury Secretary Mnuchin to the President himself. All have, at times, trumpeted the idea that bitcoin is flawed as a currency (or as a store of value) because of its volatility. None seem to fully appreciate, or at least admit, that bitcoin is a direct response to the systemic problem of governments creating money via central banks or that bitcoin volatility is a necessary and healthy function of price discovery.

But luckily for all of us, bitcoin is not too volatile to be a currency and often the experts are not experts at all. Setting logic aside, the empirical evidence shows that bitcoin has proven to be an exceptional store of value over any extended time horizon despite its volatility. So how could an asset such as bitcoin be both highly volatile and an effective store of value?

Bitcoin Value Function Revisited

Consider why there is fundamental demand for bitcoin and why bitcoin is naturally volatile. Bitcoin is valuable because it has a fixed supply and it is also volatile for the same reason. The fundamental demand driver for bitcoin is in its scarcity. To revisit bitcoin's value function from a previous edition, decentralization and censorship-resistance reinforce the credibility of bitcoin's scarcity (and fixed supply schedule) which is the basis of bitcoin's store of value property:

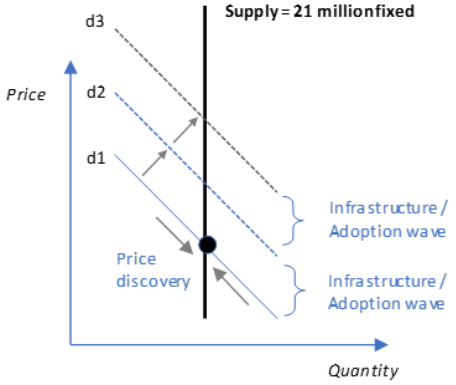


While demand is increasing by orders of magnitude, there is no supply response because bitcoin's supply schedule is fixed. The disparity in the rate of increase in demand (variable) vs. supply (fixed) combined with imperfect knowledge amongst market participants causes volatility as a function of price discovery. As Nassim Taleb writes in The Black Swan of Cairo: *"Variation is information. When there is no variation, there is no information."* As bitcoin's value increases, it communicates information despite the volatility; the variation is the information. Higher value (dependent on variation) causes bitcoin to become relevant to new pools of capital and new entrants which then stokes an adoption wave.

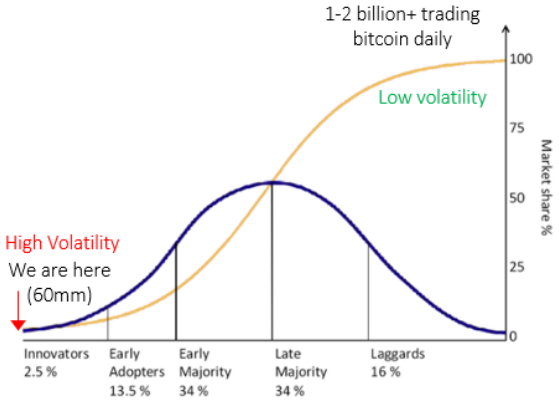
Adoption Waves & Volatility

Knowledge distribution and infrastructure fuel adoption waves and vice versa. It is a virtuous feedback loop and a function of both time and value. As value rises, bitcoin captures the attention and mindshare of a much wider audience of potential adopters, which then begin to learn about the fundamentals of bitcoin. Similarly, an appreciating asset base attracts additional capital not only as a store of wealth but also to build incremental infrastructure (e.g. more on-ramps & off-ramps, custody solutions, payments layers, hardware, mining, etc.). Developing an understanding of bitcoin is a slow process, as is building infrastructure, but both fuel adoption which then further distributes knowledge and justifies additional infrastructure. *Knowledge → Infrastructure → Adoption → Value → Knowledge → Infrastructure*

Fixed Supply vs. Expanding Demand



Stages of Technology Adoption (S-Curve)



Today, bitcoin is still nascent and current adoption likely represents <1% of terminal adoption. As a billion people adopt bitcoin, new adoption will represent orders of magnitude for any foreseeable future period which will continue to drive significant volatility; however, with each new adoption wave, the value of bitcoin will also reset higher because of higher base demand. Bitcoin volatility will only decline as the holder base reaches maturity and as the rate of new adoption stabilizes. Said another way, for a billion people to be using bitcoin, adoption will have had to increase by ~20x, but the subsequent 100 million adopters will only represent an additional 10% of the base. All while the supply of bitcoin remains on a fixed schedule. So long as adoption represents orders of magnitude, volatility is unavoidable, but on that path, volatility will naturally and gradually decline.

As Vijay Boyapati explained on Stephan Livera's podcast, "establishment economists deride the fact that bitcoin is volatile, as if you can go from something that didn't exist to a stable form of money overnight; it's completely ludicrous." What happens between adoption waves is the natural function of price discovery as the market converges on a new equilibrium, which is never static. In bitcoin hype cycles, the rise, fall, stabilization and rise again is almost

rhythmic. It is also naturally explained by speculative fear, followed by accumulation of fundamental knowledge and the addition of incremental infrastructure. Rome wasn't built in a day; in bitcoin, volatility and price discovery are core to the process.

Historical Adoption Wave

For a more tangible explanation of the relationship between volatility and value, it is helpful to think about the most recent adoption wave from the end of 2016 to present (2019).

While adoption can never really be quantified, a rough but fair estimate would be that bitcoin adoption increased from ~5 million people to ~60 million (an increase in demand of ~12 times) from 2016 to present, yet the supply of bitcoin only increased by approximately 10% over the same period. And naturally, the information and capital possessed by market participants varies significantly. As a massive adoption wave occurred, it was met by bitcoin's fixed supply schedule. What would one expect to happen when demand increases by an order of magnitude but supply only increases by 10%? And what would happen if the knowledge and capital of the new entrants naturally varies greatly?

The very logical end result is higher volatility and a higher terminal value, if even a small percentage of new entrants convert to long-term holders (which is exactly what happened). New adopters who initially purchased bitcoin in its astronomical rise, slowly accumulate knowledge and convert to long-term holders, stabilizing base demand at a far higher terminal value compared to the prior adoption cycle.

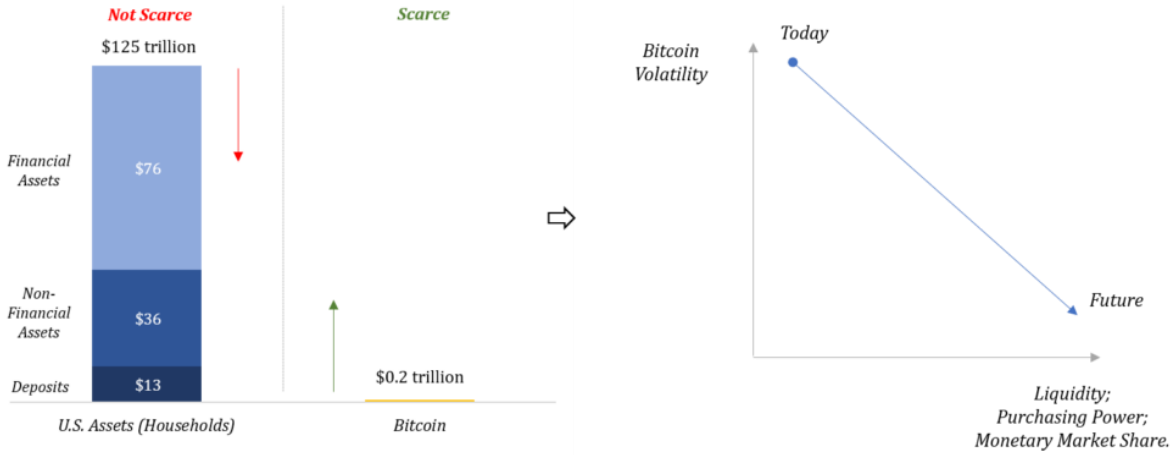
Because bitcoin is nascent, the aggregate wealth stored in bitcoin on a relative basis is still very small (~$200 billion) which allows for the rate of change between marginal buyers and sellers (price discovery) to represent a significant percentage of the base demand (volatility). As base demand increases, the rate

of change will begin to represent a smaller and smaller percentage of the base, reducing volatility over time and only after several more adoption cycles.

Managing Volatility

If we can accept that bitcoin volatility is both natural and healthy, why doesn't current volatility prevent the adoption required to transition bitcoin to a stable form of money? Very simply: diversification, portfolio allocation theory and time horizon. There exists a global network (bitcoin) through which you can transfer value over a communication channel to anyone in the world, and it is currently valued, in total, at less than $200 billion. Facebook alone, on the other hand, is worth in excess of $500 billion. For further frame of reference, U.S. household assets are estimated to be valued at $125 trillion (see here, page 138).

In a theoretical world, bitcoin volatility would be an issue if it existed in a vacuum. In the real world, it doesn't. Diversification comes in the form of real productive assets as well as other monetary and financial assets, which mutes the impact of bitcoin's present volatility. Separately, information asymmetry exists and those that understand bitcoin also understand that, in time, the cavalry is coming. These concepts are obvious to those that have exposure to bitcoin and actively account for its volatility in short and long-term planning, but it's apparently less obvious to the skeptics, who struggle to grasp that bitcoin adoption is not an all or nothing proposition.



While bitcoin will continue to steal share in the global competition for store of value because of its superior monetary properties, the function of an economy is to **accumulate capital** that actually makes our lives better, **not money**. Money is merely the economic good that allows for coordination to accumulate that capital. Because bitcoin is a fundamentally better form of money, it will gain purchasing power relative to inferior monetary assets (and monetary substitutes) and increasingly take market share in the economic

coordination function, despite being less functional as a transactional currency today.

Bitcoin will also likely induce the de-financialization of the global economy, but it will neither eliminate financial assets nor real assets. During its monetization, these assets will continue to represent the diversification which will mute the impact of bitcoin's day-to-day volatility. See example here which highlights the risk/return of a 1% bitcoin + 99% dollar portfolio compared to gold, U.S. treasuries and the S&P 500 (@100trillionUSD). Also see The Case for a Small Allocation to Bitcoin by Xapo CEO Wences Casares. Both provide a look through into how volatility and risk can be managed should bitcoin experience a significant drawdown or even fail (which is still a possibility).

While failure is a possibility and significant drawdowns are an inevitability, each day that bitcoin doesn't fail, its survival becomes more and more likely (Lindy Effect). And over time, as bitcoin's value and liquidity increase due to its fundamental strengths, its purchasing power will also increase in terms of real goods, but as its purchasing power represents a larger and larger share of the economy, its volatility relative to other assets will proportionally decrease.

The End Game

Bitcoin will become a transactional currency over time but in the interim, it would be far more logical to spend a depreciating asset (dollars, euro, yen, gold) and save an appreciating asset (bitcoin). Establishment economists and central bankers really struggle with this one; but I digress. On bitcoin's path to full monetization, store of value must come as a logical first order and bitcoin has proven to be an incredible store of value despite its volatility. As adoption matures, volatility will naturally fall, and bitcoin will increasingly become a medium of direct exchange.

Consider the person or business that would demand bitcoin in direct exchange for goods and services. This person or business collectively represent those that have first determined that bitcoin will hold its value over a particular time horizon. If one did not believe in the fundamental demand case for bitcoin as a store of value, why would they trade real-world goods and services in return? Bitcoin will transition to a transactional currency only as its liquidity gradually shifts from other monetary asset to goods and services which will occur along the path to mass adoption. It will not be a flash cut or a binary process. On a more standard path, adoption fuels infrastructure and infrastructure fuels adoption. Transactional infrastructure is already being built but more material investment will only be prioritized as a sufficient number of individuals first adopt bitcoin as a store of wealth.

Ultimately, bitcoin's lack of a price stability mandate and fixed supply will continue to result in near-term volatility but will drive long-term price stability.

It is the literal opposite model pursued by Mark Carney of the BOE, the ECB (and its twitter account), the Federal Reserve and the Bank of Japan. And, it is why bitcoin is antifragile; there are no bailouts and it's a market devoid of moral hazard, which drives maximum accountability and long-term efficiency. Central banks manage currencies to mute short-term volatility, which creates the instability that leads to long-term volatility. Volatility in bitcoin is the natural function of monetary adoption and this volatility ultimately strengthens the resilience of the bitcoin network, driving long-term stability. Variation is information.

Nassim Taleb & Mark Blyth (Black Swan of Cairo)

"Complex systems that have artificially suppressed volatility tend to become extremely fragile, while at the same time exhibiting no visible risks." "This is one of life's packages: there is no freedom without noise—and no stability without volatility."

Ben Bernanke, Chairman of the Federal Reserve (during the Great Financial Crisis)

"The Federal Reserve is not currently forecasting a recession." – January 10, 2008 "The risk that the economy has entered a substantial downturn appears to have diminished over the past month or so." – June 9, 2008

Projection and Throwness

By The Bitcoin Observer

Posted August 11, 2019

Part III — Bitcoin's 10x Advantage Over Gold Might Not Lie Where You Think

TLDR: This is a multi-part series about the many ways in which Bitcoin is such a unique, inter-disciplinary, and inter-temporal technology. The third part touches on an overlooked advantage of Bitcoin over other traditional forms of commodity money, including gold.

I have been thinking for a while about why sound money survived for thousands of years but was quickly killed in the age of nation-states. When I bumped into this insightful tweet from Nick Szabo the reasons became clear to me. As we will see below, the points he makes are extremely important to understand Bitcoin's advantages over gold. They might go beyond Bitcoin's more rigid monetary policy and also have to do with the limitations of metallic money in regards to the expansion of commerce and trade.

Click here if you would like to read this series from the first text.

The Long and Winding Road From Metallic Coins to Paper Banknotes

Contrary to what some think, fiat money was not implemented suddenly in 1971 when Nixon closed the gold window or in 1974 when the IMF changed the SDR composition from gold to a basket of fiat currencies. Jim Rickards showed in his book *The Road to Ruin* that the classical gold standard was actually killed in stages starting with the Austro-Hungarian ultimatum to

Serbia and the outbreak of World War I in 1914. The next five paragraphs summarize his argument.

Right after the start of WWI, nations were aware that gold reserves were a determinant factor of victory and suspended redemptions in specie. The two exceptions, for different reasons, were the US and the UK. However, that's exactly when gold coin circulations were replaced by 400-oz bars, the gold delivery standard until today, in London, which was the undisputed global financial center at the time. This change gradually disincentivized people to hold and transact money in-specie (a 400-oz gold bar today is worth about $500,000) and use banknotes instead.

With the end of WWI in 1918, the new habit of holding banknotes instead of gold coins was ingrained not only in the UK but throughout Europe and increasingly in the US. Gold could still be privately owned, but it was buried out of sight and out of mind. Another major boost to monetary base centralization was FDR's famous 1934 order 6102 that required US citizens to surrender private gold to the government. Fort Knox was built three years later.

In stages between 1914 and 1934, U.S. gold went from private hands, to bank hands, to central banks, to the Treasury. This paralleled the process that took place in the United Kingdom and other developed economies. Governments made gold disappear.

At the outbreak of World War II, gold convertibility, to the extent that remained, was again suspended. The only major gold dealer at that point was the Bank of International Settlements (BIS). The BIS acted as a broker of Nazi gold, including gold taken from Jews and other Holocaust victims. By the end of WWII, gold did not circulate as currency anymore. The Bretton Woods Agreement of 1944 introduced the gold exchange standard, meaning it applied to nation-states but not to its citizens.

It should be clear by now that it was only a matter of time until the implementation of a full fiat monetary system, which came in 1971 when Nixon closed the gold window. The growing influence of Milton Friedman and his idea of "elastic money" as a remedy that could have avoided the Great Depression provided the intellectual justification politicians needed for the implementation of the monetary system we have until today.

Demonetization Of Silver Revisited

Jörg Guido Hülsmann, probably the greatest monetary economist alive, went a step further and also analyzed the process of demonetization of silver under the perspective of monetary base centralization in his monumental *The Ethics of Money Production*.

Many Bitcoiners believe that gold won the battle against silver due to its higher stock-to-flow ratio. According to Hülsmann, this view is misguided. There is plenty of evidence that the demonetization of silver was not a free market process, but one heavily engineered by governments. Mises seems to be more or less in accord with this view when he discusses this matter in *Theory of Money and Credit:*

And while some thus regarded gold as nothing less than the embodiment of the very principle of evil, all the more enthusiastically did other exalt the glistering yellow metal which aline was worthy to be the money of right and mighty nations. It did not seem as if men were disputing about the distribution of economic goods; rather it was as if the precious metals were contending among themselves and against Paper for the lordship of the market. All the same, it would be difficult to claim that these Olympic struggles were engendered by anything but the question of altering the purchasing power of money.

Here I'll summarize Hülsmann's argument. Until the 1860s, only the US and some major parts of the UK empire had been on what we today call the classical gold standard. Things changed with the German victory in the Franco-Prussian war of 1870–71. Germany obtained an indemnity in gold and used that to institute a monetary model similar to Britain's. The Prussian Central Bank, later rebranded the Reichsbank in a marketing coup, was instituted four years later.

Why did the Germans institute a gold standard and not a silver standard or the bi-metallic systems that were floating around? One factor is that gold had better externalities — Britain, the world's financial center — was on gold and the major silver countries (Austria and Russia) had suspended silver payments at the time of German victory. Gold at that time provided more advantages from an international division of labor standpoint. But Hülsmann points to another reason as well:

Moreover, one should not neglect that silver, the only serious competitor for gold among the commodity monies, has one grave disadvantage from the point of view of a government bent on inflationary finance. Because of its bulkiness, the use of silver entails higher transportation costs, which makes it less suitable than gold for fractional reserve banks trying to quash systematic bank runs through cooperation.

Virtually all western countries followed suit. By the early 1880s, all countries of the West and their colonies had adopted the British monetary model. The silver lining of the classical gold standard was that it demonstrated how a world monetary system can emerge without central coordination. There was no conference, no treaty. The countries adopted it independently of each other.

However, this was done at the discretion of national governments, not at its citizens'. The classical gold standard was brought by the coercive elimination of the alternative monies and it paved the way for government interventions in the monetary system. It ignited the age of national central banks and private fractional-reserve banks taking control of the monetary system. This does not look like a bulwark for the liberty movement.

We have to stress these facts because many advocates of the free market believe the classical gold standard was something like the paradise of monetary systems. This reputation is underserved. The classical gold standard differed only in degree, not in essence, from its successors, all of which have been widely and deservedly criticized in the literature on our subject.

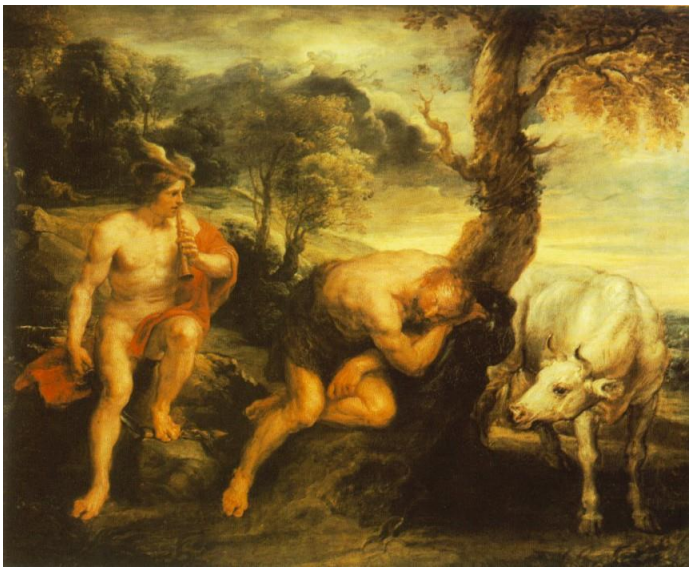
In sum, Hülsman states that the lethal hit that World War I brought to the classical gold standard only anticipated its death from its own cancer. This is not a silver bug argument, but an argument against coercive centralization of the monetary base. Earlier in this same book Hülsmann defines what fiat money is: one that artificially circulates more than the unhampered market would set. This definition also applies to gold in the classical gold standard.

Bitcoin's 10x Improvement Over Gold Might Not Lie Where You Think it Does

So now we understand that the institution of the fiat system was just the culmination of a process that was going on for about one hundred years before Nixon's order in 1971. Citizens were coerced to trade silver coins for gold coins, then gold coins for gold bars stored in private banks and finally to gold bars stored with the government. Without this fiat money would be a lot harder, or maybe even impossible, to implement.

How was this process so swiftly accepted by the population? In my opinion, this centralization of the monetary base that led people to trade in IOUs instead of in specie actually brought some advantages to commerce and trade. As Nick Szabo points out, metallic money is hard to assay/validate and is also relatively hard to transport.

As economic activity expands with respect to number of transactions and to geographical footprint, dealing with physical money becomes impracticable. IOUs were a boon to commerce and trade from this standpoint, despite all the additional trust it required and all the monetary base centralization it entailed. Metallic money does not scale well in response to more commerce and trade activity, fiat money actually beats gold there. Bitcoin fixes this.



Mercury is the Roman god of financial gain, commerce, thieves, among other things. Peter Paul Rubens, a true Bitcoin OG, portrayed in 1635 Mercury rescuing a no-coiner after realizing how Bitcoin makes his job a lot easier. "Bitcoin is sound money, free money, and darknet money", Mercury purportedly said.

Bitcoin makes the cost of transportation and validation negligible without adding any counterparty risk to the system. This monetary evolution can not be overstated. At this point, I also hope that the importance of these properties for a sustainable sound money in the internet age is clear. Metallic money did not survive the age of globalization and nation-states because it did not scale well. Bitcoin optimizes for that while still sustaining the highest stock-to-flow ratio of any monetary asset. That's its 10x improvement right there!

Bitcoin's harder monetary policy compared to gold is usually cited as the main factor that will make it succeed. This is certainly an advantage and a pre-condition for it to be sound money in the first place. However, the question of whether this improvement is enough for Bitcoin to leapfrog gold's massive Lindy effect is a valid one that has been bothering me for a while. Answering this with the possibility of gold mining in space might be a bit far-fetched at this point. The catalyst for Bitcoin's extremely high stock-to-flow ratio to shine is how well it scales with commerce and trade activity.

References

- *The Road to Ruin* by James Rickards. I certainly do not agree with Ricards' views about Bitcoin. However, I appreciate much of his view about money and enjoy his prose. This is a good read for bitcoiners!
- *The Ethics of Money Production* by Jörg Guido Hülsmann. This is required reading for anyone who wants to understand why sound money matters.
- Theory of Money and Credit by Ludwig Von Mises. The best book on money written by the best economist of all time. By now it should be clear why this is required reading.

Tweet: Opinion on Wealth Concentration

By Nic Carter

Posted August 14, 2019

My view on wealth concentration

- bitcoin is an emerging monetary system, it started with a GINI of 1 and decreases over time
- 'fairdrops' don't work; see the voucher programs in the USSR
- the best thing you can hope for is equality of opp. and no seignorage (bitcoin has both)
- long term holders sell out as their wealth increases. this is empirically observable in Bitcoin (@unchainedcap 's Hodl waves analysis makes this point)
- this is a natural and organic force which disperses supply
- wealth concentration is something to worry about if wealth can be transformed into political power, because you kick off a feedback loop of wealth -> power -> discretion over system features -> more wealth
- luckily, bitcoin manifestly does NOT care if you are wealthy
- in this context, the concentration of wealth in bitcoin is not something that worries me, even a little bit. Bitcoin 'governance' is nicely poised between nodes, devs, miners
- if wealth meant power in Bitcoin, S2X would have prevailed. it didn't. compare that with other chains
- given that wealth does NOT equal power in Bitcoin, worrying about the concentration carries sinister undertones
- it insinuates that the outcomes in Bitcoin are 'wrong' and may need to be remediated
- if you believe in free market money, you believe in free market outcomes
- thanks to a decade of PoW and an unrepeatable launch where coins where freely traded for years *without* a $ value, Bitcoin has an enviable distribution
- the chosen metric (% of addresses owning % of supply) is comically bad
- every other coin is empirically more concentrated
- this is a great case study in how data can be both trivially correct and very misleading
- the default thing people do with data is misrepresent things
- this is a difficult subject which requires nuance & a patterned analysis, not just a single metric
- if you think that 'bitcoin is unevenly distributed' will inhibit adoption, you are in for a surprise

- Bitcoin has long succeeded in spite of political unacceptability and bad optics. this probably won't stop it
- fin

Bitcoin Does Not Waste Energy

By Parker Lewis

Posted August 16, 2019

How many times have you heard the safety instructions before a standard commercial flight? You probably know them by heart, but every time, prior to takeoff, flight attendants instruct passengers traveling with children to put their oxygen mask on first and then tend to the children. Instinctively, it's counterintuitive. Logically, it makes all the sense in the world. Make sure you can breathe, so that the child dependent on you can breathe too. The same principle applies to the coordination function of money in an economy and the resources required to protect that function. In a more philosophical safety warning, the flight attendant may say, "please make sure the money supply is secure so that we can continue to coordinate the activity of millions of people to build these hyper complex planes that afford you the opportunity to even contemplate the problem I'm about to explain."

We will come back to this, but you will never hope to understand the justification for the amount of energy bitcoin consumes without first developing an appreciation for the fundamental role money plays in coordinating economic activity and all the things we collectively take for granted. What is money? How does it work? How should it work? What is its function in society? If you haven't stopped to ask these questions, you can't begin to grasp the weight of the problem bitcoin intends to solve. And without an appreciation for the problem, the cost to secure the solution will never seem justified.

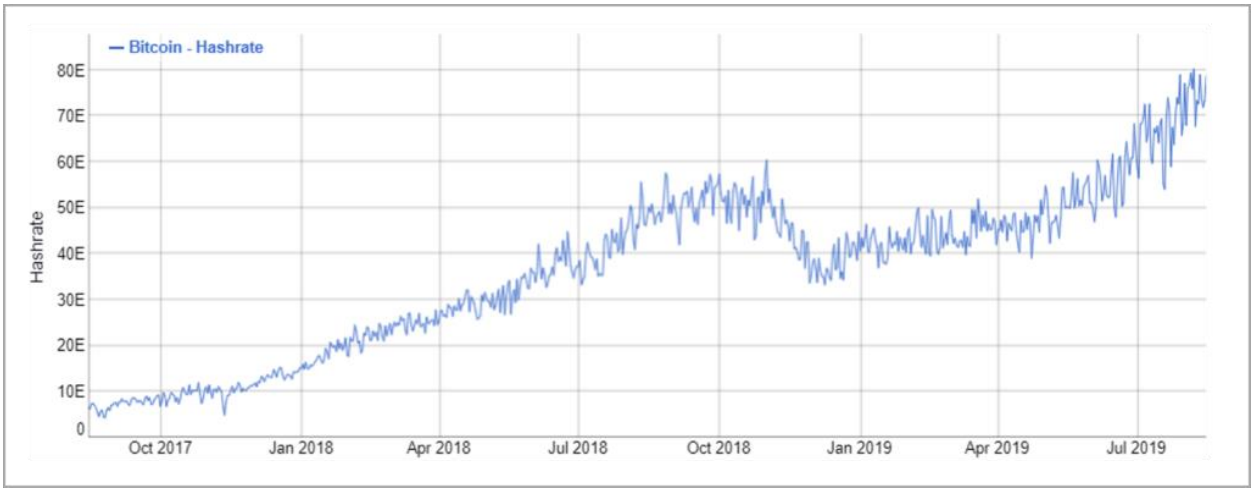
Any number of concerned onlookers raise the red flag about the amount of energy consumed by the bitcoin network. This concern stems from the idea that the energy consumed by the bitcoin network could otherwise be utilized for more productive functions, or that it is just plain bad for the environment. Both ignore the fundamental magnitude of how critical bitcoin's energy consumption actually is. In the long-game, there may be no greater, more important use of energy than that which is deployed to secure the integrity of a monetary network and constructively, in this case, the bitcoin network. But, that doesn't stop those that do not understand the problem statement from raising concerns.

"The fundamentally wasteful nature of bitcoin mining means there's no easy technological solution coming." –the Guardian "In the context of climate change, raging wildfires, and record-breaking hurricanes, it's worth asking ourselves hard questions about Bitcoin's environmental impact." –Vice Media

Bitcoin Energy Consumption

For background, bitcoin is secured by a decentralized network of nodes (computers running the bitcoin protocol). Economic nodes within the network generate, validate and relay transactions as well as validate and relay bitcoin blocks (time sequenced groups of transactions). Mining nodes perform similar functions but also perform bitcoin's proof of work function to generate, solve and transmit blocks to the rest of the network. By performing this work, miners validate history and provide a "clearing" function for current transactions, which all other nodes then check for validity. Think the clearing function of the New York Fed but on a completely decentralized basis every ten minutes (on average).

The work performed requires massive amounts of processing power contributed by miners all over the world, running 24 hours a day, 7 days a week. This processing power requires energy. For context, at 75 exahashes per second, the bitcoin network currently consumes approximately 7-8 gigawatts of power, which translates to ~$9 million per day (or ~$3.3 billion per year) of energy at a marginal cost of 5 cents per kWh (rough estimates). Based on national averages in the U.S., the bitcoin network consumes as much power as approximately 6 million homes. Yeah, it is definitely a lot of power, but it is also what secures and backs the bitcoin network.



How could this much energy be justified? And what will bitcoin consume when a billion people are using it? The dollar works just fine, right? Well that's just the thing, it doesn't. These resources are being devoted to fix a problem most don't understand exists, which makes justifying a derivative cost challenging. To help ease the pain of environmentalists and social justice warriors, we often point out a number of countervailing narratives to make it seem more palatable:

- A significant portion of bitcoin's energy consumption is generated from renewable resources.
- Bitcoin will spur innovation in the development of renewable energy technology & resources.
- Bitcoin consumes energy that is otherwise wasted, if not,flared into the atmosphere.
- Bitcoin consumes only the energy that the free market will bear at a free market rate.
- Bitcoin consumes energy resources that would otherwise not be economic to develop.
- The nature of bitcoin energy demand will improve the efficiency of energy grids.

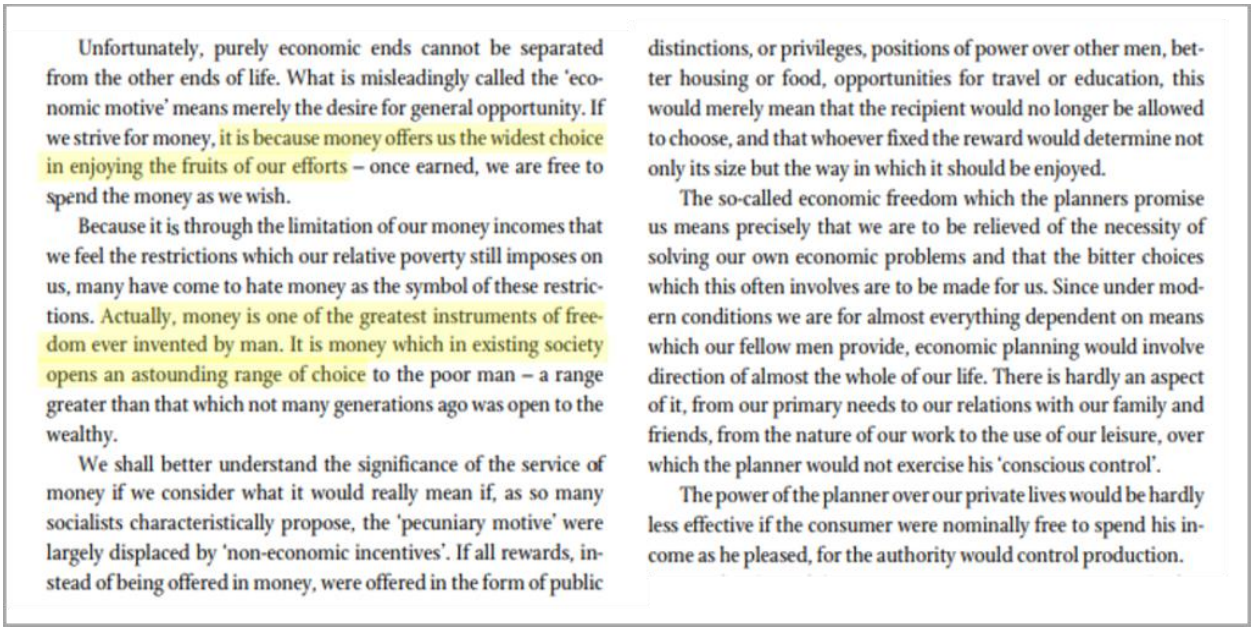
These considerations help enumerate why a simple view that bitcoin's energy consumption is necessarily wasteful or necessarily bad for the environment fails the proverbial test. However, without an appreciation for the enormity of the monetary problem bitcoin intends to solve, the marginal cost could never be justified. Bitcoin represents a solution to the systemic issues that exist within our legacy monetary framework and it relies on energy consumption to function. Economic stability depends on the function of money and bitcoin provides a more sound monetary framework which is why there is no more important long-term use of energy than securing the bitcoin network. So rather than expand on the many individual counterpoints to the mainstream narrative, there is no better place to focus than the first principle problem itself: the money problem or the global QE (quantitative easing) problem, see here.

The Function of Money

The problem of money is enormous, though most people do not recognize it. Most can feel it in their daily lives but cannot identify the root cause. Working harder, longer hours, going into debt and still barely getting by. There has to be a better way, but in order to identify a solution, one has to first see and understand the problem. The problem that exists is with our money and the impact it has on society is pervasive.

Without getting into the details of what money is (read the Bitcoin Standard or Nick Szabo's Shelling Out), we can more easily describe its function in society. Money is the good that facilitates economic coordination between parties that otherwise would not have a basis to cooperate. Put simply, it is the good that allows society to function, and it allows us to accumulate the capital that makes our lives better, which takes different forms for different people. There is a saying that money is the root of all evil, but as Hayek more appropriately describes it in the Road to Serfdom, money is an agent of freedom.

"Money is one of the greatest instruments of freedom ever invented by man."F.A. Hayek, The Road to Serfdom (*Reader's Digest Condensed Version*)



Unfortunately, purely economic ends cannot be separated from the other ends of life. What is misleadingly called the 'economic motive' means merely the desire for general opportunity. If we strive for money, it is because money offers us the widest choice in enjoying the fruits of our efforts – once earned, we are free to spend the money as we wish.

Because it is through the limitation of our money incomes that we feel the restrictions which our relative poverty still imposes on us, many have come to hate money as the symbol of these restrictions. Actually, money is one of the greatest instruments of freedom ever invented by man. It is money which in existing society opens an astounding range of choice to the poor man – a range greater than that which not many generations ago was open to the wealthy.

We shall better understand the significance of the service of money if we consider what it would really mean if, as so many socialists characteristically propose, the 'pecuniary motive' were largely displaced by 'non-economic incentives'. If all rewards, instead of being offered in money, were offered in the form of public distinctions, or privileges, positions of power over other men, better housing or food, opportunities for travel or education, this would merely mean that the recipient would no longer be allowed to choose, and that whoever fixed the reward would determine not only its size but the way in which it should be enjoyed.

The so-called economic freedom which the planners promise us means precisely that we are to be relieved of the necessity of solving our own economic problems and that the bitter choices which this often involves are to be made for us. Since under modern conditions we are for almost everything dependent on means which our fellow men provide, economic planning would involve direction of almost the whole of our life. There is hardly an aspect of it, from our primary needs to our relations with our family and friends, from the nature of our work to the use of our leisure, over which the planner would not exercise his 'conscious control'.

The power of the planner over our private lives would be hardly less effective if the consumer were nominally free to spend his income as he pleased, for the authority would control production.

More specifically, money is the good that allows for specialization and the division of labor. It allows individuals to pursue their own interests; it is how individuals communicate their preferences to the world, whether in work or in leisure, and what creates the "range of choice" we all take for granted. Our modern economy is built on the foundation of freedom that money provides, but the end result is a highly complex and specialized system.

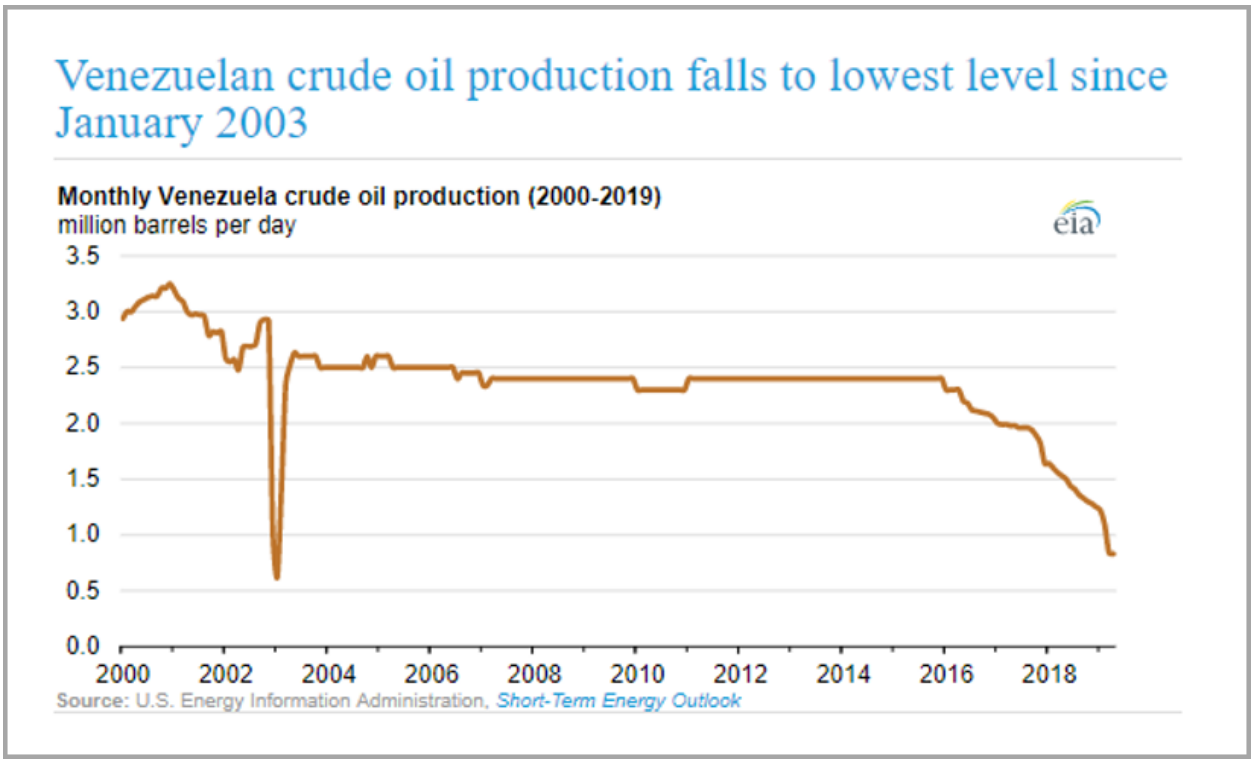
To simplify the concept, Milton Friedman explains the complexity of a pencil (see here), detailing how no one individual is capable of producing a standard lead pencil. He details the wood required, the saw to cut the wood, the steel to make the saw, the iron ore to make the steel, the lead, the rubber for the eraser, the brass ring, the yellow paint, the glue, etc. He explains how making a single pencil requires the coordination and cooperation of thousands of people, including people who don't speak the same language, who likely practice different religions and who may even hate each other if they were ever to meet in person. And he explains that the ability to cooperate is a function of the price system and the economic good we call money.

Abstracting from the pencil, now consider the complexity of our modern economy. From cars to airplanes to the internet to mobile phones, even to your local grocery store. Modern supply chains are so complex and so specialized that they require the coordination of millions of people to deliver any of these basic functions. The orchestration of all this activity which fuels global trade is only made possible by the function of money.

A Living Example: Venezuela

Venezuela provides a tangible macro and micro example of the vital role money plays in economic coordination and the dysfunction that follows when a monetary good fails. Venezuela is one of the most oil rich countries in the world, but as an end game function of monetary debasement, Venezuela's currency has recently hyperinflated. As its currency deteriorated, basic economic functions broke down to the point where getting food at grocery stores or basic healthcare is no longer the baseline. It is a full-on humanitarian crisis, and at the root level, it is a function of Venezuela no longer having a stable currency to coordinate economic activity and to produce the goods it needs to trade within the global economy.

How does this relate to bitcoin and energy consumption? Being an energy rich country, oil was (and is) Venezuela's primary export; or rather, the good it needs to produce in order to trade. Despite being one of the most energy rich countries in the world, Venezuela's oil production is plummeting.



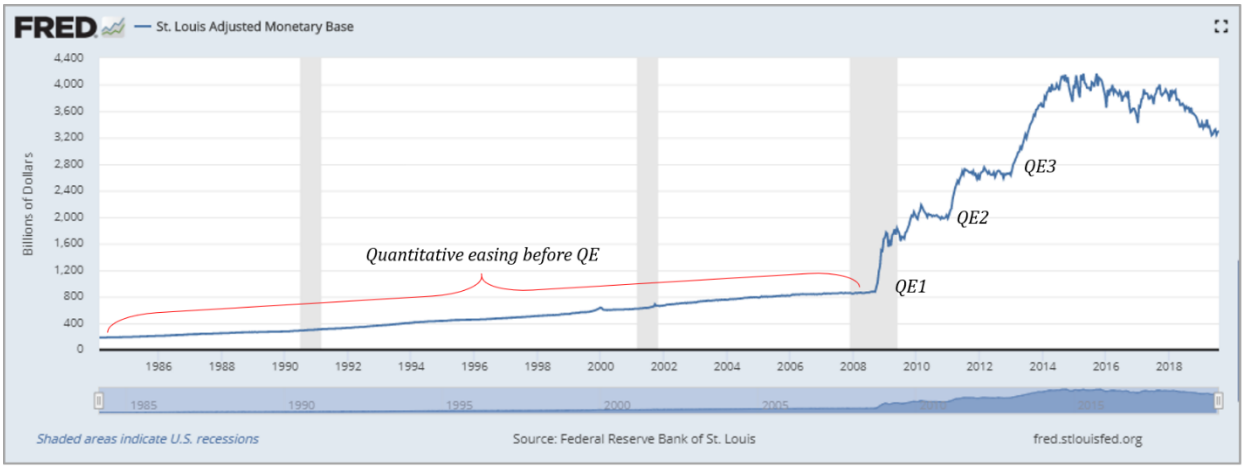
Venezuela can no longer import the technology or coordinate the resources it needs to extract its primary trading currency (oil). This has caused significant deterioration in its local economy, impairing its ability to produce the electricity needed to power its own energy grids, causing extended blackouts and preventing the delivery of basic services such as power, clean water or healthcare.

What is occurring in Venezuela is devastating, and it is a function of the economic deterioration caused by hyperinflation of an unstable currency.

Monetary debasement distorts the price mechanism of a currency, which then creates economic imbalances. As economic coordination deteriorates, complex supply chains become disrupted resulting in a decline in the supply of real goods (e.g. food on shelves, oil production, etc.) and creating an imbalance between supply and demand. As more money is created, real goods become relatively scarce compared to the supply of money, which causes the very function of money to breakdown. Individuals have a disincentive to hold currency as real goods become more and more scarce, instead choosing to sell currency as quickly possible, creating a run on basic necessities and causing the currency to hyperinflate. Economic deterioration by monetary manipulation 101.

The Developed World Application

Now, many sitting comfortably in the developed world will look at Venezuela and think, "it could never happen here," but that ignores all first principles. Whether it is well understood or not, the market structure of the Venezuelan bolivar or the Argentine peso is identical to that of the dollar, the euro or the yen. The Fed, the European Central Bank or the Bank of Japan may be better at managing stability (for now), but it does not change the fact that the underpinnings of all fiat currency systems are the same.



Note: The Adjusted Monetary Base is the sum of currency (including coin) in circulation outside Federal Reserve Banks and the U.S. Treasury, plus deposits held by depository institutions at Federal Reserve Banks. These data are adjusted for the effects of changes in statutory reserve requirements on the quantity of base money held by depositories.

To highlight the U.S. as an example, the Federal Reserve expanded the monetary base from $180 billion in 1984 to a peak of $4.2 trillion following QE3, an increase of 23x. Because of the nature of the Fed's credit-based economy, the economic distortion of this debasement occurred gradually (see here) until the financial crisis which occurred suddenly; and we presently sit further out on the same ledge as a function of the large scale QE required to "alleviate" the crisis. If you believe the developed world is not in a precarious situation or not subject to a similar monetary foundation as Venezuela, I would respectfully point to patients zero: the Fed, the ECB and the Bank of Japan. Often, faith

placed in these institutions is blind to both first principles and common sense, but consider the quote below from a resident Fed economist during the aftermath of the financial crisis and as the Fed was in the middle of creating $3.6 trillion new dollars as part of quantitative easing:

“Also, I want to just emphasize that I think the gaps in our understanding of the interactions between the financial sector and the real sector are profound” David Wilcox – Fed Economist (August 2011)

An honest review of history demonstrates the ill-temperament of those put in charge of managing our economies from central command. While admitting profound gaps in their ability to understand the implications of actions taken on the real economy, the response was to continue down the same path but in a bigger way, while expecting a different result: the definition of insanity. Our present choice is one between two great contrasts. A) a centrally-planned form of currency that is designed to lose its value; or B) a decentralized currency with a fixed supply. The latter comes with cost in the form of energy consumption, but the positive externality will be long-term economic stability.

Economic Stability via Energy Consumption

Future economic stability is fundamentally why there can be no more important source of demand for the consumption of energy than the security of bitcoin’s monetary system, especially when the alternatives (fiat and gold) are structurally flawed. If we wait to see the signs of hyperinflation, we’re already lost. But Venezuela is not just an example of what transpires as a result of hyperinflation, it is a living example of the importance of energy production to the functioning of society. Some energy input is required for everything that we consume in our daily lives. The coordination of those energy inputs is dependent on the reliability and stability of the money we use.

Ignore your morning coffee for a minute and think basics: clean water, sanitation, food, medicine, basic healthcare, etc. The coordination of resources to deliver these basic services is dependent on a functioning monetary system. When a monetary system breaks down, social coordination and even the social fabric begins to go with it. If the basis of all trade is energy, and if we need money to coordinate trade, the highest and best use of that energy should first be to protect the monetary system. Put your proverbial “oxygen mask” on first and then shift to dependents. Secure the foundation of trade and then focus on all of the derivatives.

Any and all concerns about the amount of energy bitcoin consumes or will consume is a red-herring. It is not that we should sacrifice electricity that could otherwise power homes; instead, it’s that we will never have the electricity to power those homes if we do not have a reliable monetary system to coordinate economic activity and marshal resources. In practice, bitcoin will not

practically compete for the same energy resources that fuel the basic productive and consumptive functions of our economy (not zero sum); instead, bitcoin's function as a currency system will ensure that those very energy needs can continue to be fulfilled.

What would be bad for society is if more countries deteriorated into the economic and humanitarian disaster that is Venezuela, where basic health and human services cannot be reliably provided. And this is not to present a draconian vision or a dystopian future; instead, it is to articulate the importance and interconnectedness of both the money function and the energy function in complex, highly specialized economies.

"If it prevents one instance of hyperinflation such as Venezuela from happening [...], bitcoin's energy consumption would be the best bargain humanity ever got." – Saifedean Ammous,The Bitcoin Standard Research Bulletin

Bitcoin represents a backup switch to the current architecture of the global financial system and is soon to be its primary engine. Setting aside the systemic risks that currently plague our financial system, bitcoin is a fundamentally more sound monetary system from the ground up. And, it is one secured by the production and consumption of energy. You do not have to believe that the dollar's fate will be that of the Venezuelan bolivar to recognize the importance and interplay between the stability of a monetary function and the production of energy resources that provide basic economic necessities. And the risk inherent in even the possibility of hyperinflation is so negatively asymmetric that the price of bitcoin energy consumption is of small relative cost.

Bitcoin will consume any and all energy resources necessary to secure its monetary network, which is inherently driven by the base demand to hold it as a currency. The more people that value the long-term stability it provides, the more energy it will consume. In the end, this consumption will ensure all other derivatives of energy consumption will continue to be fulfilled, which is why there is no more important long-term use of energy than securing the bitcoin network. Put a price on economic stability and the economic freedom a stable monetary system provides; that is the true justification for the amount of energy bitcoin should and will consume. Everything else is a distraction.

Tweetstorm: Shallow Safety vs. Deep Safety

By Nick Szabo

Posted August 17, 2019

Shallow safety vs. deep safety:

Shallow: estimated from volatility, assumes nothing goes wrong at lower layers of the protocol stack

Deep: what happens to your assets upon underlying failures? e.g. how would your digitally centralized assets fare against sanctions or cyberwar?

Digitally centralized assets have poor deep safety. They were designed in & only work in a legally stable environment.

Real estate & gold have deeper safety, assuming strong local security.

Trust-minimized Bitcoin uses computer science to achieve unprecedentedly deep safety.

Digital centralization has made it possible, for the first time in history, for authorities to routinely extract haircuts and "negative interest". Some countries in Europe have already used these techniques against digitally centralized cash balances.

At the behest of political activists, digitally centralized financial services have frozen accounts and cut off access to a wide variety of people based on their political views.

In a deep or prolonged recession, attacks by technocratic authorities & political activists against digitally centralized assets will increase in volume & scope. Other forms of political or legal instability could also lower the safety of digitally centralized assets.

One can think of shallow safety as the technical analysis of safety based on technical factors such as price volatility. Deep safety is a fundamental analysis of the underlying technological, political, and legal environments which actually control the assets.

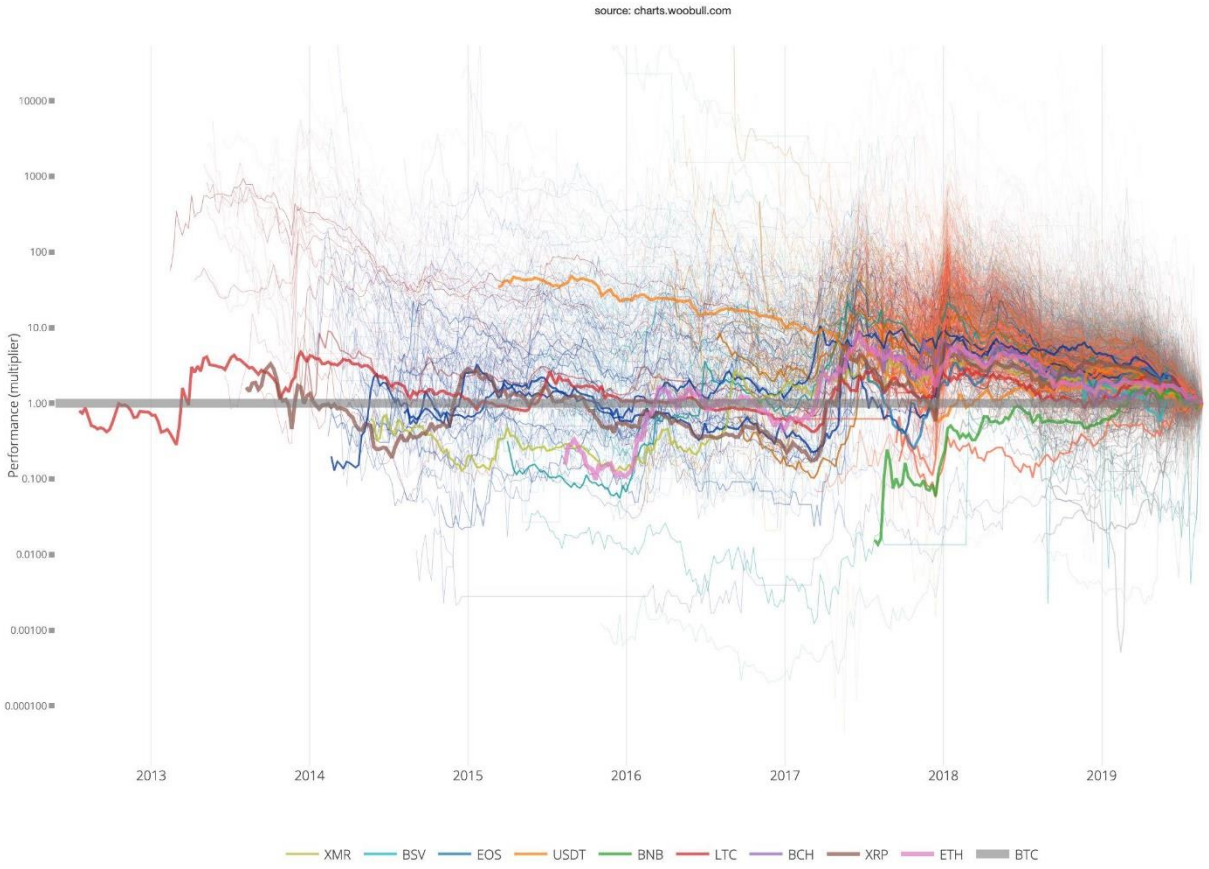
Deep safety varies greatly between different people & organizations. Risks to digitally centralized property vary greatly between different people & organizations & their different political & legal environments. Price movements don't tell you much about your particular safety.

Tweetstorm: Performance Against Bitcoin

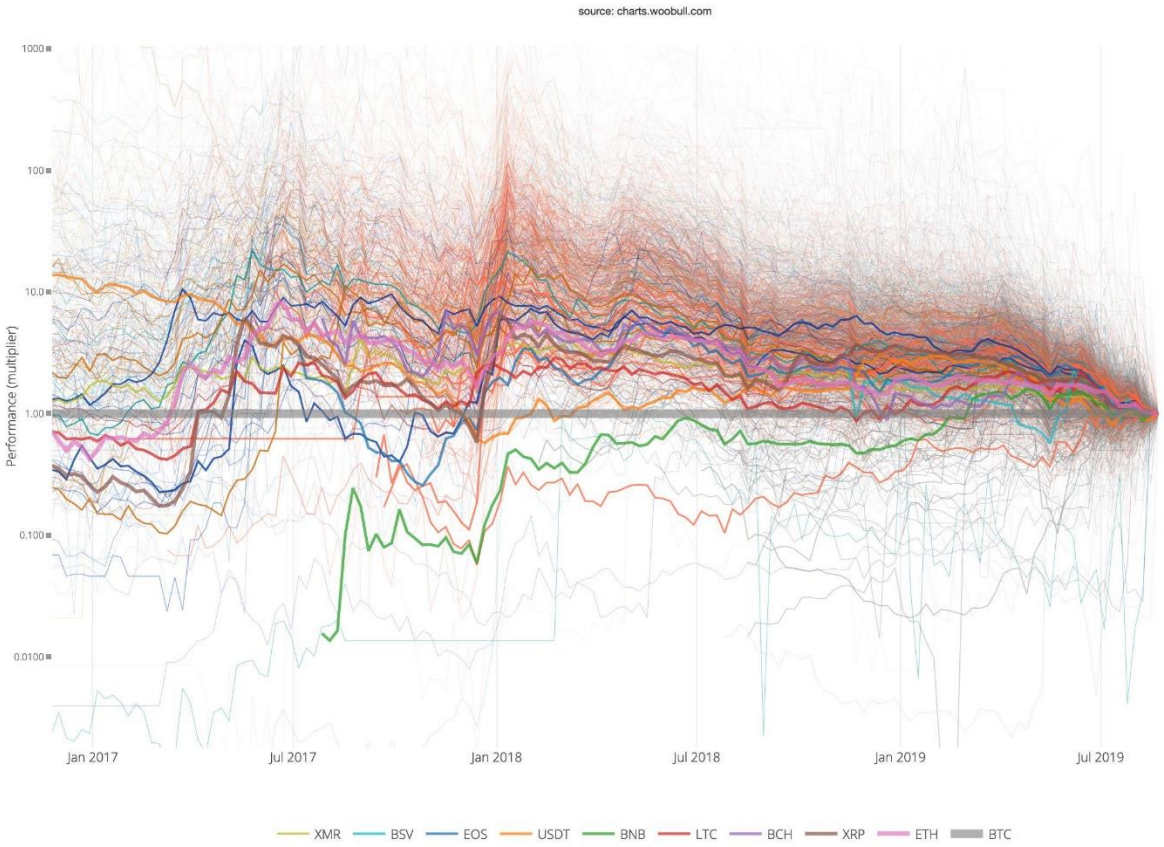
By Willy Woo

Posted August 17, 2019

The entire crypto market in one visual. This is the historic performance of 2000+ coins in satoshi value (performance against BTC).



Zooming in, here's the 2017 shitcoin boom and bust. Powers of 10 on the y-axis, so alts lost 90-99% of their satoshi value.



One thing to note is this is all a race to achieve Lindy Effect, only a few coins have achieved this. They are the thick lines (sufficient cap and SoV scale), that stayed horizontal of better (kept up with Bitcoin), for a long time (at least one full 4 year bull bear cycle).

The data also questions the common wisdom that alts are leverage plays on BTCUSD. We only saw this in the 2016/17 bubble, there is very little evidence of that happening in the 2012/13 bull. In the first bull cycle pre-2012 alts were performance neutral as they didn't exist.

Bitcoin Did The Things That Didn't Scale Initially, Which Is Why It Remains The King Today

By Anthony Pompliano

Posted August 19, 2019

To investors,

One of my favorite writers in technology and/or investing is Paul Graham, co-founder of YCombinator and investor in many of today's most successful startups. He doesn't write often, but when he does, his words are concise, intelligent, and encourage the reader to think bigger and more critically. I recently re-read one of his most popular posts, titled "Do Things That Don't Scale," which was published in July 2013.

(This photo is from privateinternetaccess.com)

In this piece, Graham shares a piece of advice for entrepreneurs who are just starting out — do things that don't scale. He begins by saying:

"One of the most common types of advice we give at Y Combinator is to do things that don't scale. A lot of would-be founders believe that startups either take off or don't. You build something, make it available, and if you've made a better mousetrap, people beat a path to your door as promised. Or they don't, in which case the market must not exist. Actually startups take off because the founders make them take off. There may be a handful that just grew by themselves, but usually it takes some sort of push to get them going. A good metaphor would be the cranks that car engines had before they got electric starters. Once the engine was going, it would keep going, but there was a separate and laborious process to get it going."

Graham then goes on to highlight a framework for implementing the idea of unscalable actions. As I kept reading, I couldn't help but think "this is how Bitcoin grew." Below I have summarized or shortened each section of Paul Graham's framework (you will still get the general concept), along with adding commentary on how Bitcoin's rise applies.

RECRUIT

"The most common unscalable thing founders have to do at the start is to recruit users manually. Nearly all startups have to. You can't wait for users to come to you. You have to go out and get them." In this section, Graham gives examples of successful startups who manually recruited early adopters in a very unscalable way. They didn't run Facebook ads, launch TV commercials, or even have a marketing budget, but instead they spent their time showing a small group of people their product, soliciting feedback, and onboarding users one at a time.

Bitcoin's initial adoption was very similar. Satoshi Nakamoto didn't have a for-profit company. He/She/They didn't raise money to build the product or market it. Bitcoin's software was written, then a white paper was put together, and eventually a very small group of cryptographers were told about the cryptocurrency via a cryptography email list. The Bitcoin "founder" was literally emailing early users one on one, including answering questions and discussing features. Eventually, the discussion of this small group grew from emails (very private) to Internet forums (a little more public), but throughout the entire process, users were encouraged to download the software and start using/testing it.

FRAGILE

"Airbnb now seems like an unstoppable juggernaut, but early on it was so fragile that about 30 days of going out and engaging in person with users made the difference between success and failure. That initial fragility was not a unique feature of Airbnb. Almost all startups are fragile initially. And that's one of the biggest things inexperienced founders and investors (and reporters and know-it-alls on forums) get wrong about them. They unconsciously judge larval startups by the standards of established ones. They're like someone looking at a newborn baby and concluding "there's no way this tiny creature could ever accomplish anything."

Imagine telling someone that a new form of money, only in digital form and not backed by a sovereign nation, would grow from a single user to millions of people and hundreds of billions of dollars in market cap within a decade. Or that this new form of money would be covered daily on investment shows like

CNBC and Bloomberg. Or that public pensions, university endowments, and other institutional investors would eventually incorporate this digital currency into their portfolio. Not only would very few people believe you, but most people would think it was utterly impossible. And for the most part, it was. As my partner Mark Yusko likes to say, "The miracle of Bitcoin is not having it reach $10,000, but rather that it went from $0.003 to $1." The initial fragility of Bitcoin can't be overstated and the odds of the flywheel of adoption actually taking place are hard to comprehend.

DELIGHT

"You should take extraordinary measures not just to acquire users, but also to make them happy. For as long as they could (which turned out to be surprisingly long), Wufoo sent each new user a hand-written thank you note. Your first users should feel that signing up with you was one of the best choices they ever made. And you in turn should be racking your brains to think of new ways to delight them."

While Satoshi Nakamoto was not sending out thank you notes to individual users, he/she/they were answering individual emails and forum posts from the first users. There was a level of "customer service" that occurred, but it wasn't what you would normally categorize as customer service. There were no call centers. No sales people. Just a simple, yet eloquent, 9-page white paper that described what Bitcoin was and how it worked, along with a founder willing to engage in the perfect tone with the initial target market of cryptographers.

EXPERIENCE

"I was trying to think of a phrase to convey how extreme your attention to users should be, and I realized Steve Jobs had already done it: insanely great. Steve wasn't just using "insanely" as a synonym for "very." He meant it more literally — that one should focus on quality of execution to a degree that in everyday life would be considered pathological. All the most successful startups we've funded have, and that probably doesn't surprise would-be founders. What novice founders don't get is what insanely great translates to in a larval startup. When Steve Jobs started using that phrase, Apple was already an established company. He meant the Mac (and its documentation and even packaging — such is the nature of obsession) should be insanely well designed and manufactured. That's not hard for engineers to grasp. It's just a more extreme version of designing a robust and elegant product."

Personally, I think this is the most important point that Graham makes. When the initial users of Bitcoin started testing it, they had an epiphany that was lacking in other attempts at building a digital currency — Bitcoin was a product

that simply worked. The transactions worked. The cryptography worked. The mining mechanism worked. The delightful experience of trying something new, having it work, and realizing that it was a major improvement over sending US dollars via the traditional banking system (faster, cheaper, more secure, not reliant on a centralized third party, etc) was really, really important to pulling in the initial users.

FIRE

"Sometimes the right unscalable trick is to focus on a deliberately narrow market. It's like keeping a fire contained at first to get it really hot before adding more logs. That's what Facebook did. At first it was just for Harvard students. In that form it only had a potential market of a few thousand people, but because they felt it was really for them, a critical mass of them signed up. After Facebook stopped being for Harvard students, it remained for students at specific colleges for quite a while. When I interviewed Mark Zuckerberg at Startup School, he said that while it was a lot of work creating course lists for each school, doing that made students feel the site was their natural home."

Bitcoin had a single target market initially — cypherpunks. (*A cypherpunk is "any activist advocating widespread use of strong cryptography and privacy-enhancing technologies as a route to social and political change."*) These individuals had a shared set of ideals, ethos, and view of the world. They were the exact people looking for a decentralized, secure, digital currency that removed the need for centralized authorities. And when Satoshi Nakamoto built the right product and handed it to the cypherpunks, they knew exactly what to do with it — mine it, hold it, and use it. Bitcoin found product-market fit almost immediately, which accelerated adoption (it also didn't hurt that money is an extremely viral product).

Manual

"There's a more extreme variant where you don't just use your software, but are your software. When you only have a small number of users, you can sometimes get away with doing by hand things that you plan to automate later. This lets you launch faster, and when you do finally automate yourself out of the loop, you'll know exactly what to build because you'll have muscle memory from doing it yourself. When manual components look to the user like software, this technique starts to have aspects of a practical joke. For example, the way Stripe delivered "instant" merchant accounts to its first users was that the founders manually signed them up for traditional merchant accounts behind the scenes."

Many of the first pieces of Bitcoin infrastructure followed a similar trajectory of starting out manual behind the scenes, but eventually building software that "automated" those processes over time. This was true in payment processing, exchanges, and a number of other instances.

Big Launch

"I should mention one sort of initial tactic that usually doesn't work: the Big Launch. I occasionally meet founders who seem to believe startups are projectiles rather than powered aircraft, and that they'll make it big if and only if they're launched with sufficient initial velocity. They want to launch simultaneously in 8 different publications, with embargoes. And on a tuesday, of course, since they read somewhere that's the optimum day to launch something. It's easy to see how little launches matter. Think of some successful startups. How many of their launches do you remember? All you need from a launch is some initial core of users. How well you're doing a few months later will depend more on how happy you made those users than how many there were of them."

Big launches almost never matter and thankfully, Bitcoin had the exact opposite of a big launch. It was quietly built and then sent to a very small group of people. The founder didn't even want to be known, so they used a pseudonym, before eventually disappearing. The focus from day one has always been on the product, along with the ability for it to simply work.

My Conclusion

Paul Graham's advice is likely to stand the test of time. It focuses on the most important aspect of building a company — finding product/market fit in a high probability way. As you can see above, Bitcoin was able to follow a similar playbook, whether intentionally or not.

But my favorite part is that almost every token project since Bitcoin has chosen to take a different path. They have mostly pursued large funding rounds, extravagant company launches, or egregious spending on "marketing." These pursuits are not only unlikely to work, but they also give founders a false sense of traction. They make it easier to confuse motion with progress.

Bitcoin is the largest market cap cryptocurrency today. It is unlikely that will change any time soon. The network effects are too strong. The brand awareness is too strong. And since money is a belief system, too many people believe Bitcoin will be the winner.

It is fun to look back at the last 10 years of Bitcoin's rise and realize that the playbook was simple — do the things that don't scale. Just don't understatement how hard that playbook is to execute :)

-Pomp

The Bitcoin/Government Battle is Vaporware

By Jesse Lawler

Posted August 21st, 2019

For bitcoiners, it is something of a parlor game to think of ways Bitcoin could be killed. In its decade-long history, the world's first cryptocurrency has already dodged numerous bullets: exchange hacks, software bugs, ideological civil wars, massive price-crashes, being labeled "rat poison" by Warren Buffett, and no less than 370 "Bitcoin is dead" articles published by writers who've consistently been premature in their vulture-like stance. So far, rain or shine, Bitcoin has always taken its lumps, dusted itself off, and gone on producing blocks—to the glee of its fans and the astonishment of its detractors. But, like a plucky video game character advancing to bigger scraps with tougher bad guys, Bitcoin has larger fights coming. And Bitcoin's user community—like X-Box-watching friends yelling advice from the couch—spends a lot of time speculating about the next fight, the optimal strategy, and how *they'd* play if they were the one behind the controller. For many, the *ultimate* fight they imagine to be coming is the showdown that will happen when governments "wake up" to Bitcoin, become scared for their own national currencies, and rouse themselves to go on the offensive. **The *apocalypto-philia* goes something like this:**

"Bitcoin will be declared illegal. Anyone who's ever held a Coinbase account will be forced to renounce their private keys and swear monetary allegiance to the Dollar, Euro, etc. Armed drones will deliver incendiary grenades to any building found with an open port 8333 on its Internet router."

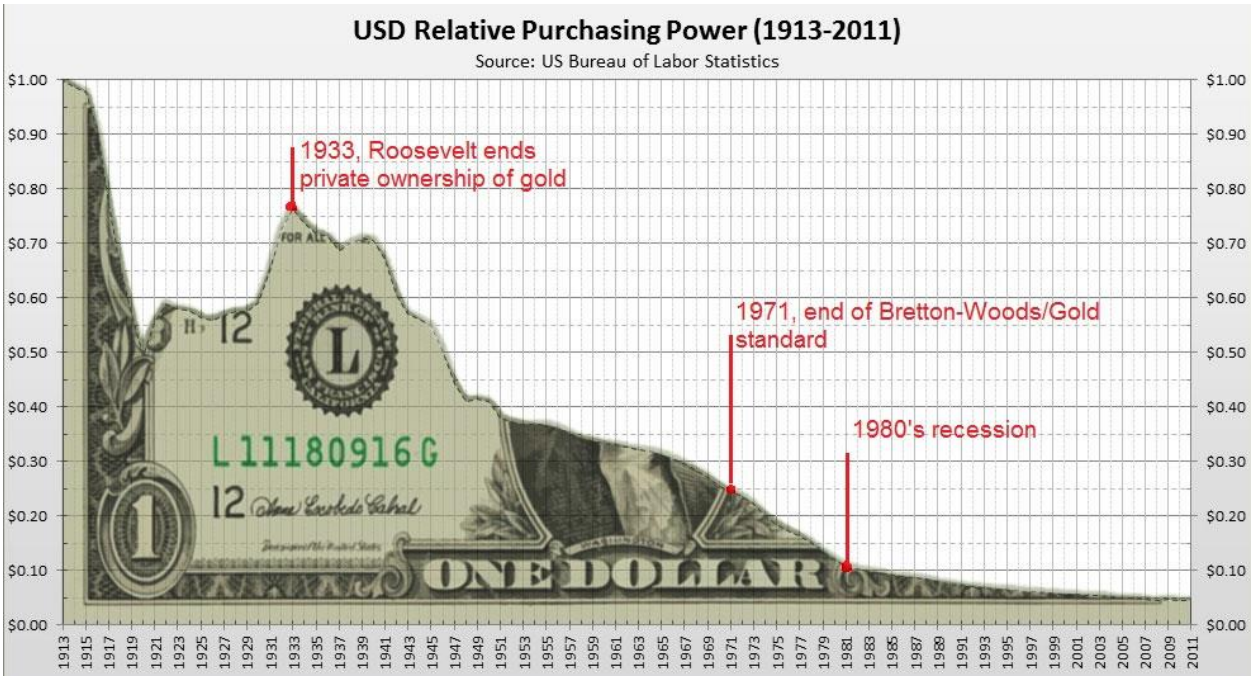
This, my friends, is a fever dream.

Before I begin, let me admit my biases:

- I love dystopian science fiction as much as the next guy.

- I love dystopian sci-fi as much as the next guy *even when the next guy is a fellow bitcoiner.*
- And yes, as a group we love dystopian sci-fi about 50 times more than the average person. Bitcoin, after all, sprung from a nest of cypherpunks.

Why is sci-fi and cypherpunkery relevant to this popular delusion? Because the big, bad final boss in the cypherpunk genre (going back as far as George Orwell) is always a high-tech, neofascist, all-seeing government. So naturally—like David vs. Goliath or the Rebel Alliance vs. the Galactic Empire—eventually Satoshi's band of pseudonymous code-phreaks and their Austrian-economics pals are destined to square off against the central bankers that have dominated international finance for the past century. These monetary villains have inflated away over 95% of the US Dollar's purchasing power since the inception of the Fed. (Astonishingly, the Dollar seems to have *gotten off lucky* compared to most other currencies.)



So if Bitcoin *doesn't* fight this epic monetary bad guy…then what happens?

Gentlemen, I'm sorry, but the Wachowskis will not be directing this movie. Bitcoin's future history is going to merit a Ken-Burns-style documentary, not an action flick.

Goliath shrugged.

The cartel system of global central banking has been, without question, the most successful tool in history for wealth extraction. Gold bugs, bitcoiners, and anyone who has done even minimal research into the history of fractional-reserve banking already understands this. The Cantillon Effect is real, and it is spectacular.

Despite all this, I'm telling you that the beneficiaries of this *most excellent of cons*—the people who even now are reaping ill-gotten gains through the expansion of the world's money supply—are going to leak away their power without a fight. There will be no monetary Armageddon.

The Revolution will not be worth televising.

I'm making this rather bold prediction that I know few people will agree with, but I'm confident in doing so. And here's why: The world's central banking cartel *isn't* best compared to the biblical Goliath. If we keep things sci-fi, a better comparison would be to Jean-Luc Picard's nemesis from *Star Trek: The Next Generation* — the Borg.

Decentralization Goes Both Ways

Decentralization is what makes the Internet impervious to nuclear attack. Decentralization is what makes Bitcoin permissionless and un-censorable. Decentralization is what makes mosquitoes the world's deadliest animal, despite the bigger, toothier competition. But while we bitcoiners are conditioned to think of decentralization as a slam-bang strategy for *defense* …this isn't always true. Decentralization is a great strategy *when a small sliver of survivorship can get the job done*. If the name of the game is eradication-avoidance, then decentralization is your friend. But many contests aren't like this. Sometimes success requires unanimity—or at least a robust majority—if things are to work right. A marching band or a synchronized swim team isn't

made more cohesive because it is decentralized. In fact, just the opposite: its performance is impressive specifically because it is difficult to maintain a unified performance *in spite of decentralization*. The world's monetary system of co-integrated central banks is decentralized in this second way—the way of marching bands and swim teams (and of the Borg). A few people marching out of step or swimming off in the wrong direction will have disastrous, show-stopping consequences. United they stand, divided they fall.

The economics of conflict.

"You can kill ten of my men for every one I kill of yours. But even at those odds, you will lose and I will win."—Ho Chi Minh, 1946

Ho Chi Minh was the father of the modern Vietnamese state, and he spoke the words above as a warning to the French colonial government in the aftermath of World War 2. During that war, both the French and the Vietnamese homelands had been occupied by Axis Powers—France by the Nazis, Vietnam by Imperial Japan. With geopolitics in post-war flux, Ho Chi Minh wasn't about to passively trade one occupying power for another. Gamblers at the time wouldn't have picked the scrappy Southeast Asians as eventual victors against the French. France was backed by the USA—which had just kicked the ass of the country that had kicked Vietnam's ass. But Ho Chi Minh saw the match-up versus France in a different way, stripped down to its brutal, economic reality: It was much, much cheaper for the Vietnamese to kill Frenchmen than for occupying Frenchmen to kill Vietnamese.

In a war of attrition, Ho Chi Minh knew he would win.

In 2008, Satoshi Nakamoto designed a system with economic realities similar to those which made the underdog Vietnamese successful against the French (1954), and later, the Americans (1975). Ho could put combatants into the field inexpensively—and not just the "men with guns" kind of combatants. The televised optics of an industrialized country's military suppressing a determined underdog that *only wanted to be left alone* created allies among the (decentralized) public within the enemy nations. It wasn't Vietnam's battlefield strength but a slow splintering of its enemies' will to fight that eventually yielded victory.

I am Bitcoin. I am legion.

Satoshi's system—Bitcoin—was designed with incentives such that, for its entire eleven-year history, it has *always been more economically rational to help Bitcoin than to fight against Bitcoin*. With a handful of exceptions made up of vanishingly few people, that bold statement is true for every human on Earth. In the decentralized network of human society, each person is a potential convert to side with Bitcoin versus the central banks' monetary monopolies. Siding with the central banks gets you…the status quo you're already enjoying. (Is that a golf clap I hear?) Unless you're a top banking executive or hold a regulatory role that earns you licit or illicit profits from the banking industry, there's nothing "in it for you" to fight against free-market monetary competition. If central banks impel their respective nation-states to move against Bitcoin, you stand nothing to gain. On the other hand, should you at any point decide to invest a triflingly small amount of your personal savings into Bitcoin (on the off-chance that like-minded others will do the same) and proceed to go about your life, you have a plausible chance of making massive returns from your passive investment.

Fun Fact: Thus far in Bitcoin's history, there has never been a period where you could buy-and-hold for 3 years and *not* be able to sell at a profit. During most three-year spans, the profits would be dramatic.

Are such everyday Bitcoin-owners active foot-soldiers in an epic battle against government-backed currencies? Not at all. But do they have a dog in the proverbial fight? Sure. Will they want their governments to take overt action *against* their investment? Of course not. There are—based on "Know Your Customer" banking records from government-sanctioned Bitcoin exchanges—at least 10 million Americans who have registered for an account through which they can buy Bitcoin. It is estimated there are 30 million Bitcoin owners worldwide.

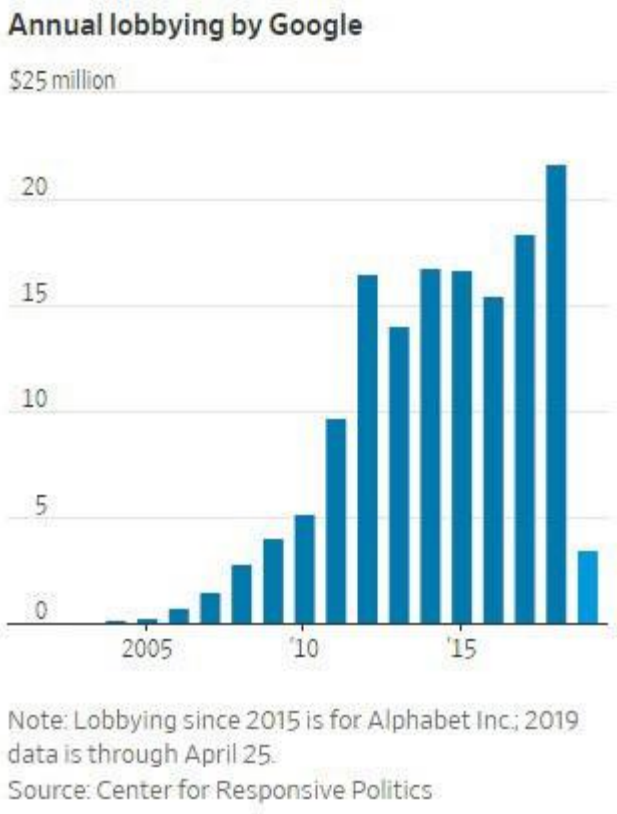
The Trojans have already left the Horse.

Of the 10-million-plus Americans sitting on a little Bitcoin (or maybe a lot), how many of these are politicians? How many are regulators? How many work inside the banking system? If you know the first thing about investments, you've heard the word *diversification*. It's the one word you can drop in financial conversations that are otherwise over your head and not sound like a moron. So how many people in the "investor class" have picked up a little Bitcoin to diversify their investment portfolios outside the traditional asset classes? And can't we assume that people with enough capital to invest exert more than their fair share of pull with the government, demographically speaking? (This is a question that answers itself.) Congressman Patrick McHenry of North Carolina recently said:

"The world that Satoshi Nakamoto, author of the Bitcoin white paper, envisioned—and others are building—is an unstoppable force… We should not attempt to deter this innovation. Governments cannot stop this innovation, and those that have tried have already failed."

This is an out-of-the-closet bitcoiner. Nobody asked McHenry how much Bitcoin he personally owns (he was among the committee's panel of members, not a witness)—but can you really read that quote and have any doubt?

Tech giant Google (Alphabet, Inc.) spends over $20 million per year lobbying the US government. At first blush, this seems unrelated to Bitcoin. It's tempting to say "Google is a corporation; they've got people whose job it is to advance their interests. Bitcoin is just a decentralized, pseudonymous network. No one is lobbying on behalf of Bitcoin."



But does this assumption really stand up to scrutiny? If you were a "Bitcoin whale"—one of the early adopters who was either lucky or prescient enough to buy large amounts of bitcoin when its price was 100 or more times less than it is today—why on Earth *wouldn't* you take out the world's simplest insurance policy on your digital riches?

"And what is that insurance policy," you ask?

It's simple: You insure your investment by putting some Bitcoin directly into the hands of currently-neutral legislators who could influence policy in the future.

If you had given someone $1000 worth of Bitcoin exactly 3 years ago today, one of two things has happened:

1. They kept it, and are looking at a 2,000% (20x) profit.
2. They sold it sometime since—and now they wish they hadn't.

Whichever scenario occurred, you would have guaranteed this person understands Bitcoin's potential—and you've very possibly created a sleeper-cell advocate for future policy. If you are, say, Cameron and Tyler Winklevoss

(founders of the Gemini exchange and purported owners of 1% of the world supply of Bitcoin), it would practically be fiduciary malpractice *not* to lobby in this way.

- **Note:** I'm not saying that I know any whales are lobbying like this. I am saying it defies common sense to think none of them are.

Follow the money.

Ho Chi Minh beat the odds because he could add allies to his cause *cheaply*. Satoshi Nakamoto's system can add allies not just cheaply but *profitably.* Every new bitcoiner is not only an interested party, not only a potential cheerleader, but also a small but consequential ratchet raising the value of all the other bitcoin held by all the other bitcoiners.

The central banks won't mount a fight against Bitcoin because they'll find themselves unable to field an army. (At least, not one that can avoid ongoing mass defections.) They have no moral authority to inspire troops.

They have no booty to promise aside from the status quo. And they have no enemy to demonize except for a globally distributed network with no ideology or ulterior motive. Bitcoin is simply an opt-in, open-source software with the historically reliable property of making its users wealthy.

tl;dr: If you can't beat 'em, join 'em.

And this is what more and more *nocoiner* neutrals will choose to do. The slope from Bitcoin curiosity, to toe-dipping, to enthusiasm, to advocacy is a slippery one indeed. I'm sorry, my cypherpunk friends, but your apocalyptic future-war visions will have to wait for the killer robots.

The world's national currencies will offer Bitcoin only a sputtering resistance—more in word than deed—and they'll dwindle into irrelevance as their defenders fail to defend, their battlements go unmanned, and the central banks' centers will not hold.

The final capitulation will be less William Gibson and more Douglas Adams: *Not with a bang, but with a snicker.*

The Rise of the Sovereign Individual

How power is re-aligning itself in an internet-native world

By Gigi

Posted August 22, 2019

Photo cc-by Studio Incendo

Not too long ago, the internet was a fringe phenomenon. Very few people saw the benefits of a global communications network. Even fewer people had the vision and the foresight to see what it might enable. Today, most people take the internet for granted. It is simply expected to be there, like running water in your home.

Even before the internet became ubiquitous, technologists and visionaries realized the potential of this transformative technology. They realized that an undiscriminating network combined with the magical power of public-key cryptography tips the power-balance in the individual's favor.

Eavesdropping-resistant communication which can't be stopped is poison to authoritarian regimes, which, after all, are in the business of suppressing and controlling the flow of information. If people are still able to communicate and assemble, they can rise up and speak truth to power. We saw the liberating potential of communications technology during the Arab Spring, and we continue to see individuals rise up and fight authoritarian rule today.

What the cypherpunks understood 30 years ago is starting to play out right before our eyes: the tools of our information age have the potential to empower individuals like never before.

The Freedom to Transact

As I am writing these lines, hundreds of thousands of people are marching in the streets of Hong Kong, protesting against an extradition bill proposed by the

government. As always, protests like these shine a light on the current power balance between individuals and the powers that be.

Unfortunately, the current system of surveillance, automated facial recognition, and cashless transfers enables not only a single point of failure, but also a single point of control in times of unrest. If the government doesn't like your opinion or the fact that you were part of a (peaceful) protest, a simple truth becomes apparent: your freedom of assembly was an illusion, as was your freedom to transact freely.

In a free society, these freedoms should be guaranteed. How? Well, as we have seen in the past, information technology and strong cryptography — if used carefully — *guarantee* the right to speak freely. After all, no amount of violence will ever solve a math problem. In the same vein, an information technology exists today which *guarantees* the right to transact freely: Bitcoin.

It is easy to forget that "permissionless" and "censorship-resistant" are more than mere buzzwords. Under difficult circumstances, these words become a matter of life and death. The Hong Kong protests make evident once again what privacy advocates have been preaching for years, even decades: if censorship and surveillance are built into the system, it will be used and abused by those who are in charge. And if you don't have the option to detach from your identity, free speech, free thought, and free action are impossible.

What is true for WeChat, Facebook, and Google, is also true for our current payment rails and the financial institutions of this world. No matter how noble the motivation of building central controls into communication or financial systems — power corrupts, and absolute power corrupts absolutely, as the saying goes.

"Decentralized and private payments are a necessary innovation for a digital future where we retain our civil liberties and personal freedoms." —Alex Gladstein

Strong cryptography allows us to reclaim our right to private conversations in the digital age, thanks to end-to-end encryption. The same cryptography allows us to reclaim our right to transact freely in a digital world, thanks to digital signatures, cryptographic hashes, and the global machine of truth and freedom which is Bitcoin.

The Freedom to Remain Private

In today's digital world — as Hong Kong protesters know — finding out who went to which protest is as easy as retrieving data from a database. Whether it is from people's bank accounts, WeChat, Alipay, or other virtual profiles, the convenience of the status quo inevitably leads to a system of total surveillance, and thus total control.

The solution to this conundrum is enabling privacy by default, which has been the default setting for thousands of years. Neither the internet nor Bitcoin is perfect in this regards, which is why constant vigilance and the development of privacy-enhancing technology are a necessity.

In the last couple of years, efforts to encrypt all internet traffic by default have been made. In the next couple of years, we hope to see continued efforts being made to make every bitcoin transaction even more private than they are now (which is one of the reasons why Bull Bitcoin uses Wasabi's CoinJoin by default).

As is evidenced by the long lines at Hong Kong's train ticketing machines, surveillance renders all other freedoms useless.

Source: Mary Hui

The current situation in Hong Kong paints a vivid picture of the disastrous side-effects of a cashless society. Without a way to transact privately and anonymously, people are enslaved to the masters of finance. And no amount of going digitally dark will allow you to avoid this slavery.

Arguably, things are bound to go from bad to worse. The financial elite which controls the most important good of our society — money itself — is playing god with our shared macroeconomic reality. In the last couple of decades, a concerted effort was made to attack another financial freedom: the freedom to save.

The Freedom to Save

Even without people marching in the streets, it is apparent to most that these are chaotic times. Currencies are not holding their value. A recession is looming. The most powerful men in the world are openly fighting currency wars and are bragging about it on twitter. All while the endless printing of

money continues and politicians/bankers are spewing propaganda to normalize negative interest rates.

People talk about Quantitative Easing (QE) and Negative Interest Rate Policies (NIRPs) as if they were anything other than pure insanity. The first is simply printing massive amounts of money, the second is paying borrowers and stealing from savers.

Gone are the days where you would get interest from your money in the bank. In the world of NIRPs, *you have to pay the bank to hold your money*. In the same vein, gone are the days where you have to pay back your loan plus a little extra to reimburse your lender for taking on the risk. In the world of NIRPs, *you are getting paid to take out a loan*. Need some money? No worries! We are giving you the money and are paying you a little extra, for enjoying the privilege of giving you a loan!

As should be apparent for every child which is offered the choice between two marshmallows today, or one marshmallow tomorrow: the current financial world is defying common sense. I repeat: pure insanity.

More and more people realize that this insanity has to stop and decide to exit a system in which a global negative-yielding debt of $15 trillion is the new normal. The broken financial system, with its negative interest rates and "modern" monetary policies, are, in part, responsible for the rise of sovereign individuals all over the world.

Source: Rachel Cheung

People begin to realize the stupidity of this game. Putting pressure on this broken system by making a run on banks is one form of peaceful protest. Storing your value in an asset which can not be inflated, can not be confiscated, and can not be subject to the whim of politicians and bankers is another one.

"Sats are my safe haven." —Matt Odell

Bitcoin is quickly becoming a safe haven asset, especially for people who don't have easy access to more "stable" currencies than their own. On a long enough time scale, bitcoin offers stability in a world of global instability. It _guarantees_the right to save: nobody will be able to take away your sats — you must give them away willingly.

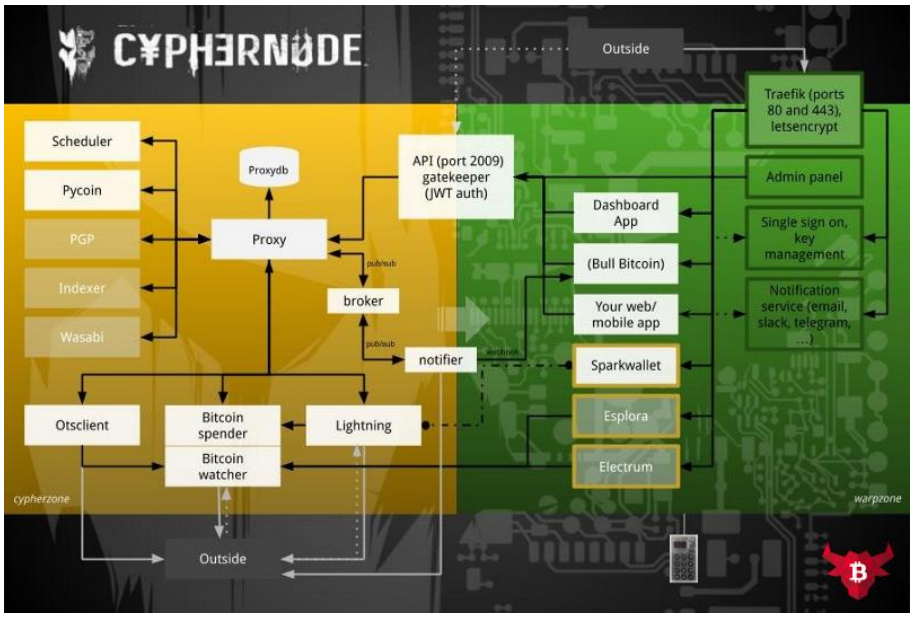
Building towards a Sovereign Future

People are fed up with the tyranny of the banks, the tyranny of the state, the tyranny of Facebook, WeChat, Sina Weibo, and everything else which is "too big to fail."

It is our collective responsibility to build a better future. A future where the freedom to transact, the freedom to remain private, and the freedom to save your wealth over time are guaranteed. In the words of the United Nations: the same rights and freedoms people have offline must also be protected online.

We want to help build a world which enables sovereign individuals to strive. A world where every individual — and every company, for that matter — can use freedom-enabling technologies, as they see fit, without asking anyone for permission. This is one of the reasons why we have released cyphernode, a suite of software and utilities to operate enterprise-grade Bitcoin services, as free software.

Cyphernode — free as in freedom.



While it is debatable whether Bitcoin can literally solve every problem of the world, it is undoubtedly a big piece of the puzzle. Technologies which empower the individual are more important than ever before. Technologies which enable you to remain private, speak and transact freely, or tip the balance of power towards the individual in another way will be invaluable for the world we are heading towards.

China is giving us a taste of what living in a dystopian surveillance state is like: you cross the street at the wrong place or the wrong time, and thanks to facial recognition, a fine is automatically deducted from your bank account while an

algorithm adjusts your social credit score downwards. You pay for a bus ticket to take part in a peaceful protest, and you are at risk of being erased from the central registry, effectively erasing your ability to live a normal life as a citizen. It might happen today, it might happen tomorrow, or at any point in the future. The surveillance state does not forget.

The tools to guarantee freedom for all exist today, they are just not evenly distributed, not well understood, and not widely deployed. However, with every passing day, more and more people are realizing what kind of power is in their hands.

We encourage you to stay strong. We encourage you to keep on building. We encourage you to not give in to tyranny. We, and many people like us, will do our best to build towards a better future. Stay safe out there, and don't forget to buy bitcoin.

Bitcoin is Not Too Slow

By Parker Lewis

Posted August 23, 2019

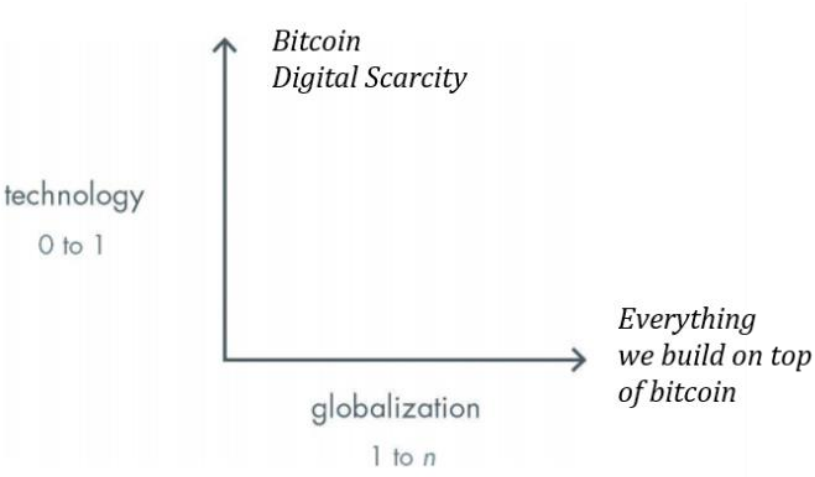
In Peter Thiel's *Zero to One*, he outlines the impact new technology has on building a non-zero sum future. While the book is focused on individuals and companies, bitcoin as a monetary system is the ultimate zero to one technology leap. For historical examples, Thiel highlights the advent of the steam engine as well as the shift from typewriters to computer processors among others. He also articulates a view that innovation has largely stagnated since the early 1970s, while noting that technological progress since then has been more 1 to n than 0 to 1. Bitcoin fixes this. Bitcoin's innovation is not only zero to one; it is fundamentally distinct from the class of innovation that is the focus of Thiel's book. Bitcoin is a monetary protocol built on digital scarcity, the impact of which will be far broader than steam engines and computer processors.

Bitcoin fixes this

There's a new meme floating around the internet; whatever the problem, *bitcoin fixes this*. Negative yielding debt? Bitcoin fixes this. Wealth inequality? Bitcoin fixes this. Endless global war? Bitcoin fixes this. Financial crises? Bitcoin fixes this. Rage culture? Bitcoin fixes this. We're not exactly sure how just yet, but it's an articulation of the balancing effect a sound and stable monetary system will have on every aspect of society. Money is the coordination function of society. It allows hundreds of millions of people to cooperate who otherwise would not have a basis to do so. And, bitcoin is the tool that will allow for more peaceable coordination because it is both unmanipulable and devoid of moral hazard. How it globalizes is the "1 to n" problem (not in the express sense as Thiel describes), but the solutions to scale bitcoin will naturally be incremental. The non-zero sum collective benefit that follows may not literally cure every ill in the world, but the invention of a step-function change monetary network is fundamentally different than any single product because money is the economic good that coordinates all other economic activity.

"The problem is precisely how to extend the span of our utilization of resources beyond the span of the control of any one mind; and therefore how to dispense with the need of conscious control and how to provide inducements which will make the individuals do the desirable things without anyone having to tell them what to do." – F.A. Hayek, The Use of Knowledge in Society

Hayek writes about the invention of money and the price mechanism as the tool that allows society to dispense with the need of "conscious control." Bitcoin is the superior successor to this mechanism, and its zero to one innovation is digital scarcity, not payments or speed of transactions. While bitcoin's property of scarcity still needs further stress testing, it is a profound achievement and what makes bitcoin unique. Never before bitcoin has any asset, let alone a digital one, been finitely scarce; the end result of its innovation is the hardest form of money that has ever existed. That is the zero to one achievement and a phenomenon that almost certainly will not be repeated.



Every other problem that bitcoin will have to overcome is more pedestrian relative to scarcity. Digital payments? The idea that human ingenuity can create digital scarcity but that we then cannot layer on payments technology does not logically follow. Payments technology is just one of the many 1 to n innovations that will be built on top of bitcoin to globalize its adoption. Not only are payments easier to solve, it is also not a critical path that needs solving **today**. The primary use case for bitcoin today is as a savings mechanism, not payments. Over time, as adoption increases and as more infrastructure is built, bitcoin will evolve into a more transactional currency, but that process will occur gradually, not suddenly. And as the shift occurs, bitcoin adopters will continue to leverage legacy monetary systems and legacy payments rails.

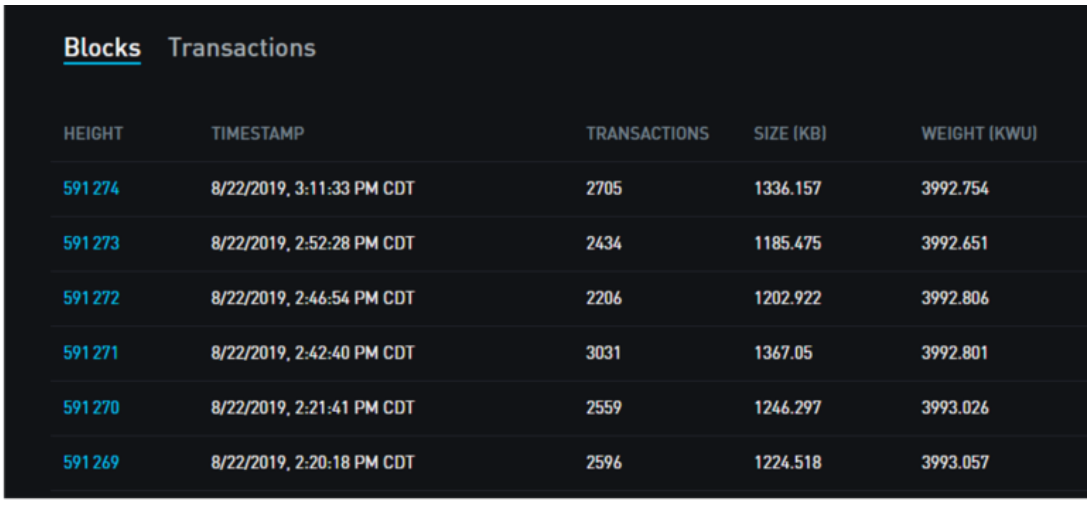
Not a Payments Rail

The bitcoin blockchain will never be a layer for mass payments, but there is a considerable amount of debate on this topic. Many hold the view that for bitcoin to be "successful" it needs to be a one-stop shop, combining the roles of currency issuer, settlement layer and payments rail. While bitcoin fulfills the first two functions beautifully (currency issuer + settlement layer), it is categorically not a payments rail. Both for reasons of speed and scale, bitcoin

fails the payments test. The good news? We don't need the bitcoin network to be a payments rail.

Much of the confusion in the philosophical (rather than technical) debate stems from the opening salvo of the bitcoin whitepaper: "a Peer-to-Peer Electronic Cash System." Peer-to-peer has been interpreted by some to imply that bitcoin needs to be able to handle every last transaction in the world between any two peers. Separately, others believe that if bitcoin transactions cannot occur at the scale or speed of Visa or Mastercard, it is structurally flawed. Essentially, according to skeptics, if bitcoin cannot meet both of these standards, it fails on its promise. Thankfully it does not.

For additional background, bitcoin blocks are solved every 10 minutes **on average*; however, bitcoin blocks are not solved precisely every 10 minutes on a fixed schedule. The next block may be solved in 1 minute or 20 minutes, 30 seconds or 36 minutes. The network adjusts such that blocks are solved on average every 10 minutes. How could a merchant or transaction processor live in a world either this slow or unpredictable? Separately, bitcoin blocks have a limited amount of space to include transactions. While there is not a fixed transaction capacity in bitcoin by count, each bitcoin transaction consumes a limited amount of block space; as a function of limited capacity, blocks include approximately 2,700 transactions on average. With ten-minute average block intervals, six blocks per hour, 24 hours per day, 365 days per year, that equates to a network capacity of approximately 145 million transactions per year which is the equivalent of approximately 4.6 transactions per second. Visa on the other hand processes 124 billion transactions per year at a rate of ~4,000 transactions per second (see here).



Blocks Transactions

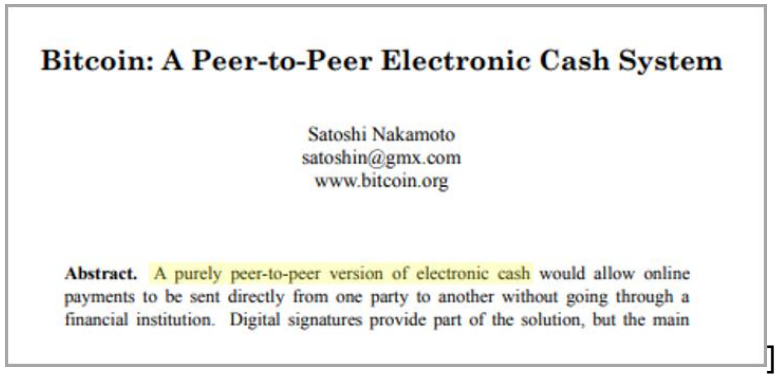
HEIGHT	TIMESTAMP	TRANSACTIONS	SIZE (KB)	WEIGHT (KWU)
591 274	8/22/2019, 3:11:33 PM CDT	2705	1336.157	3992.754
591 273	8/22/2019, 2:52:28 PM CDT	2434	1185.475	3992.651
591 272	8/22/2019, 2:46:54 PM CDT	2206	1202.922	3992.806
591 271	8/22/2019, 2:42:40 PM CDT	3031	1367.05	3992.801
591 270	8/22/2019, 2:21:41 PM CDT	2559	1246.297	3993.026
591 269	8/22/2019, 2:20:18 PM CDT	2596	1224.518	3993.057

Source: blockstream.info

How can bitcoin be the purely peer to peer engine that powers the global financial system, if it operates at nearly one one-thousandth the scale and speed of Visa alone? The reality has always been that, if bitcoin were to have a

non-zero value, the consequence would be a system so valuable that any base layer would not be able to handle all transactions without sacrificing decentralization or censorship resistance. Without these properties, bitcoin would not be a zero to one innovation and its value function would break down. Ultimately, the bitcoin protocol layer provides the function of currency issuance and final settlement, but it is not capable of storing every small purchase, including your Starbucks, for the rest of time for everyone.

If it were the latter, all transactions by all people, no matter how big or how small, would have to be validated and stored by every other person on earth. Without a mechanism to align the interests of network participants, a tragedy of the commons problem would exist and the end result would be a less secure currency system subject to centralization. Instead, we accept a mechanism to limit transaction throughput at the base layer, shifting aspects of bitcoin's peer-to-peer transactional architecture to separate layers that integrate with bitcoin. These tradeoffs have been made in order to secure the foundation of bitcoin's monetary system (decentralization → censorship resistance → fixed supply).



Bitcoin: A Peer-to-Peer Electronic Cash System

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

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main

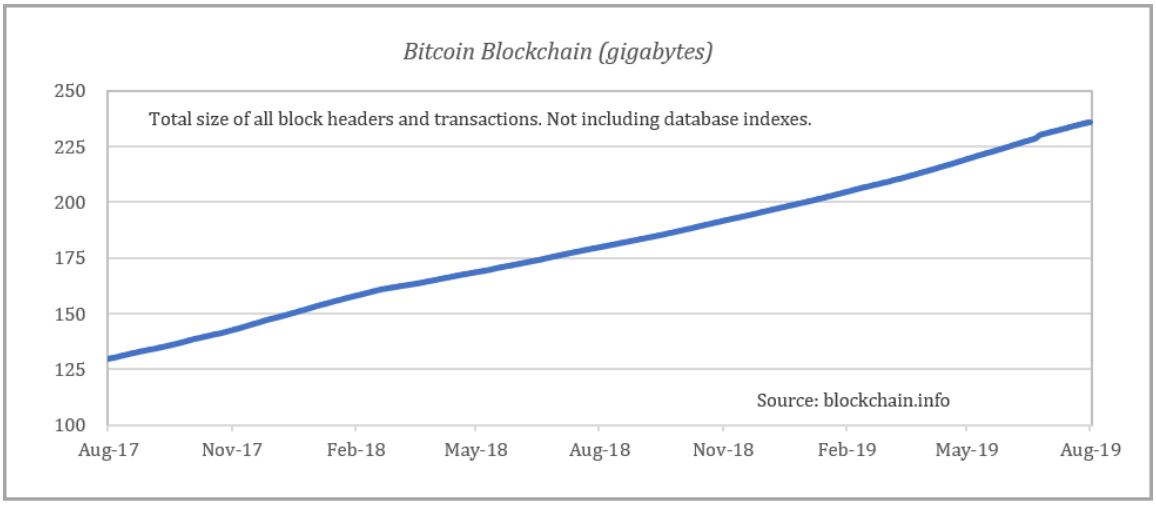
]

Many point to this text from the bitcoin whitepaper released by its pseudonymous founder as evidence that bitcoin was always intended to fulfill every payment by every possible network peer. It does say "purely peer-to-peer" after all. However, more important to bitcoin than anything written in this summary (or any interpretation) is bitcoin's consensus mechanism. Everything critical in bitcoin is enforced by a consensus of network participants, including its fixed supply and ultimately the capacity within each bitcoin block, which limits the number of transactions it can process. This is the fundamental difference between bitcoin and the legacy financial system: monetary policy by consensus rather than by fiat. Bitcoin's founder created a system that ultimately removed critical decisions from any central authority, instead deferring to the wisdom of market consensus. It is a system that is flexible enough to be adapted but rigid enough that any material change is very difficult. As a consequence, network peers have to decide, on a decentralized basis, how best to scale bitcoin. It is through this consensus mechanism that bitcoin dispenses of the need for "conscious control."

Security Trade-offs

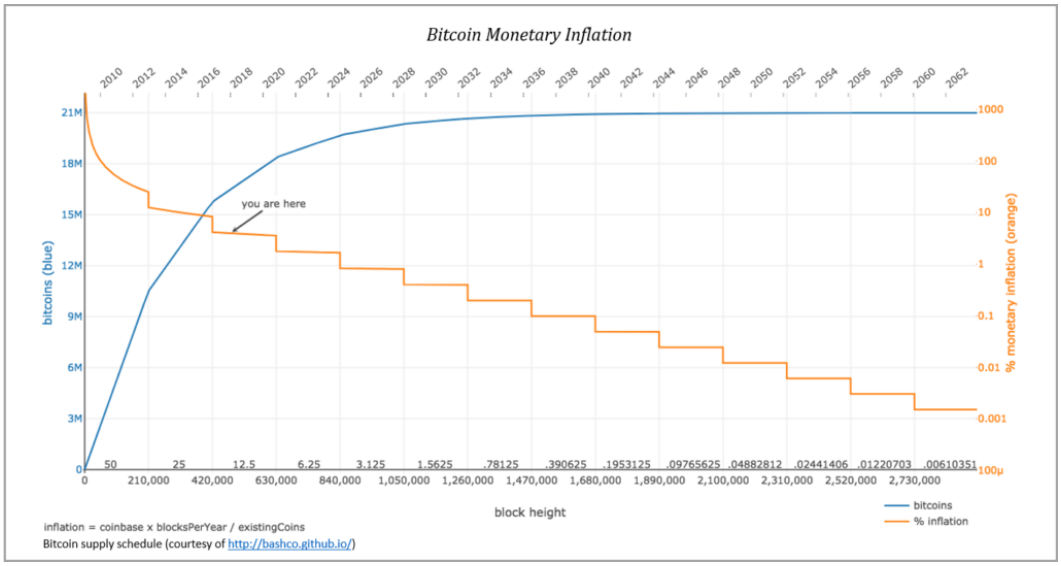
Everything comes with trade-offs. In bitcoin, there are two holy grails: a fixed 21 million supply and preventing the currency from being spent multiple times (the double spend problem). The value of bitcoin is derived from its ability to secure both of these functions on a decentralized, trustless basis and both are inextricably linked to bitcoin's fixed network capacity. Think of the capacity within each bitcoin block as valuable digital real estate. All market participants seeking to clear bitcoin transactions have to compete for block capacity. Scarcity in network capacity is the function by which bitcoin's shared resource is optimized. Or, think of it as bitcoin's solution to the tragedy of the commons. Competition for this scarce resource ensures that the resource is used efficiently and that its value is maximized. Ultimately, scarcity causes market participants to compete with each other, bidding up the value of the network's capacity, rather than shifting negative externalities on to the rest of the network.

In bitcoin's free market, the highest value and most profitable transactions are prioritized. Without scarcity in transaction capacity, this value function would break down. It is less important that we optimize for transaction capacity and more critical that scarcity exists. No one really knows the optimal amount of transaction capacity at any point in time, partly because demand is ever changing but also because it is generally growing over time. The critical piece is that capacity is known and scarce, which allows market participants to plan and ultimately, to compete. The commons is never depleted; instead participants compete and innovate to figure out how best to utilize a scarce asset. Scarcity ensures that the commons is not abused and creates a predictable rate of growth in the overall size of bitcoin's blockchain, which ultimately protects and promotes decentralization.



As discussed in a prior edition (see here), miners secure the bitcoin network by devoting real world energy resources to run cryptographic hashing functions and to solve bitcoin blocks. By solving blocks, miners validate history and clear current transactions which are then checked and validated by the rest of the network. In return, miners are paid in bitcoin. Devote resources to secure the network and get paid in the network's native currency (bitcoin). The actual compensation paid to miners comes in two forms: newly issued bitcoin and transaction fees. In order to devote resources today to secure the network, miners have to reliably expect that aggregate compensation will hold its value into the future.

Approximately every four years, the newly issued bitcoin paid to miners gets cut in half (the bitcoin "halvening"). Today, with each block, 12.5 new bitcoin are issued. In approximately eight months, when the next halvening event occurs (see here), that amount will be reduced to 6.25 new bitcoin per block. Approximately four years after that, 3.125 new bitcoin per block will be issued. This process will continue until we reach the smallest unit of bitcoin (1/100,000,000th) and thereafter no new bitcoin will be issued. This is the issuance function that governs bitcoin's fixed supply (21 million), and as a derivative function, it also shifts compensation to secure the network from (mostly) new bitcoin today to ultimately a system relying completely on transaction fees.



But how does this relate to Visa and transaction capacity? If it were not for the scarcity of capacity in each bitcoin block, there would not be a mechanism to create a transaction fee market. Scarcity in block space creates competition between market participants to clear transactions which causes them to bid up the value of real estate and to use it efficiently. Without a fee market, the only mechanism to pay miners to secure the network would be to alter bitcoin's fixed monetary policy and increase supply. But recall that scarcity in

bitcoin's fixed supply (21 million) is the basis of its store of value property, which is where the rubber meets the road. By creating scarcity in network capacity, we also ensure the integrity of bitcoin's fixed supply, which makes the whole value cycle function. Working within this reality, scarcity is a far more important property than either the speed or ultimate capacity of transaction throughput.

Fixed Network Capacity → Limited Transaction Capacity → Fee Market → Fixed Supply of Bitcoin

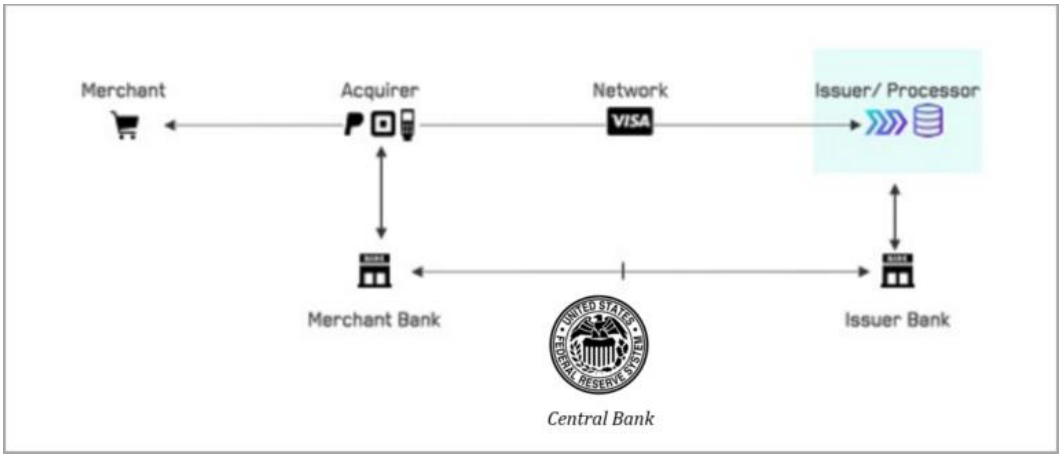
And because the real problem bitcoin is intending to solve is that of money and global QE (not payments), those that store wealth in bitcoin would much rather secure the money supply than sacrifice its long-term integrity and credibility for transaction throughput. In short, the future of bitcoin is far more secure in a world where all market participants can depend on it having a reliably fixed and scarce supply, while accepting lower transaction throughput or speed as trade-offs. What good is high transaction throughput and faster speeds if the fundamental value of the underlying currency is at risk? The existing financial system has already made the opposite trade-off for us. High transaction throughput and fast transactions by way of centralization but with the cost of an architecture susceptible to systemic monetary debasement. Bitcoin represents the alternative, and we are not about to make the same mistake twice.

Bitcoin ≠ Visa

Ultimately, bitcoin is not competing with Visa for supremacy in global payments. Instead, bitcoin is competing with the dollar, euro, yen and gold as money, and any comparison to Visa, its transaction volume or transaction speed is fundamentally flawed. Bitcoin fulfills the role of currency issuer and final settlement. As a result, the proper comparison would be between bitcoin and the Fed as currency issuer and as a clearing mechanism. No one makes the mistake of confusing the functions of Visa for that of the New York Fed, but for some reason, the comparison is often made between Visa and bitcoin.

While it would require time and investment, Visa's payment network could sit on top of the bitcoin network to fulfill payments much the same way it sits on top of the existing banking system. Rather than clearing the currency through a central bank, final settlement of transactions would clear through the bitcoin network. In the existing architecture, the payments layer (Visa) and the settlement layer (banking network/central banks) are separate and distinct. The principal problem bitcoin intends to solve has little to do with the former, but instead, with the mechanism by which currency is issued and cleared (think the Fed and QE). Visa helps move dollars but Visa is not the dollar. It is a

technology company that provides a service; it has 17,000 employees. Bitcoin has none.



Whether credit or debit, Visa is an inherently trust-based credit system. While consumers generally associate swiping a Visa card (or the equivalent) at a point of sale terminal as payment, it really is not. Instead, balances are checked, transactions are authorized and settlement occurs later. Dollars are not actually cleared through a central bank or settled at the point of sale every time a transaction is processed. Individual transactions are also never really cleared. Instead, transactions are batched together, netted and settled at a later point in time; only then are accounts credited with proper balances. So when someone attempts to equate a Visa transaction with final settlement, that is just not the way the world works. But that is the comparison that is implicitly being made when someone attempts to compare Visa with bitcoin.

Bitcoin vs. the Federal Reserve

When compared against its real competition (the Fed, ECB, BOJ, etc.), bitcoin begins to look like a Ferrari. Final global settlement approximately every 10 minutes, 24 hours per day, 7 days a week, 365 days a year on a permissionless basis. Compare this to the existing permissioned financial system, which is subject to multiple layers of bank and central bank intermediaries and only open during “business” hours. This is the great misnomer that exists within bitcoin. Those that believe bitcoin to be too slow or lacking in network capacity are comparing bitcoin to the wrong application. We could set up a network of banks on top of the bitcoin network and the payments system could function as it does today.

The push back on this point is the risk of centralization. If bitcoin were to just sit in centralized banks, it would increase the possibility that the bitcoin network could be co-opted and undermined by a network of banks and central banks, whether to force changes to network consensus rules or to censor end users. Ultimately, this was gold’s failure as a monetary medium. It

was susceptible to centralization, which then spawned fiat currencies, which have turned out to be easily manipulable. While this is unlikely (and hopefully not) how bitcoin scales, money and payments technology are distinct problems. The fundamental reason being that there are two sides to every value transfer; one side almost always involving money and the other as the fulfillment of goods and services. Payments layers help provide a bridge.

Because of the nature of trade, the two sides of a value transfer generally, and naturally, occur by different processes and at different points in time. Think about the settlement of currency on one side and the transfer of title to a home or car on the other. Or, payment for a good on Amazon and the fulfillment of that good two days later. Two different processes, occurring at two different times. And, it is important to recognize that bitcoin has no knowledge of the outside world, whether identities or the second leg of a value transfer; all bitcoin knows how to do is issue and validate currency (whether a bitcoin is a bitcoin). This is really the function and limitation of any base currency system. Payments layers provide a bridge between currency settlement (the Fed or bitcoin) and the fulfillment of goods and services. Gold solved mass payments via bank centralization, the dollar, the Fed and large payments processors such as Visa. Bitcoin likely solves payments through a technologically superior mechanism, but we have time to solve what is a separate and distinct problem from that of money.

Scaling Bitcoin is 1 to n

If we solve the problem of money through digital scarcity first (zero to one), the technology advancements to scale transactions and ultimately solve payments are 1 to n. It is not credible to think that human ingenuity can solve the former but then fail on the incremental derivatives. It is not just a matter of hope and faith; instead, it is one of reason and logic, considering both the advancements in scaling solutions that are already being pursued and the challenges relative to the problem bitcoin has already solved. Permissionless innovation and the economic incentives inherent in bitcoin will coordinate and accelerate solutions to any number of future challenges. Market participants have an incentive to increase the value of the network and to innovate to scale the network, but the solutions will have to work within the network's consensus or garner sufficient consensus to change the rules.

Because of the nature of bitcoin's economic incentives, it is far more likely that scaling solutions work within existing consensus rules. One such example of an advancement to scale bitcoin within the network's consensus is the lightning network. The lightning network builds on top of bitcoin as a trust-minimized layer to scale transaction capacity, which still remains fundamentally distinct from payments fulfillment. However, if successful, lightning will be used to create bitcoin payment channels that enable far greater transaction

throughput at far lower cost, the scale and speed of which would rival Visa. While it may not be the ultimate solution, it is an example of the innovation that bitcoin is fostering. Lightning is also only one of many solutions that are actively being developed, and competition will drive us toward the best scaling solutions, of which there may be a combination of many.

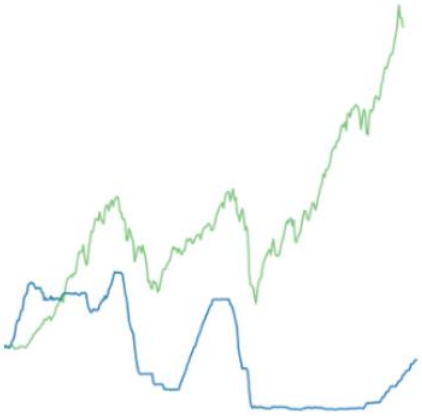
The approach to scaling bitcoin is a slow and conservative process. Bitcoin is too important to follow the Silicon Valley mantra of move fast and break things. Instead, it's move slowly and don't break anything. If a global financial system is to be built on a decentralized monetary system, the foundation must be protected at all cost. Ensure the security of the base monetary layer (bitcoin) first and then allow network participants to innovate on top of it in a permissionless manner. Remember that bitcoin is only ten years old; we are in the very inception of bitcoin's monetization event, and infrastructure is still being built to allow for the proliferation of this new technology.

It's a little ridiculous to contemplate the problem bitcoin has already solved and then immediately pivot to a "but why not mass payments today" line of thinking. Especially when considering that bitcoin, in its clearing function, is already faster and more reliable than comparable mechanisms for final settlement of dollars, euros, yen or gold. Then, when understanding that the fundamental use case for bitcoin today is as a long-term savings mechanism (not to fulfill payments), it becomes more clear that not only is the problem misdiagnosed but also that the desired solutions can wait. We will need the ability to fulfill payments in the future, but we have time before we get there. In due time, we're going to have our cake and eat it too.

Bitcoin for safety

By James O'Beirne

Posted August 24, 2019



The fed funds rate (blue) vs. S&P500 (green), and chairs of the Federal Reserve.
Starting in 2008, central banks injected an unprecedented amount of new money into the global financial system. Along with big gaps in wealth distribution, this has created profound systemic risk. The last few months have shown indications that this risk is starting to come to the surface.

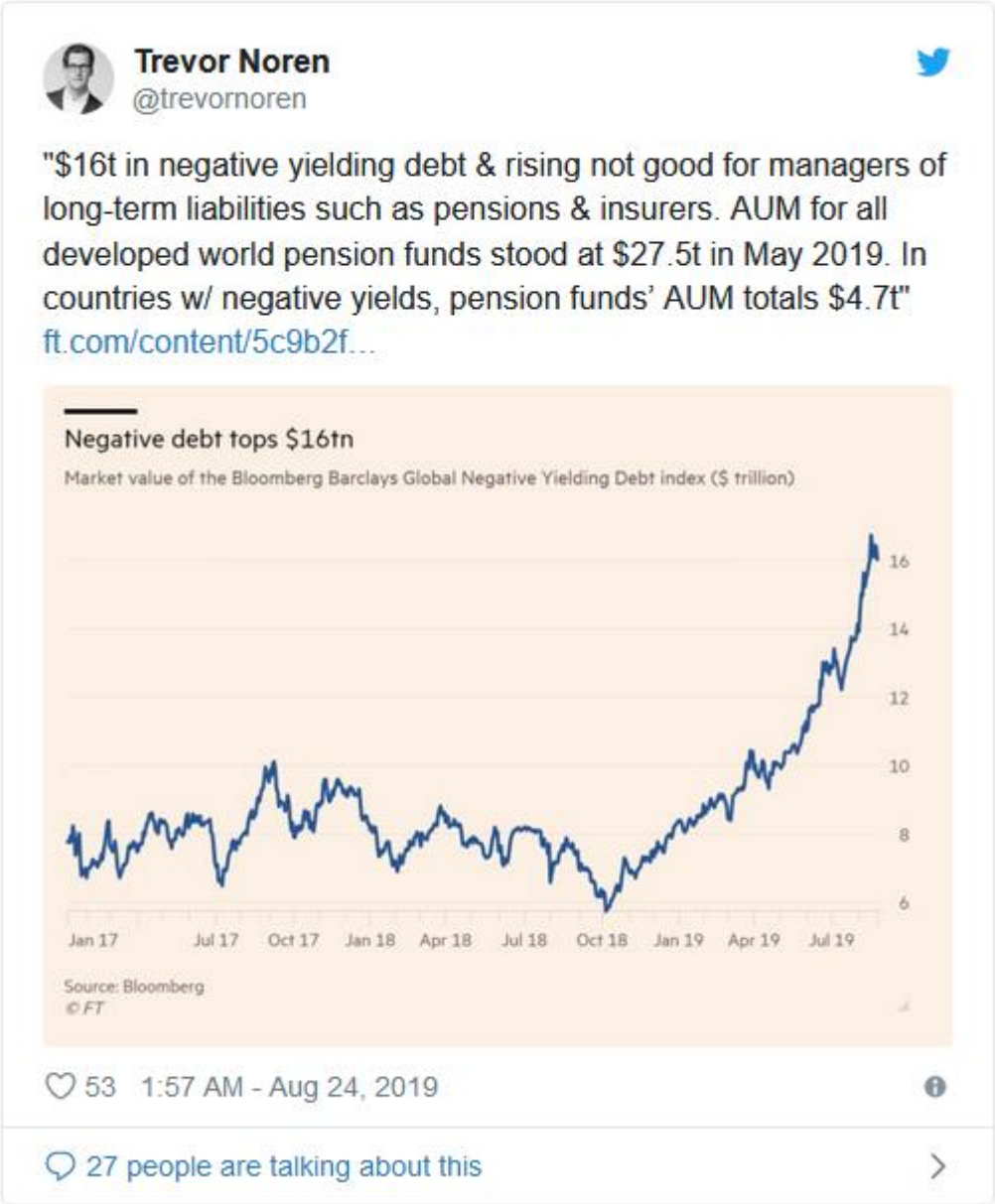
The setup in front of us is not for a garden variety recession. It's for potential cataclysm: a drawdown that will hit normal investors hard, but retirees and pensions especially so, threatening the premise of our financial system. This crash, or even just the threat of it, will lead our governments to take extraordinary action in an attempt to avert a long depression. That action will cause an incredible level of inflation.

As I've watched the following events play out, some of the only optimism I feel is due to the emergence of Bitcoin as a nascent asset class. I see this new tool as one of the only potential safeguards that people in normal income brackets have against the kind of trouble I'm forecasting.

As I lay out the narrative I've watched unfold over the past few years, I'll occasionally interject with observations (formatted like this) on why I think Bitcoin is going to become increasingly important, even relative to traditional safe-haven assets like gold. After reading a draft of this post, my brother lovingly dubbed this "the shill zone," and I don't disagree.
It should be obvious, but as an explicit disclosure: I am long Bitcoin.

Welcome to negative

It's an exceptional time in economics. Negative-yielding bonds have passed the $16 trillion mark for the first time ever. Germany's flagship 30 year bond yield has gone negative, also for the first time in history.



This means that investors are paying governments (and some companies) for the privilege of lending them money. I pay the German government $10,000 today and in thirty years I get back $11 less. Intuitively this doesn't make much sense: given the time-value of money, cash I have on hand now should be worth more than theoretical cash in 30 years, at the very least because I may not be around in 30 years to spend it.

And besides, there's what we call "counterparty risk:" the possibility that the German government might not repay me (admittedly a low likelihood) or the possibility that the euro will have suffered significant inflation since then, reducing the real purchasing power of my $10,000 (a much higher likelihood). The risks of lending money for 30 years should be offset by some reward, but with negative yields the lender is penalized for assuming this risk.

This may not seem like such a big deal, or at most a weird abstraction more or less confined to finance people, the kind of people who worry about bond yields and think in basis points.

If only.

Negative yields dramatically affect, for example, retirees because traditionally retirees have held a lot of money in "fixed income," or bonds. The deal was that you spent your prime years earning, saving, and maybe investing in risky assets (equities) and as you got closer to retirement age, you flipped most of your allocation to less risky investments that yield a consistent return - i.e. bonds. This ensured that your hard-earned savings wouldn't evaporate in an equities downturn.

Since negative rates eat at savings instead of paying out, retirees—and pension funds, but we'll talk about those later—are driven towards keeping their money in risk, or equities and lower quality credit, and basically having their savings exposed to the stock market and all its associated drama:

These low rates have been great for borrowers including countries, companies and mortgage holders, since the cost of servicing debt has dropped. On the flip side low and negative interest rates have been bad for pensions and retirees who are trying to generate enough income from their assets to meet their liabilities through lower volatility bonds. These groups need to buy riskier assets and embrace that they will need to accept more volatility in order to achieve their goals. **The bottom line is that no one really knows how this will end up since we've never seen it before.** Forbes

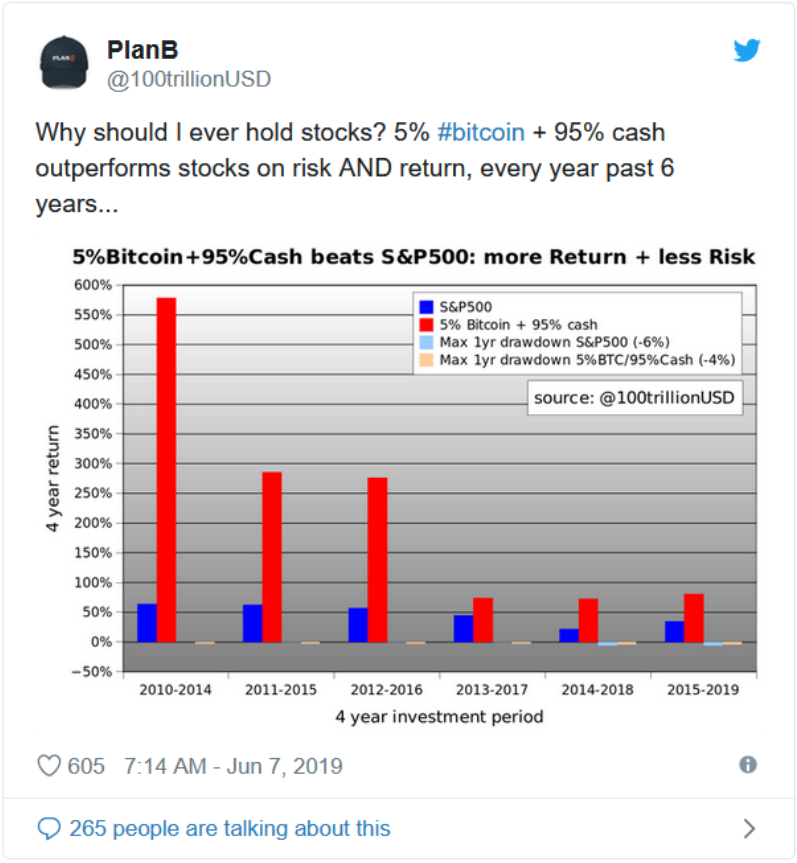
Negative rates are strange and disconcerting in themselves, but reconstructing their cause reveals other big problems as we'll see in a bit.

This is what Bitcoin is for. Bitcoin, like gold, is a "non-productive" asset, a commodity. This means that it doesn't in itself generate yield, though obviously there's been plenty of price appreciation over its ten year life.

For reasons I'll describe shortly, this new asset is a possible tool for countering increasingly negative yields and diversifying savings. A 1 to 5% allocation lets you simultaneously cordon off risk to a small percentage of your portfolio but retain exposure to considerable upside. It's the barbell doctrine incarnate.

Owning bitcoins is one of the few asymmetric bets that people across the entire world can participate in. Vijay Boyapati

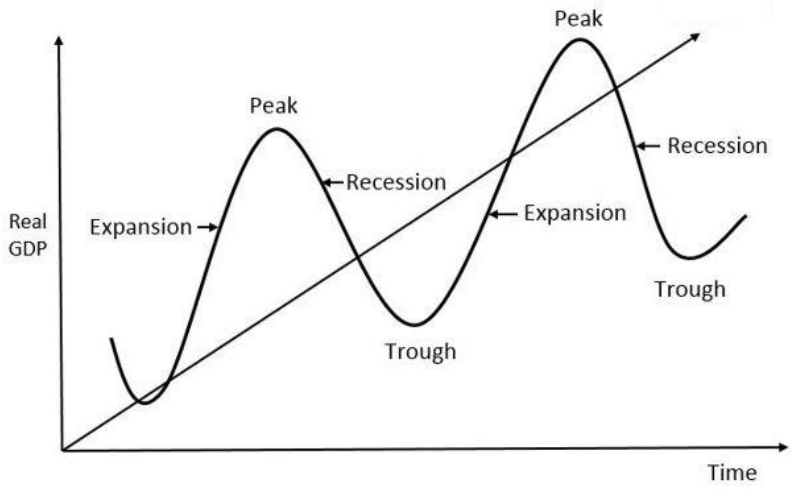
Instead of risking a huge portion of your savings in equities for positive return, you can use a small amount of Bitcoin as a metaphorical call option on a new asset class – an asset class that isn't affected by the same vulnerabilities that have created the negative rate conundrum, in addition to the other maladies we'll get around to later.



How did we get here?

So this $16T pile of negatively-yielding debt is something that's never happened before, and based on common sense it seems kind of unnatural. How did it happen?

For the past 30 years, governments and specifically central banks have been a lot more active in monetary intervention (i.e. influencing the money supply) in an attempt to be *counter-cyclical*. This means that governments basically want to smooth out the booms and busts that the business cycle is naturally subject to.

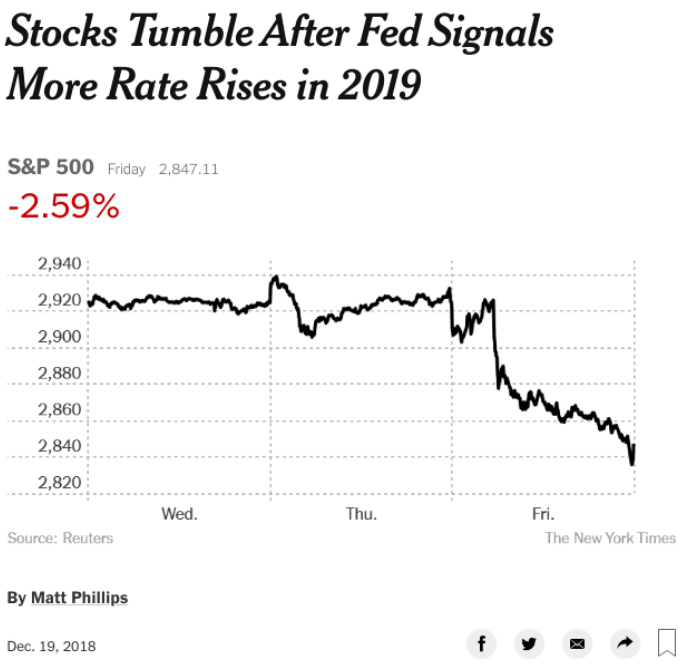


Source

When a recession or depression happens, the central bank steps in and "provides liquidity," meaning they inject cash into the banking system by doing things like buying US debt instruments from certain banks at above-market price. This gives the banks extra cash on their balance sheets to lend out, and so lowers the interest rates on pretty much everything else. This introduces unnaturally cheap credit that is supposed to stoke the economy by encouraging people to buy more things and take out more loans.

When the economy is running too hot, the Fed (the US central bank) raises the price of money and limits credit expansion, though they haven't done much of this in the past 20 years. As we'll see, the economy has become reliant on

cheap credit in deep and interesting ways.

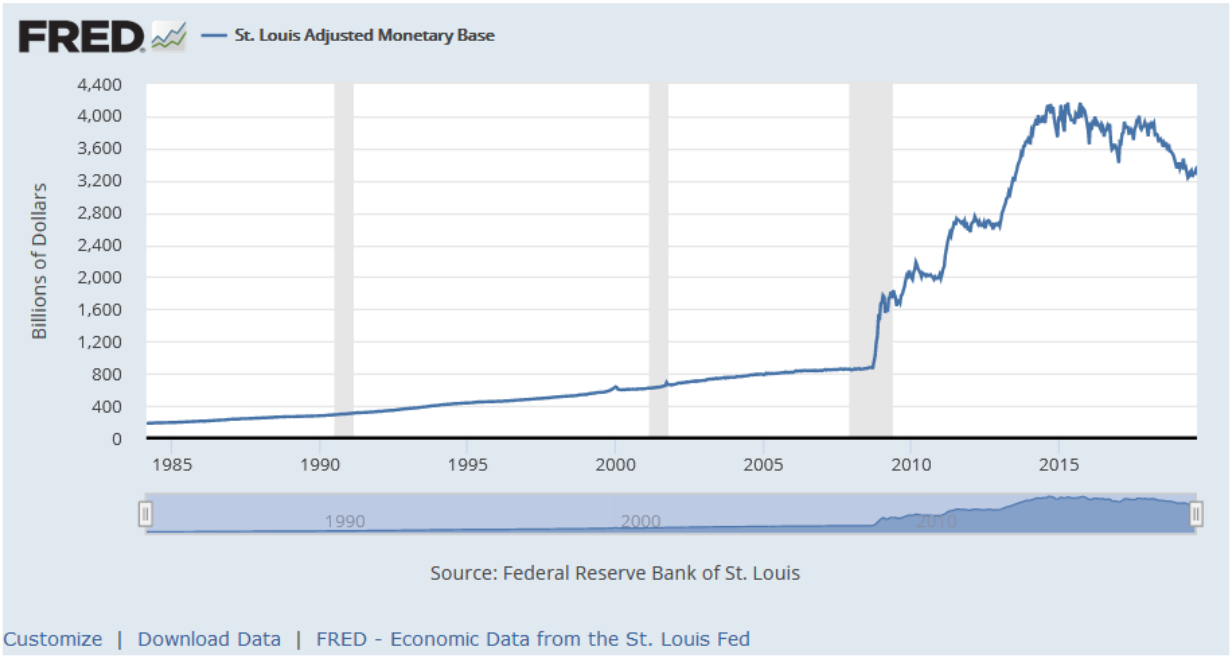


In 2018, the market crashed 11%, the worst December since the great depression, as the Fed tried to raise interest rates back to pre-crisis levels. This crash prompted the Fed Open Market Committee to do a "dovish pivot" back to rate cuts in 2019. The economy will no longer tolerate rising interest rates.

Post 2008

Central bank intervention came to a fever pitch 11 years ago. The 2007/8 financial crisis was so bad that the Fed went beyond its usual measures. It drastically upped its purchase of US Treasuries (debt) and started buying things like mortgage-backed securities.

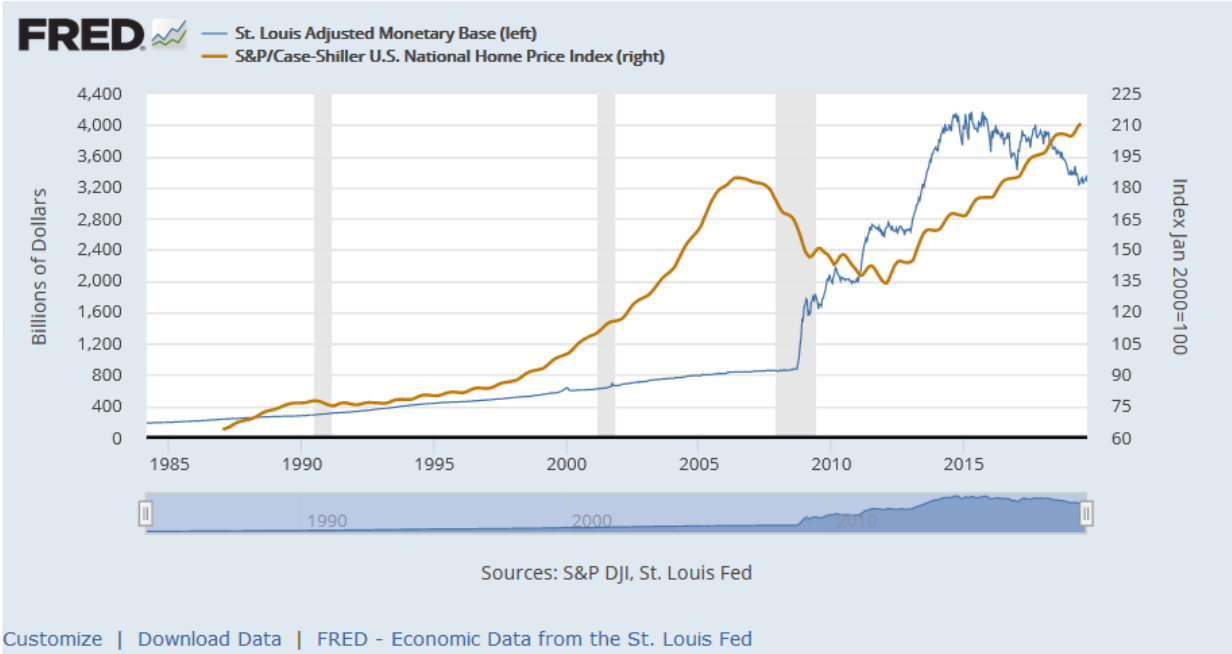
The chart below shows the level of our monetary base, or the amount of currency circulating plus the level of reserves banks hold at the Fed. This is one of my favorite charts of all time, it's just insane.



*Over $3.3 trillion **(5x)** in new money was created starting in 2008.Shaded gray bars are periods of recession.*

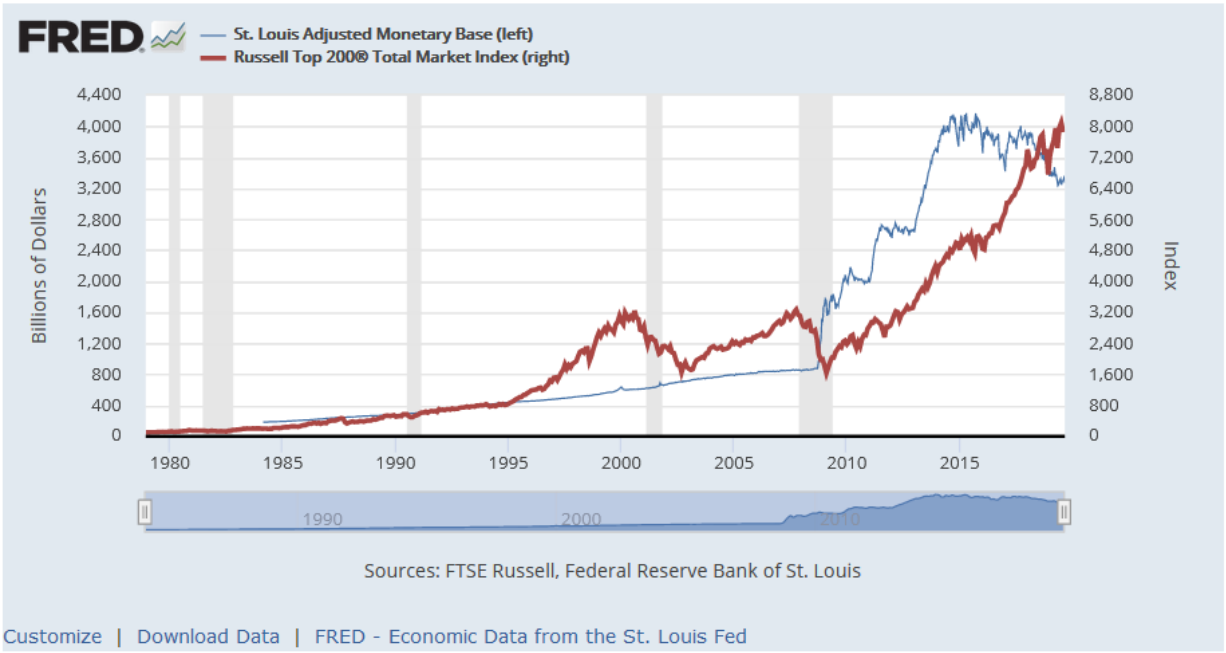
The tricky part about central bank intervention is that it's a discretionary process driven by a relatively small group of people. How much intervention is too much? In 2008, the answer seemed to be "almost no amount is too much."

As you can see above, this resulted in the supply of base money roughly *quintupling*. Why we didn't see crippling inflation is another story for a different blog[1]. Even though we didn't see traditional (and I would argue deceptive) measures of inflation like CPI and PCE spike, all this extra "liquidity" has led to systemic bubbles in important asset markets like real estate



Increase in base money (blue) vs. US home prices (orange).

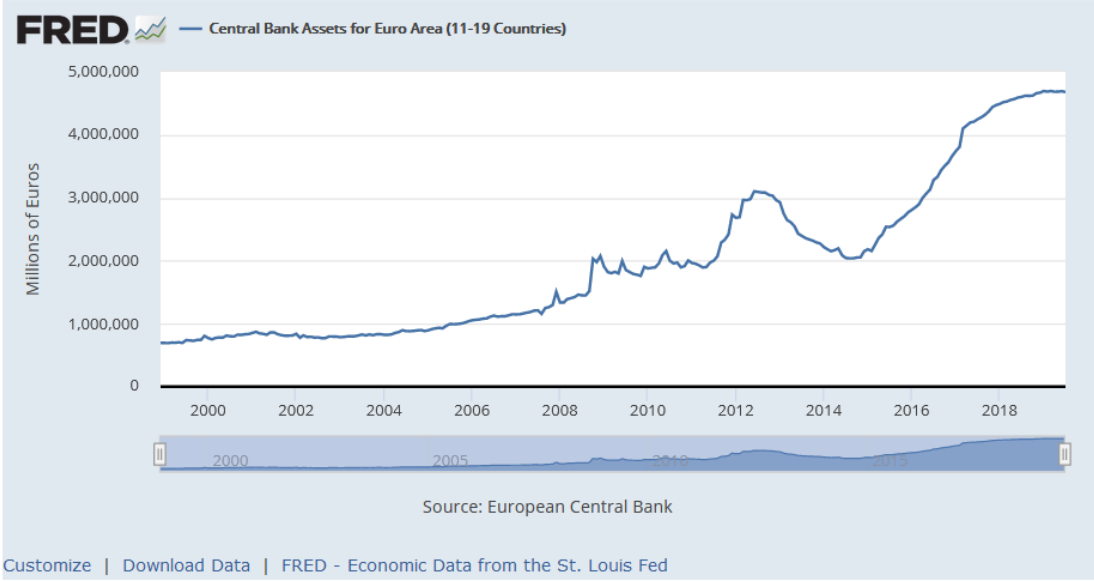
and the stock market.



Increase in base money (blue) vs. stocks (red).

So now the housing market is more overbought than before the crash in 2007 and the stock market is... well, almost two and a half times more overbought than ever.

The root of this being that well-intended central banks are trying to protect us from the volatility that comes with the natural ebbs and flows of the business cycle.[2] Our friends in Europe have basically gone through the same process, except instead of attempting to "normalize" and tighten credit in the last few years, they've had to double down on easing in order to stave off collapse, probably due to intra-EU debt problems.



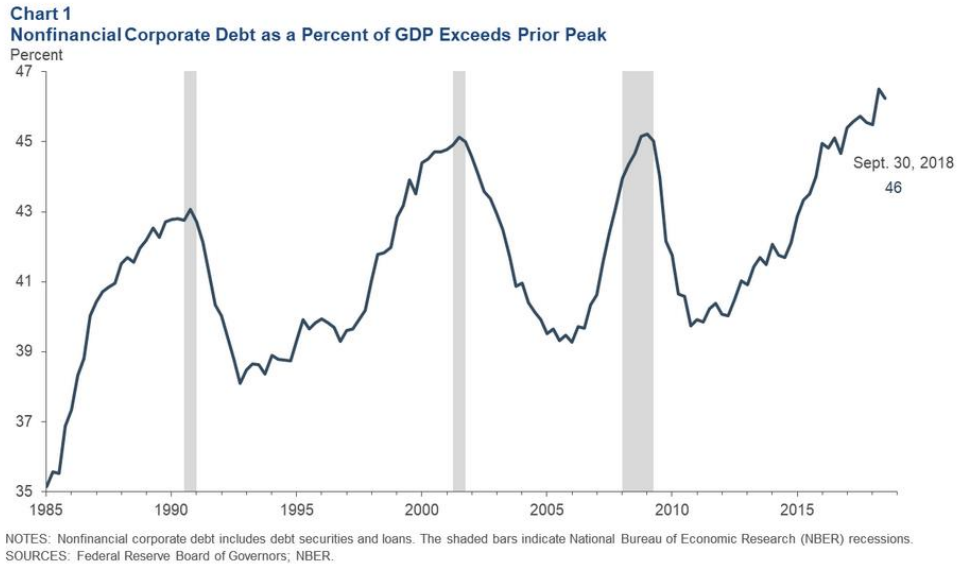
This is what has created deeply negative bond rates in Europe - the European Central Bank (ECB) has been aggressively purchasing bonds in an attempt to inject cash into the economy, which drives bond yields down and in the process hurts anyone relying on fixed income.

This is what Bitcoin is for. Bitcoin's monetary supply can't be expanded by anyone, let alone a small committee of economists. There will only ever be 21 million coins minted. Nobody can decide to try to tame credit cycles with "counter-cyclical" monetary policy.

Because Bitcoin's monetary base cannot be increased, once you have a certain fraction of Bitcoin's total supply you will *always have at least that fraction.* It is literally the only asset ever to have this property, and this fact alone makes Bitcoin extremely unique. As a result, some people refer to Bitcoin as "the metric system for value."

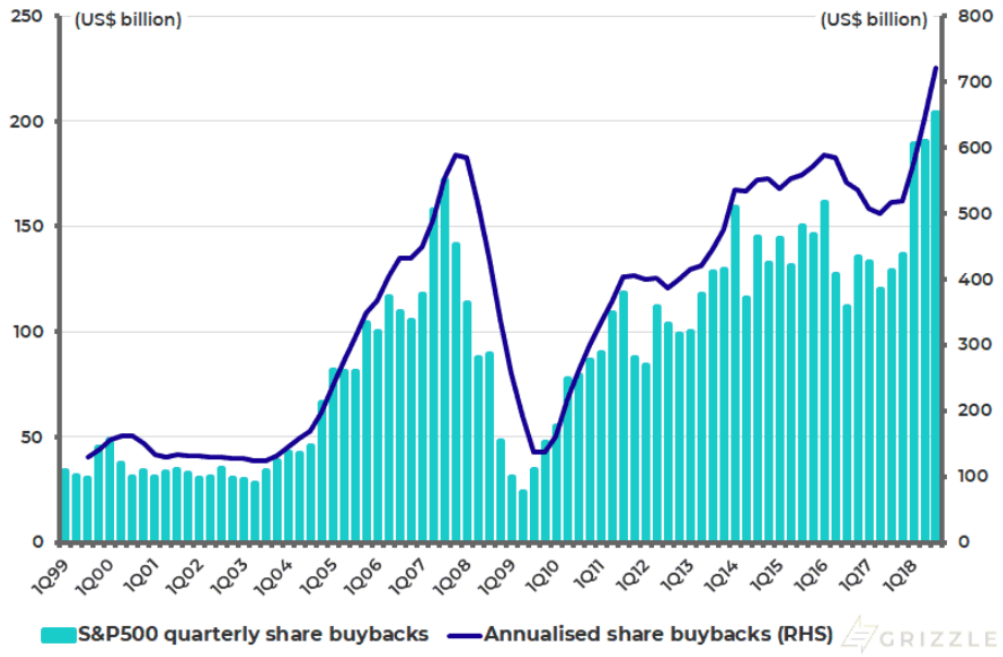
Hair of the dog

Injecting trillions of dollars into the money supply isn't something we can easily walk back from, since the resulting availability of credit has allowed our economy to stave off slowdowns by increasing "leverage," or using debt to fund expansion.



Corporate debt to GDP is higher than it's ever been. From the Dallas Fed.Shaded bars indicate recession.

One way this cheap credit is used is for leveraged share buybacks, a term you've probably heard recently. In a nutshell, this is when a company takes advantage of favorably low interest rates (enabled by the central bank's intervention) to take out a loan. Using the loan, the company buys back its own shares which (definitionally) reduces the number of shares outstanding and artificially boosts earnings-per-share, sending share prices higher. This has the genial side effect of making executive-owned stock options way more valuable.



Buybacks are more frequent than ever and are increasingly responsible for price appreciation. Source

When people talk about "the financialization" of the economy, this is one of the chief symptoms they're talking about. Activity in the real economy

is replaced with accounting semantics.

It turns out that share buybacks are now the dominant source of demand for equities. This is very interesting.

Data from Goldman Sachs

It's interesting because it creates an important dependence on cheap credit in the economy:

- investors, retirees, pension funds[3] have been driven out of "safe" bonds and into equities and riskier credit (corporate bonds) in a search for returns, so there is a systemic dependence on the stock market going up or at the very least retaining its value
- but the dominant buyer of equities are companies themselves (see table above), funded by cheap credit,
- so share prices are largely contingent on credit remaining cheap...

Corporate buybacks are dominant source of equity demand

	Net US equity demand ($ billions)			
Category	2016	2017	2018	2019E
Corporations	**$ 697**	**$ 296**	**$ 509**	**$ 600**
Foreign Investors	(188)	125	(94)	25
Pension Funds	(217)	(162)	(243)	(100)
Mutual Funds	(112)	(134)	(124)	(175)
Households	(151)	226	191	50
Life Insurance	98	(45)	(18)	-
Other	(12)	(17)	9	-
less				
Foreign equities by US	22	167	128	350
Credit ETFs	96	123	100	50
Included among holders above are:				
Equity ETF purchases	$ 188	$ 347	$ 210	$ 300

A quick note on pensions

Public pensions in America probably merit their own post because they're so horrifying, but the short version is that their prospects for solvency are not good. Even assuming a starry-eyed rate of return (7.5% per year), they're still underfunded by $2 trillion.

UNPREPARED

The Pension Hole for U.S. Cities and States Is the Size of Germany's Economy

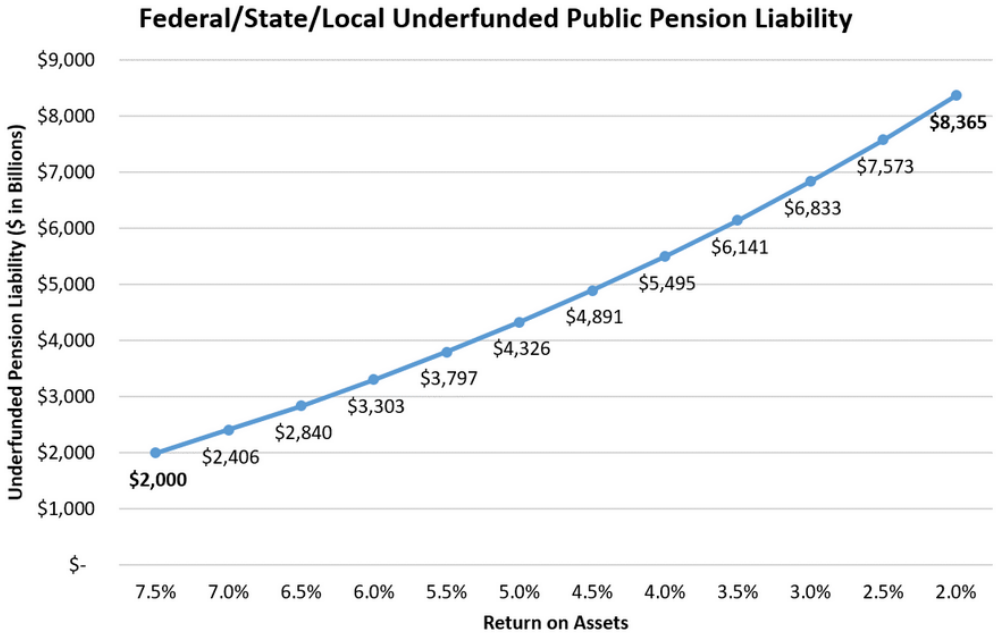
Many retirement funds could face insolvency unless governments increase taxes, divert funds or persuade workers to relinquish money they are owed

Source

There's no risk-free way to get 7.5%. In order to get returns like that, you have to expose yourself to the equities market or, as is commonly the case

these days, low-grade corporate debt. Under normal circumstances, seeing price volatility and riding out periods of loss is a guarantee for the kind of assets that net you 7.5% per annum.

If we assume that pensions get a more realistic rate of return, the unfunded liabilities rise to as much as $8 trillion.



Did I mention that public pensions are still underfunded by $2T+ assuming a 7.5% yearly return?

Keep in mind, this 7.5% of return is expected in a world where most government debt is now *negatively yielding.* In the desperate search for return, pensions are increasingly relying on large positions of risky allocations. For example, the New York State Teacher's Retirement System owns $35 million of BBB-rated General Electric bonds. If the GE fraud story has any merit, those bonds may be downgraded to BB which would compel *all pension funds nationally* to unload the bonds. The funds would sell at a sizable loss and probably crash the corporate bond market.

Because of this chase for yield, the stability of our pension system is now predicated on the stock and corporate bond markets forever performing. There is not good historical precedent for this.

This is what Bitcoin is for. Pensions could juice their returns for far less risk by selling off their large allocation of garbage BBB corporate bonds, almost certain to implode or suffer downgrades in a recession, and placing their risk in a much smaller percentage allocation of Bitcoin.

If pensions are reliant on risky assets for solvency, this means they are now reliant on cheap credit for solvency.

The huge problem starts when and if

- credit *doesn't* get cheaper: slowing and heavily indebted companies like GE and AT&T won't be able to keep buying back and their share prices will fall significantly,
- this puts a drag on the stock market and potentially creates downgrades in corporate credit, a disasterous outcome because
- by law, pension funds are now forced to sell masses of recently-downgraded corporate bonds since they are no longer investment grade (IG), sending corporate yields skyrocketing,
- which further drives the stock market lower as companies become unable to pay their debt by taking out new loans,
- which further batters pension funds and investors.

As you can imagine, this could get really, really bad. Really bad.

Imagine you're a retiree who's been forced into the equities market because you started saving late or you otherwise can't afford low rates of safe credit. You put 80% of your money into equities. Then one day the process above triggers and your wealth halves as the market crashes. This applies equally to pensions.

This is what Bitcoin is for. My guess is that Bitcoin will not be hit nearly as hard as the equity market will, assuming its price doesn't *appreciate* in a scenario like this — a scenario I'd argue Bitcoin was designed for — if it functions as a safe-haven asset. This is because institutional ownership of Bitcoin is almost nonexistent at the moment. In a rush for the exit (liquidity), large institutions will be selling off risk assets, but I don't think these institutions have any substantial volume of BTC to sell.

The kind of ownership that would be compelled to sell in a situation like this, "weak hands," have already been shaken out of their positions by BTC's volatility. The remaining owners are in it for the longterm. It's my guess that in a downturn, BTC's relative price will be neutral to positive.

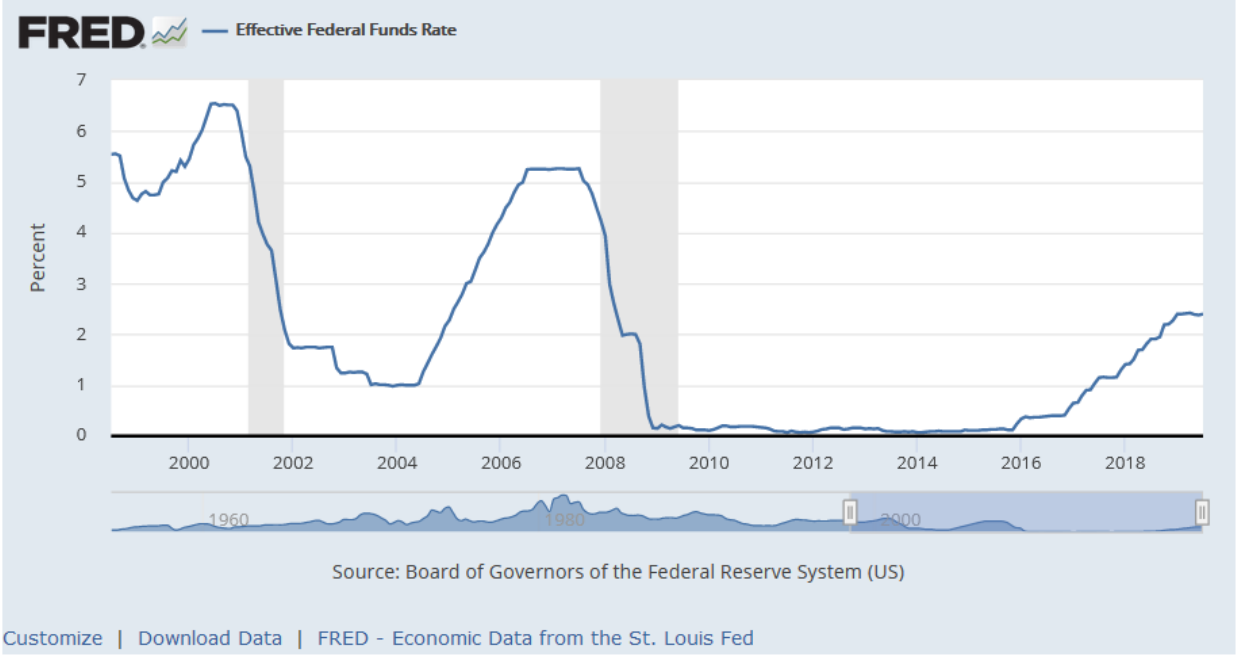
The equities market, having been stoked up on easy credit (now painfully dry) may well see a 60-70% decline. Returning to current levels won't be in the cards for years, maybe decades. We're talking about a depression and a bunch of people who are no longer able to fund their retirement. It'd be bad.

QE forever

So anyway the above is all theoretical, because there won't be a crash… not in the form we're used to, anyway. The government basically can't let this happen. They have to keep the liquidity (read: cheap credit) flowing or else we have, basically, a complete collapse in equities and low-quality debt, and therefore in public pensions (who own large amounts of these things). This starts to get to, like, civilizational severity.

Central banks will have to keep creating money to keep credit cheap so that companies can continue to buy back their own shares and prop up the equity market. This will continue to increase the money supply and will further exacerbate bubbles in real estate and equities. These bubbles will steadily widen the divide between the have-assets and the have-no-assets in America.

The sort of recession that most people expect eventually may never come, since it can't be allowed to come. We may have entered a new monetary regime after the fireworks in 2008.



Short-term interest rates, controlled by the Fed, are on their way back to zero in an attempt to keep the economy afloat.

This is what Bitcoin is for. Central banks will continue easing until there is nothing left of their currencies; I can't really see an alternative. There's no soft landing out of this credit-fueled asset bubble. There's no clean way to deleverage the pile of debt corporates have taken on.

Historically gold has been a safe haven refuge in times of contraction and inflation, and I own some small amount, but I'm no great fan. Gold is impractical: it's hard to verify, hard to custody, isn't easily divisible, and just feels kind of outdated. The only easy way to buy exposure to gold (ETFs) are still just

a paper proxy for the real thing. They're subject to the same kind of risks if there's a huge crash and financial markets are ordered to a halt. Bitcoin maintains liquidity through such a crash because governments can't stop its ability to perform transactions.

Unlike gold, the authenticity of a Bitcoin balance is immediately verifiable with off-the-shelf consumer electronics, and anyone can safely custody it themselves regardless of amount.

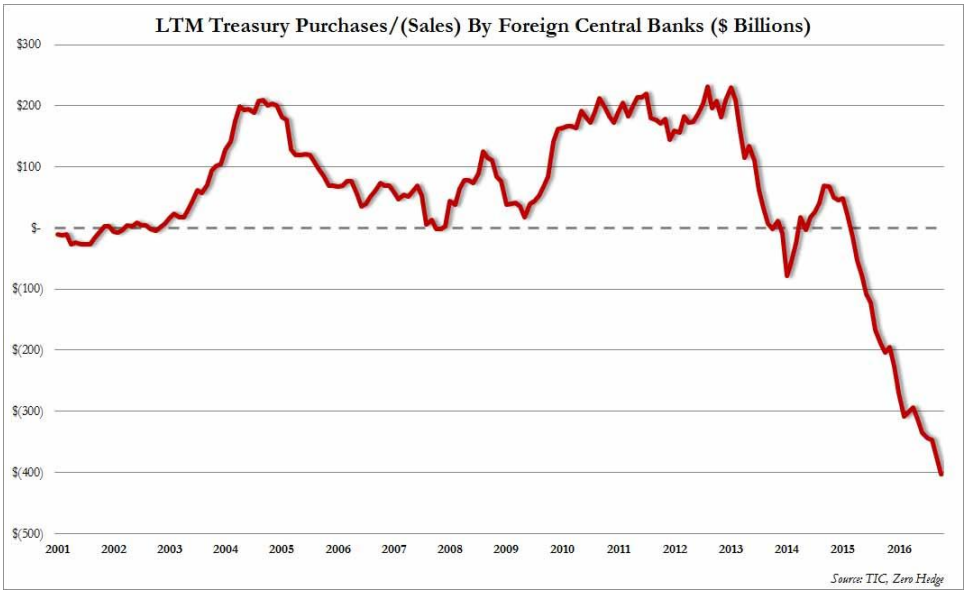
It can't be confiscated. It's perpetually and internationally liquid. It doesn't know borders and gives final settlement in hours. It makes capital flight trivial and open to people who aren't fabulously rich or well-connected. Nobody's sure yet, but for these reasons I think there's a decent chance that Bitcoin will function as a safe-haven asset, much like gold, in a significant downturn.

The macro picture

So far we've mostly just been talking about troubles in the US domestic economy. Things get really spicy when we start talking about the increasing international disgruntlement with the US dollar.

Since the Bretton Woods Conference in 1944, the US dollar has had the "exorbitant privilege" of being the reserve currency of the world. This has meant that there's always a healthy demand for the dollar, which in turn stokes reliable demand for our government debt in the form of Treasuries (well, until recently). This has let us run big deficits without worrying too much: there will always going to be other countries waiting in line to roll our debt by buying Treasuries, right? They want to buy oil, don't they?

Unfortunately, it doesn't look like this will last. Foreign banks have stopped buying US treasuries at an alarming rate.

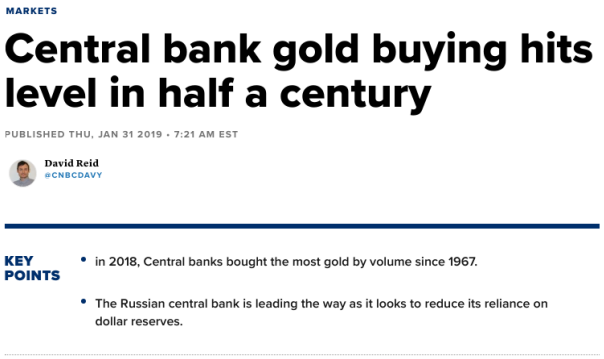


Foreign central banks' holdings of US Treasuries down precipitously (source).

US sovereign debt doesn't even have a yield advantage anymore even though treasury yields are nominally positive. It turns out that once foreign investors hedge for currency risk, US bond yields go

even more negative than their European counterparts mentioned early in the article.

Foreign central banks may not be buying our treasuries, but they're sure buying gold. Why would they be doing that? Gold's a barbarous relic, just shiny metal.

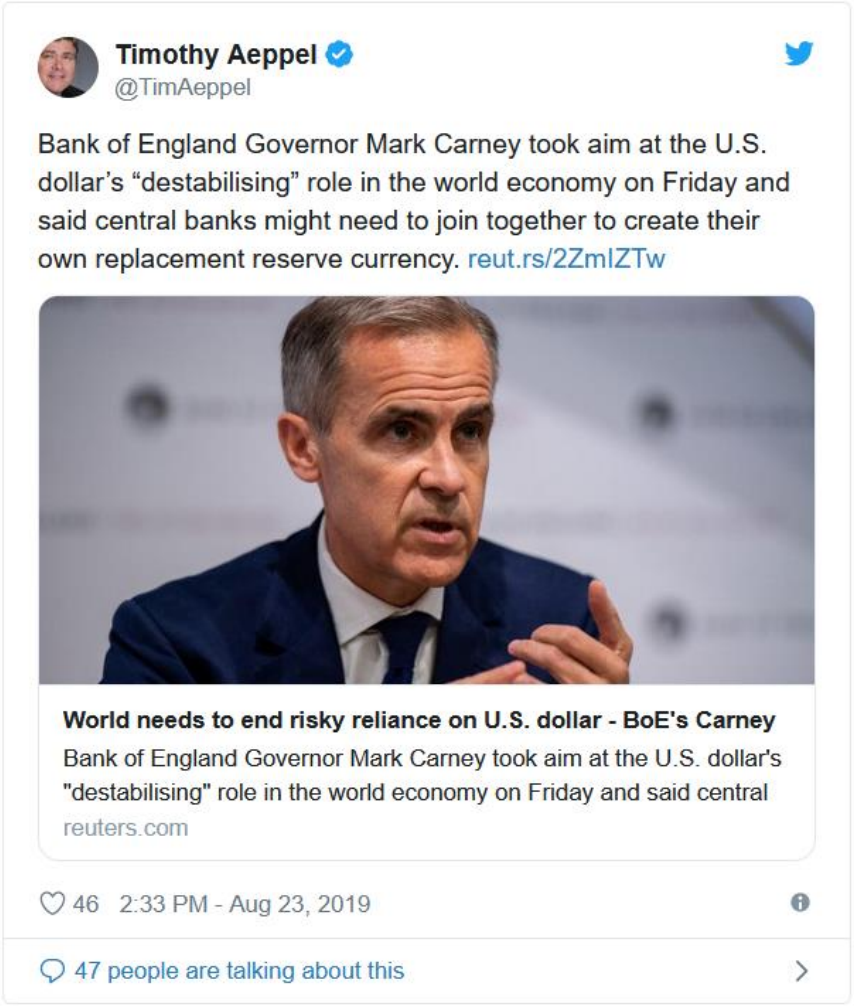


Source

The writing's on the wall. The rest of the world is getting tired of funding another country's obviously-unsustainable programs like social security and medicare while simultaneously being vulnerable to

dollar-based sanctions. Budget deficits continue to grow at record levels ($234 billion for the month of Feb 2019 and we're on track to hit a record $1 trillion for the year). Trump's unhinged Twitter indulgences are a nice foreground to the mind-numbing 222 trillion dollars of on- and off-balance sheet debt the US has set itself up for. Even if the USD is a convenient tool for most countries now, the numbers are unworkable: the US is at some point going to have no choice but to print its way out of a massive debt.

The coming years will continue to see lackluster Treasury demand, hoarding of gold by central banks, and more calls to replace the dollar with digital currency.



Politically-favored economists like Bernie Sanders' Stephanie Kelton will continue to shift the Overton window towards Modern Monetary Theory as an expedient way for politicians to completely disregard deficits and breadwin for their constituents. MMT has an inescapable gravity because it's politically palatable on both ends: politicians love spending money without having to tax, and constituents love free stuff. You will continue to see MMT in the form of a Green New Deal or some kind of Republican-friendly equivalent, probably relating to infrastructure, and deficits will launch into the stratosphere.

Our ability to get funding from the rest of the world will wane concordantly, and some combination of the Fed, the Treasury, and more loose fiscal policy will coalesce to manufacture remarkable amounts of new money. The resulting inflation will be historic.

This is what Bitcoin is for. Bitcoin is an accessible insurance policy against this increasingly likely dollar endgame for anyone who wants it.

Yes, central banks are buying gold and will likely continue to do so. Maybe some even have the intent of reforming the monetary system to sit on top of some kind of gold standard 2.0. Rumors circulate that China is working on a gold-backed cryptocurrency.

The reality is that we can never credibly return to a gold standard. Repatriating gold to do final settlement is incredibly costly and error prone. Even setting aside practical difficulties, gold (or anything gold-backed, whether it's digital or not) will always come with counterparty risk. When Nixon ended the redeemability of dollars for gold in 1971, the die was cast. You can only stain that shirt once. Is China any less likely than 1970s US to suspend gold convertibility when the going gets tough?

Bitcoin is fully digital bearer asset and as such it has no counterparty risk. Final settlement occurs indisputably within hours, not weeks. The cost of storing it is negligible. Cryptographic features like multisignature schemes and scripting abilities like timelocks enable a trustless programmability that makes it a completely new kind of financial asset, which is basically just a bonus on top of its killer feature: **hardness as a money and suitability as a safe-haven asset.**

It only gets crazier from here

I'm not sure that Bitcoin will work in the way that I think it will. Nobody is. But I *am* sure that if the narrative I spell out above is anywhere near right, the financial system in its current form is in for an abrupt change in the next few years. I *am* sure that there's no coming back from the government largesse that materialized in 2008, both in terms of the reliance on credit it introduced and the precedent for significant intervention that it set.

The kind of central bank interventions we've seen in the past 11 years are without equal. Regardless of political affiliation, most people who've been watching finance acknowledge we're in uncharted territory. The average life of a fiat currency is 27 years, and since going off the gold standard (which I'm not necessarily defending), the US government has been allowed to engage in an inflationary frenzy that has no sign of slowing down.

Bitcoin is designed, intentionally or incidentally, as a near ideal tool to have access to when this level of turmoil hits global markets, when governments start to engage in never-before-seen monetary experimentation, when Treasury departments and other political institutions start to lose their credibility. Trustless settlement makes Bitcoin the ideal "currency of enemies" and censorship resistance means unconditional liquidity.

This doesn't mean that Bitcoin will actualize on its potential in whatever next crisis lies ahead of us, but it would seem foolish not to have a small amount of your portfolio betting that it will, whether you're a pension desperate for yield or a millennial like me, disenchanted with almost every other option.

Follow me @jamesob.

Shouts to Luke Gromen, Ben Hunt at Epsilon Theory, Danielle DiMartino Booth, Raoul Pal, Jeff Snider and Erik Townsend at MacroVoices for getting the word out on this stuff.

Resources

- Is a US recession coming? by Raoul Pal
- Luke Gromen on MacroVoices talking about the dollar end game
- Dave Collum's 2018 Year In Review
- The Bullish Case for Bitcoin by Vijay Boyapati

Thanks

Thanks to William O'Beirne, Luke McGrath, Jeff Vandrew Jr, and Neil Woodfine for reading an early version of this article and providing feedback.

Footnotes

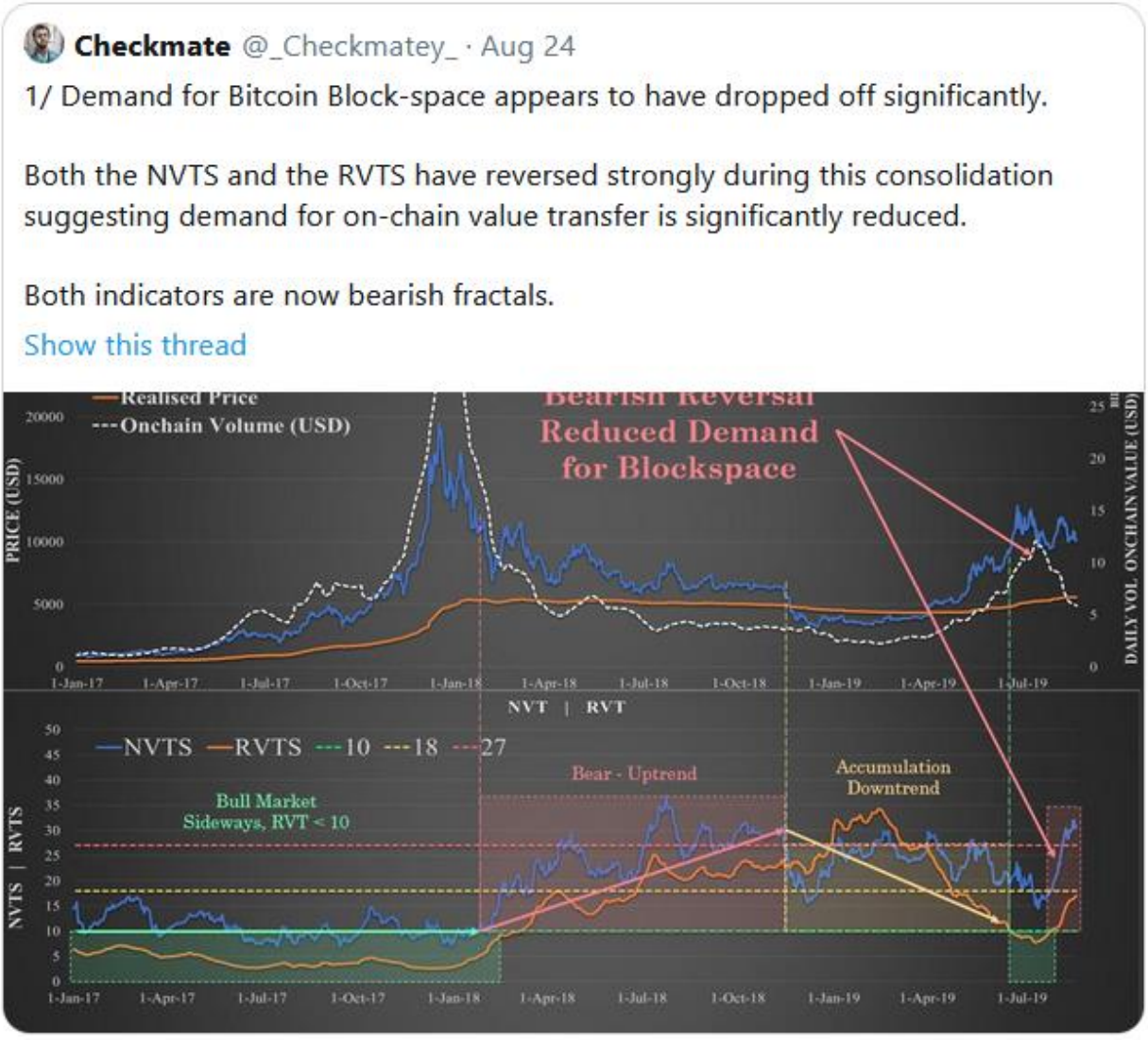
1. Why didn't all this money result in rampant inflation? Because the Fed started paying interest on excess reserves (IOER), depository institutions hold a lot of this new money in reserves at the Fed and get paid an unnaturally high interest rate to do so. *Note:* readers have pointed out that my explanation here probably isn't correct. We didn't see rampant inflation likely because banks cannot use reserves to lend. See here - thanks to David B. ⮌
2. This should be immediately and obviously sisyphean but hey nobody's perfect. ⮌
3. American public pension funds are underfunded by anywhere from $2T-$8T depending on who you ask. ⮌

Tweetstorm: HODLer Index & HODLer Network

By Hans Hauge

Posted August 24, 2019

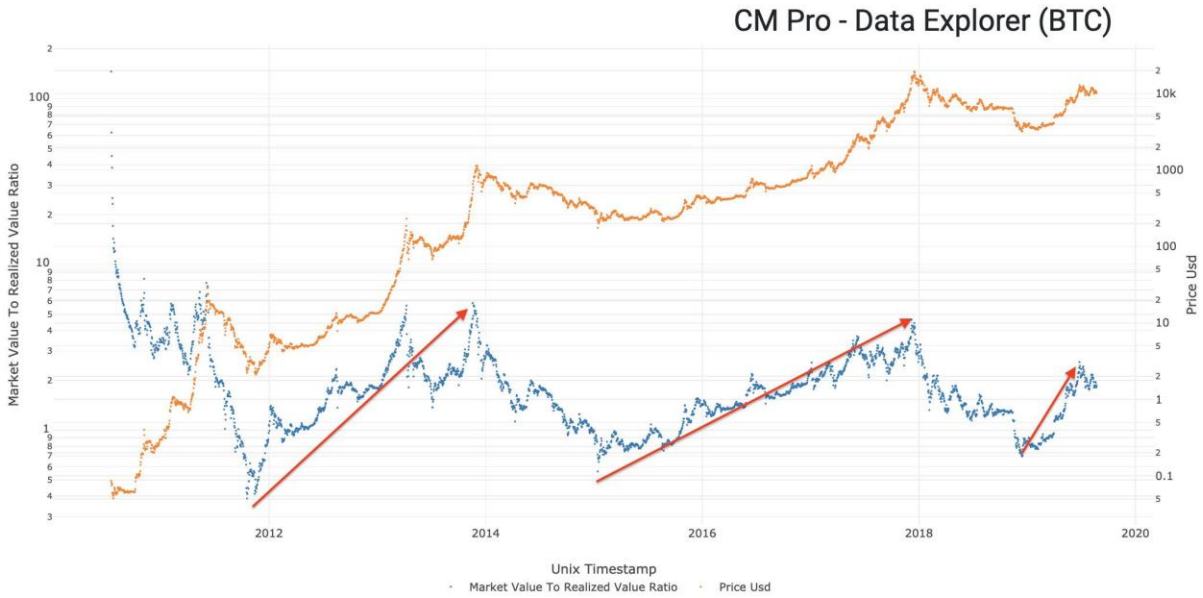
Today I'm introducing two new on-chain metrics and responding to this thread by @*Checkmatey*. On some points we agree, but I'm very bullish right now and I want to explain why using the blockchain.



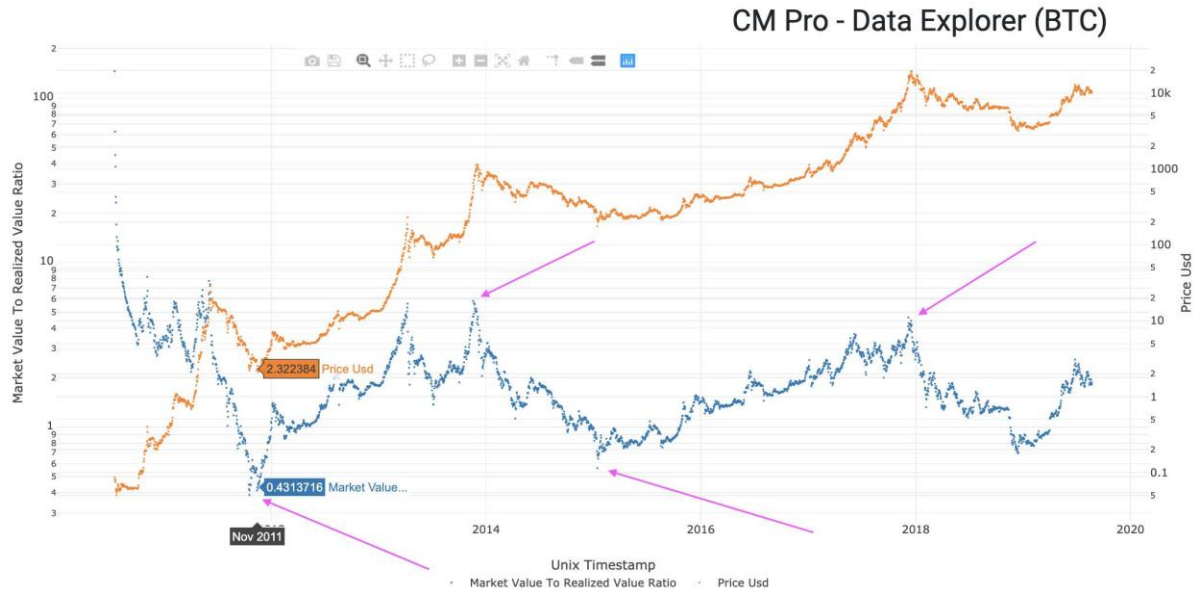
First, I agree with this "Likely this was driven by leverage, deep pockets and speculation rather than HODLERs." As whale HODLers move coins to cold storage they reducing the supply (bullish long-term) but this also means they're not the ones driving short-term price action.

I also agree that MVRV is elevated, but if we look at the MVRV ratio over time there are two important things I notice.

1. Cycle times are usually a couple years from a MVRV bottom to a top. We've only had a few months since the last bottom.

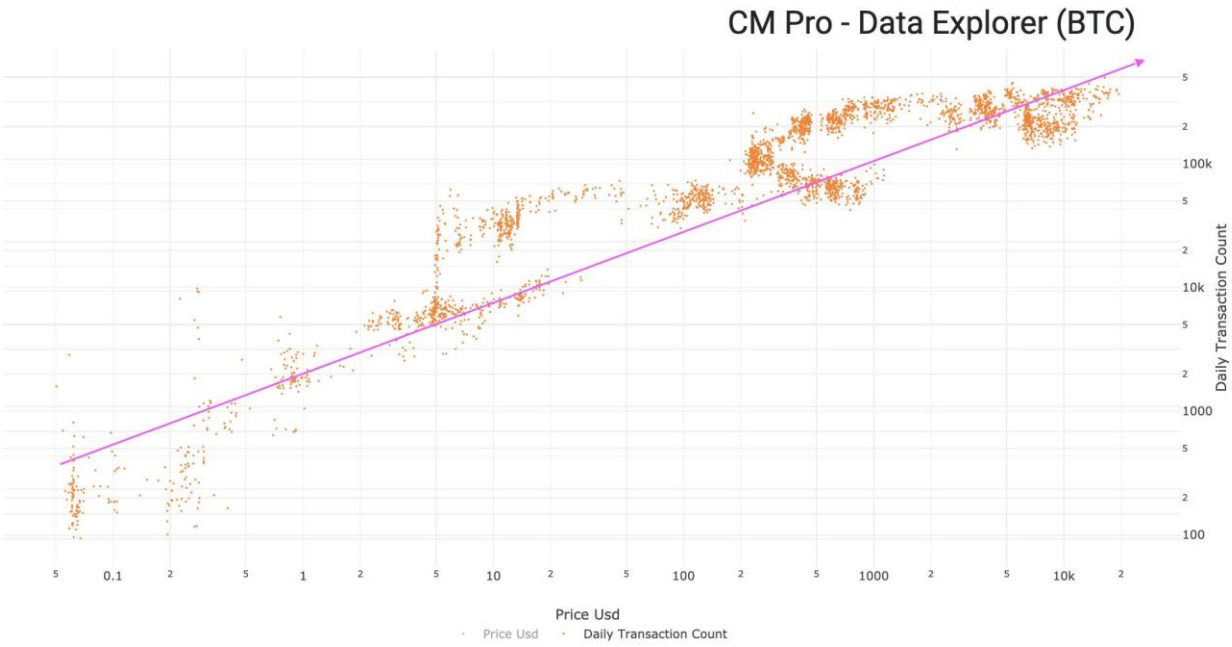


1. Also in terms of the actual MVRV ratio at the bottom versus the top, we've seen bottoms of 0.4 and 0.6 and tops around 4 and 5. Translation, unless things are radically different this cycle we are still very early in the cycle.



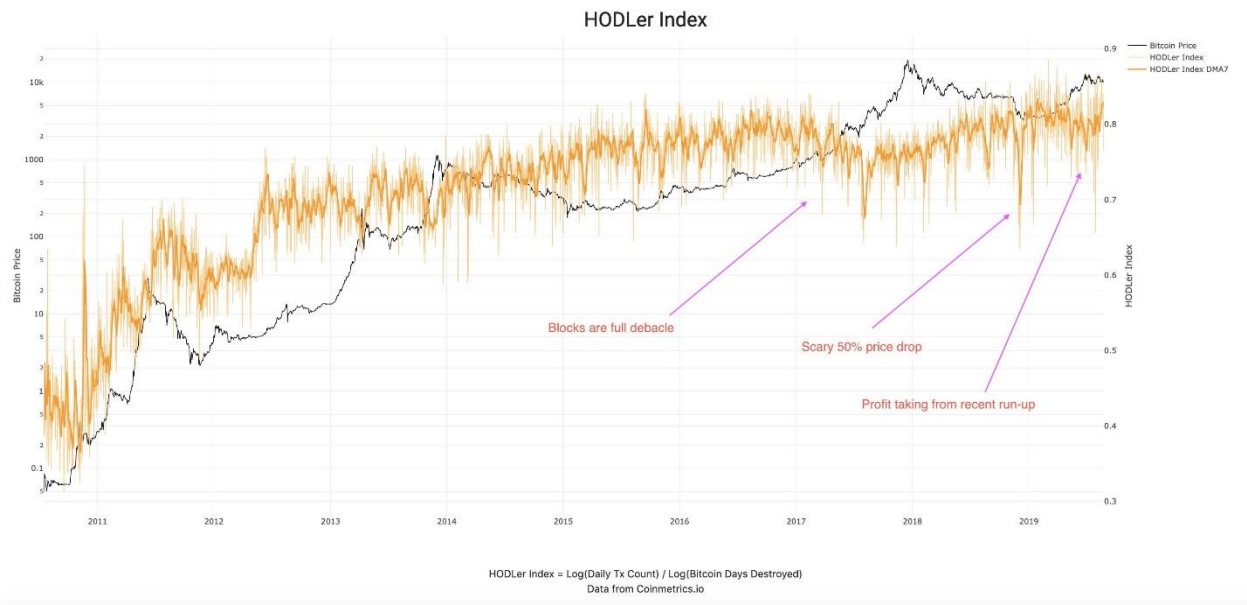
Remember that the price of Bitcoin has pulled back from a recent top close to $14k, wicking all the way down to the $9k region. This is a significant correction. Now, let's talk the decline in USD transaction value.

Let me explain how I think about transactions. A transaction is a "mote of activity" that gives us evidence of Bitcoin adoption. In general more transactions is a good thing. This relationship is easy to visualize with transactions on the y-axis, price on the x-axis.

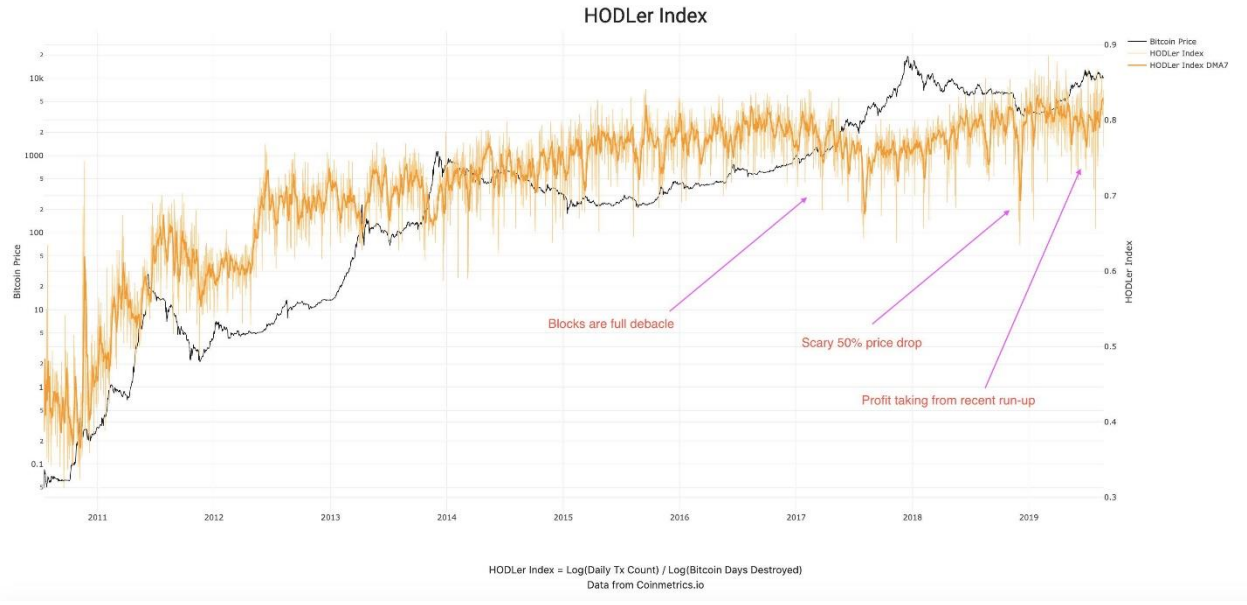


But, we also know that if a lot of Bitcoin Days are being destroyed then that means HODLers are cashing in. When this happens, HODLers move old coins from their cold storage to an exchange to sell it, which creates a transaction. So, highly destructive transactions are bearish.

This leads me to the first new metric that I'm introducing today, the **HODLer Index**. The HODLer Index is a ratio of Transactions to Bitcoin Days Destroyed. How to interpret this?



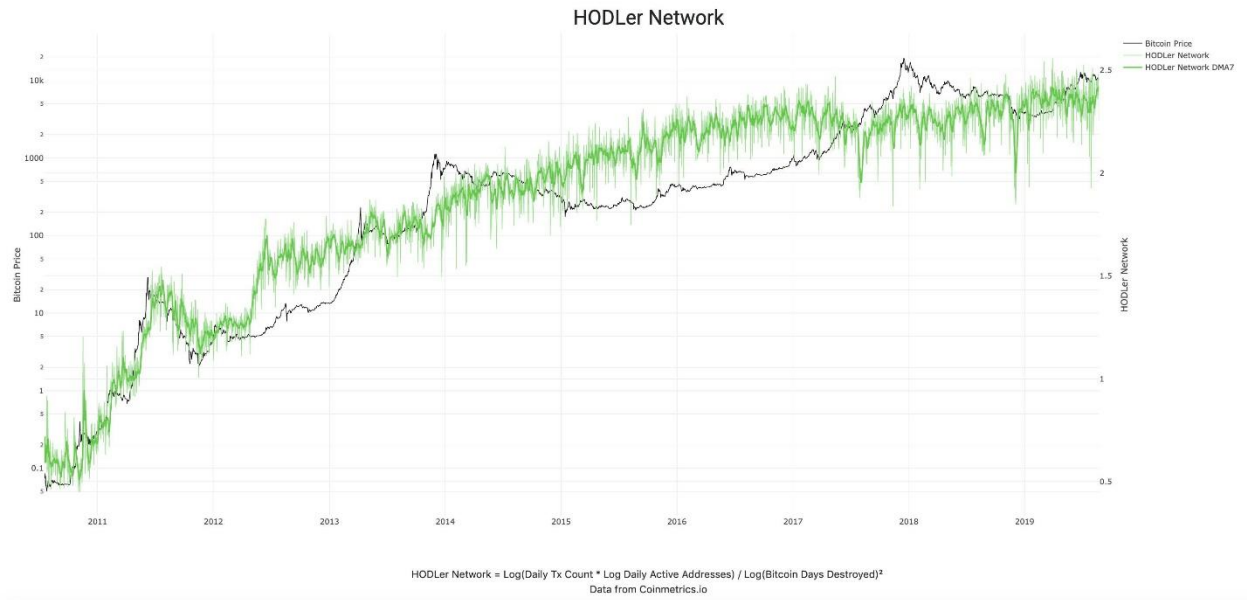
In the image below you can see how recent events affected the behavior of the network. Blocks filled up, less transactions were sent. Price dropped by 50%, people got scared. Price went up, people took profits. But what's been going on the last few weeks?



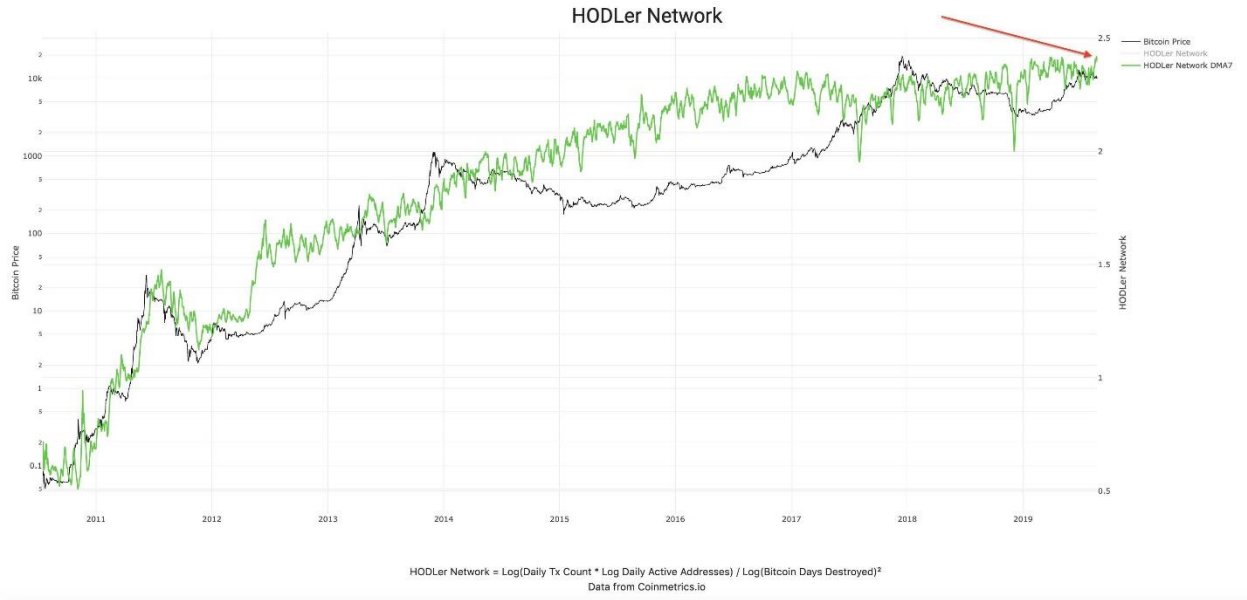
What I'm seeing is a change of direction at the very end of that orange line. HODLy transactions are increasing, meaning that the daily transaction count is increasing and Bitcoin Days Destroyed is falling.

Now let me introduce you to a special bonus (apologies to @nlw as this is turning into long reads Saturday). This is the **HODLer Network**, a slightly more

sophisticated version of the HODLer Index, which also includes the number of unique addresses into the equation.



Just a couple days ago this metric made a new all-time high in the 7DMA. This is a very bullish sign to me as it shows that more people are HODLing more than ever. As @APompliano would say, “the virus is spreading.”



Applying Carl Menger to the Monetization of Bitcoin

By Rollo McFloogle

Posted August 25, 2019

Introduction

Bitcoin promoters have been using the "digital gold" meme to illustrate its function as a store of value on its journey to full monetization. Being a store of value is one of the three generally accepted functions of money; the others are medium of exchange and unit of account. A money, the third thing used for indirect exchange, fully achieves each of these functions at correspondingly named stages with the addition of one at the beginning. These stages of monetization are collectible, store of value, medium of exchange, and unit of account.

It can be somewhat confusing, but these stages do not happen discretely but instead interact with and provide feedback for each other in a complicated monetization process.

For example, while Bitcoin will not be used widely as a unit of account until is reaches monetization, that will not stop some businesses from listing their products for sale only in Bitcoin (for both payment and denomination of price) even during the very early stages of Bitcoin. In this case, before Bitcoin is a reliable store of value, it is being used both as a medium of exchange and unit of account, but only for the isolated occasions when this business owner and his customers interact. It is only when each of these functions are universally adopted (by a society whether it is an isolated village in a jungle or the entire global economy) that we can say that an asset can be called money.

As shown in Murad Mahmudov's famous Market Cap vs Lindy Effect chart, there is still a general linear flow of progression through these four stages of

monetization despite the tendencies of the stages to overlap. Bitcoin is clearly past its stage as a collectible for cypherpunks and libertarians. It is widely known by almost everyone and is regularly discussed on various news programs. With Bitcoiners routinely promoting the idea of "hodling," it must be the case that it is in the stage of becoming a store of value. Despite its sometimes huge peaks and valleys, we can see the price of Bitcoin denominated in fiat over a long time horizon appreciating in price, so it must be the case that it is doing a good job of storing value despite the fact that more bitcoins are being emitted into the network through the mining process. Because of its superior properties that make it very useful as serving the three functions of money, the hodlers are speculating that the price today is well below (even in orders of magnitude) its future price when the rest of society comes to congregate to use Bitcoin as money.

If the hodlers are correct, they stand to be economically rewarded very well. If they are missing something and are unaware of some fatal flaw that makes Bitcoin fail in its mission to become money, then they will lose their investment.

Carl Menger's Store of Value as an Accidental Nature

While many Bitcoiners use Austrian economics to justify their bullishness on Bitcoin, some are pointing to Carl Menger's writing on money to show a blind spot for Bitcoiners. In his book, *Principles of Economics*, Menger writes:

[I]t appears to me to be just as certain that the functions of being a "measure of value" and a "store of value" must not be attributed to money as such, since these functions are of a merely accidental nature and are not an essential part of the concept of money.

At first glance, it appears that Menger contradicts the Mahmudov's and every other Bitcoiner's argument that Bitcoin must generally be used as a store of value before becoming a medium of exchange. However, this quote from Menger and the arguments of Bitcoiners need context and further exploration.

Money is the Best Medium of Exchange Available

The first point to be made is that Menger is speaking very generally. Since money removes us from the barter system of coincidence of wants and direct exchange to a system of indirect exchange, if an asset cannot function as a medium of exchange, *i.e.* the third thing with high saleability and liquidity, then it would obviously never have the chance of being money. But this is a very basic filter for what qualifies something to have the *potential to be* money but not why one asset would beat out others to claim that role.

Interestingly enough, Menger provides some insight into this just a few sentences before the above quote:

If we summarize what has been said, we come to the conclusion that the commodity that has become money is also the commodity in which valuations answering the practical purposes of economizing men and in which accumulations of funds for exchange purposes can most appropriately be made provided that no impediments founded upon its properties stand in the way.

He further elucidates this point in *On the Origins of Money*:

With the extension of traffic in space and with the expansion over ever longer intervals of time of prevision for satisfying material needs, each individual would learn, from his own economic interests, to take good heed that he bartered his less saleable goods for those special commodities which displayed, beside the attraction of being highly saleable in the particular locality, a wide range of saleableness both in time and place. These wares would be qualified by their costliness, easy transportability, and fitness for preservation (in connection with the circumstance of their corresponding to a steady and widely distributed demand), to ensure to the possessor the power, not only "here" and "now" but as nearly as possible unlimited in space and time generally, over all other market-goods at economic prices.

This means that only the assets with the best monetary properties available would become money since people would look to exchange their goods and services for the asset that they believe would provide the highest saleability. This also helps to explain why what is used as money changes over time as technological advancements helped largely by the benefits of the existing money lead to the developments of even better moneys. Menger explains this using the example of how a cattle monetary standard was eventually replaced:

But rising civilization, and above all the division of labor and its natural consequence, the gradual formation of cities inhabited by a population devoted primarily to industry, must everywhere have had the result of simultaneously diminishing the marketability of cattle and increasing the marketability of many other commodities, especially the metals then in use. The artisan who began to trade with the farmer was seldom in a position to accept cattle as money; for a city dweller, the temporary possession of cattle necessarily involved, not only discomforts, but also considerable economic sacrifices; and the keeping and feeding of cattle imposed no significant economic sacrifice upon the farmer only as long as he had unlimited pasture and was accustomed to keep his cattle in an open field. With the progress of civilization, therefore, cattle lost to a great extent the broad range of marketability they had previously had with respect to the number of persons

to whom, and with respect to the time period within which, they could be sold economically. At the same time, they receded more and more into the background relative to other goods with respect to the spatial and quantitative limits of their marketability. They ceased to be the most saleable of commodities, the economic *form of money, and finally ceased to be money at all.*

Clearly, the metals like copper and eventually gold and silver that replaced cattle as money were not immediately used as money or even media of exchange upon their discovery but had to undergo some sort of process by which people began to use them as such. It is laughable to think that the first person to pull a gold nugget out of the ground would say, "I'm going to use this to buy something from my neighbor!" People first used it for its collectability and enjoyed its ornamental functions and then industrial uses. However, its physical features such as durability, divisibility, and scarcity are what led to its monetization.

Bitcoin as a Medium of Exchange

Enter Bitcoin. What's especially interesting about Bitcoin is that it provides digital scarcity and is thus not a physical commodity and therefore cannot be used in economic consumption. It was designed to become money but given its lack of a physical nature to be used for anything but money, *it must only serve as a medium of exchange* . You cannot eat it, you cannot build physical things with it, you cannot use it in electronics, etc. The only thing you can do is sign transactions to transfer the ownership of your bitcoins to someone else. It matters not if it is somewhat expensive to transfer that ownership; the magnitude of the transaction fee does not negate its primary function as a medium of exchange.

Because someone doesn't immediately sell their gold or dollars upon receipt doesn't render those currencies useless as media of exchange. We simply call the act of delaying of spending saving. Likewise, the "accidental nature" of the store of value function of Bitcoin comes when owners decide to delay spending them. The reason for the saving is that the owner speculates that in the future more people will demand Bitcoin as a medium of exchange for payment. With this and the ever-inflating fiat system in mind, it would be destructive to the Bitcoiner's wealth to spend his bitcoins instead of his fiat. Any rational economic actor would save the thing he expects to be worth more in the future and spend the thing that will be worth less tomorrow than it is worth today. This is Thiers' law in action.

Bitcoin has not reached it's *stage* of medium of exchange yet because it is not universally used that way. Only a small fraction of the world's population own

Bitcoin at this present moment. The key nuance in understanding Menger is understanding the difference between medium of exchange as a function and medium of exchange as a stage in monetization.

Applying Menger to Gold

As few months before Satoshi Nakamoto mined the first Bitcoin block, Robert Blumen wrote a piece on Mises.org called "Is Gold Money?" He took on the above Menger quote regarding store of value as an "accidental nature" to address the reasons why gold, despite its demonetization through government forces, did not lose its store of value function despite many experts claiming it would. Although Blumen was not considering Bitcoin, you can easily insert it into his analysis, which makes Bitcoin an even more bullish proposition.

Blumen writes:

But why is gold a better store of value than most any of a vast number other nonmonetary goods? Why were Milton Friedman and the other economists wrong? Their error was the assumption that political institutions have the final say over what is and is not money. But this is not so: the market has final say. Looking at the process by which money originated from barter helps to understand why. According to Menger, money came into being through the efforts of individuals to expand the range of goods they could acquire through exchange beyond the possibilities available. [7] Some individuals in a barter economy begin by bartering their goods for a commodity that they do not need but is generally in demand throughout the market, with the intention of later exchanging that commodity for other goods. This strategy is called indirect exchange. These astute traders realize that "the acquisition by trade of the consumption goods that he needs … can proceed … much more quickly, more economically, and with a greatly enhanced probability of success." [8]

He later continues:

The result of market competition is not necessarily permanent. Market competition is an ongoing process. Even when one commodity emerged as money, there continued to be competition from other nonmonetary commodities. Once the world's money, even gold could have lost its place had a superior alternative emerged. But that is not the reason we no longer use it. Political money did not prove its superiority through a market process. What happened instead was a politically imposed change from a better system to a worse system.

Although the central bankers have used political means to replace gold with paper, they do not have the power to end the competition between their

money and commodity money. The "demonetization" of gold by central banks has rigged the competition — but not ended it.

The reason that gold is no longer used as money is not because of its inferior qualities to the government's fiat. Instead, it was gold's inability to provide security against the political means of control. In other words, as Blumen says, it was not a market process but a political process that caused the transition from gold to fiat. Those political forces, however, only elbowed gold offstage; however, the market forces (*i.e.* people trying to retain their wealth) keep it poised to remonetize as soon as the government's fiat system collapses under its own weight.

But gold's same flaws would still exist and while better technology today would stave off the centralization for perhaps a longer time than before, no technology exists for gold that would allow it to be inoculated from the clutches of government centralization. Bitcoin, however, with its superior monetary qualities over gold and fiat, has the ability to not only crush the fiat system but also deal the final death blow to gold's monetary standing. Gold losing its monetary value through competition is a good thing, because, as Blumen wrote above, it would mean that "a superior alternative emerged."

Final Thoughts

We have the privilege to live in a time when a new market-driven monetary standard is emerging for the first time in thousands of years. It's happening in sync with the way long-dead economists explained an asset monetizes. As Bitcoin proves these economists correct and *vice versa*, we have a positive feedback loop of assurances that both our Austrian economic principles and our speculation that Bitcoin will become global money are correct.

Disclaimer:

WORDS

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

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

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

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

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

DYOR | BTFD | HODL

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

- @_joerodgers