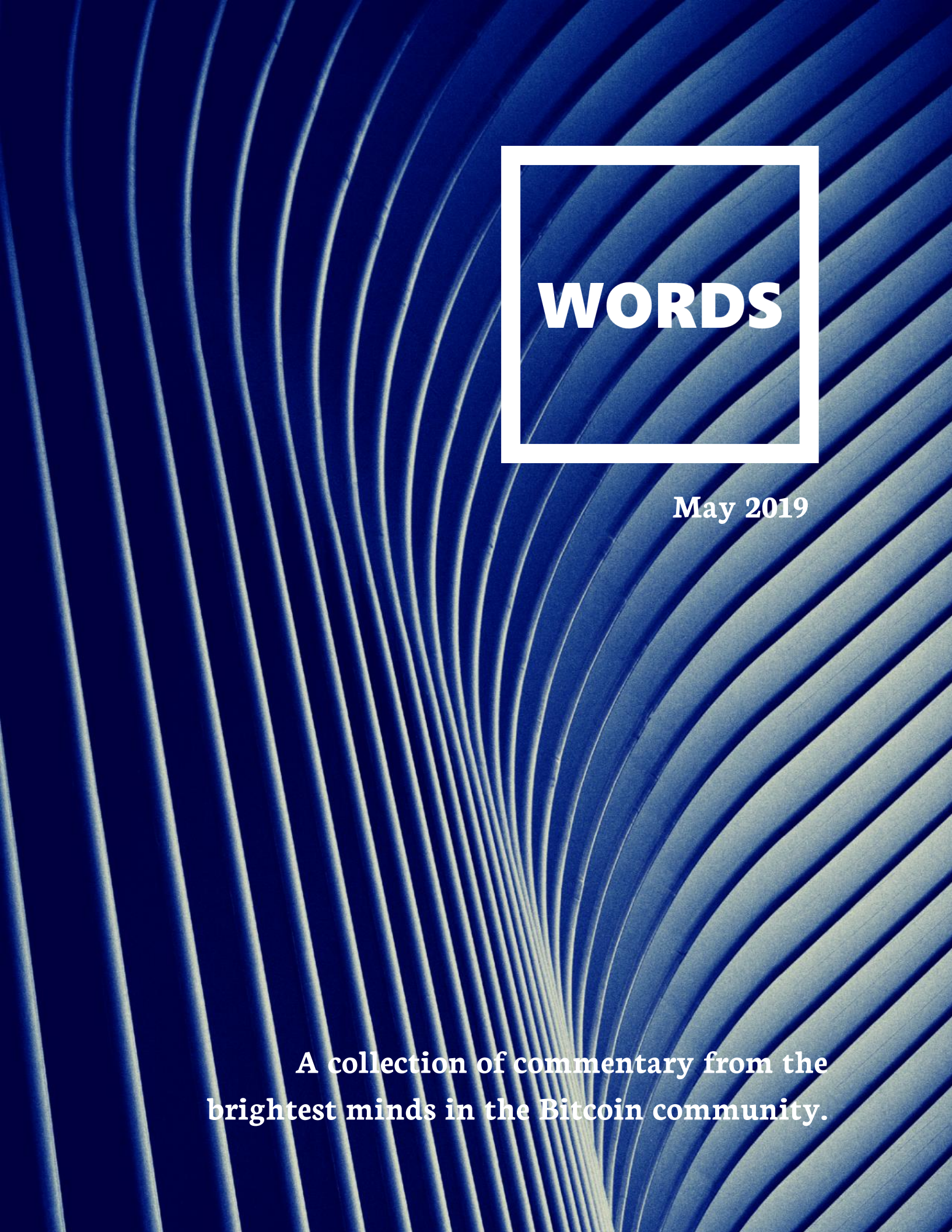


May 2019

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

Contents

Goals and Scope

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

History

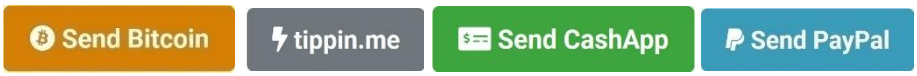
There exists a gap in Bitcoin publishing. For authors with commentary and scholarly papers on topic, the choice of publication outlets is relatively limited. The number of journals that serve as outlets for Bitcoin research is in any event too small, as the number of Bitcoin thinkers continues to grow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

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

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

Support WORDS

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



Spread the word

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

Follow us on social media

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

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

Subscribe to our newsletter

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

Our pledge

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

Updates to this journal

9-25-2019:

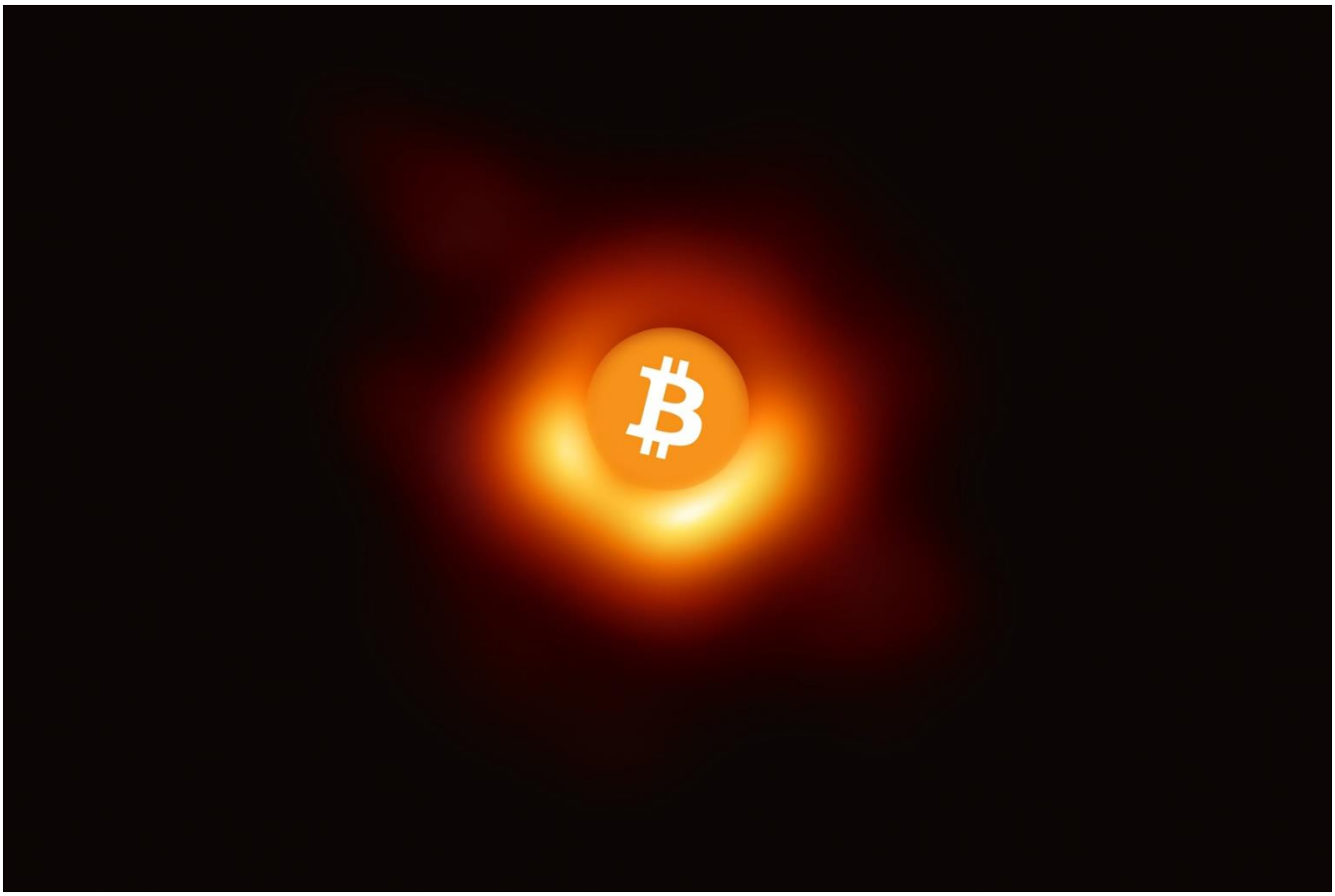
- Understanding (and Mitigated) Re-Orgs
- Decentralizing Bitcoin's Last Mile with Mobile Mesh Networks

Bitcoin's Gravity

How idea-value feedback loops are pulling people in

By Gigi

Posted May 1, 2019



Bitcoin is different things to different people. Whatever it might be to you, it is undoubtedly an opinionated and polarizing phenomenon. There are certain ideas embedded in the essence of Bitcoin, and you might be intrigued by some or all of them.

The invention of Bitcoin, and its underlying blockchain, which is so widely misunderstood, spawned many projects, networks, and communities. Some of these networks are in direct competition, which has resulted in endless conflicts and lots of debate. The root of these conflicts is ideological in nature: disagreement about how the world is and how it should be—a disagreement about ideas.

The following is an attempt to explain some of the reasons behind this polarization, explore the underlying dynamics in more detail, and illustrate why an increasing number of people seem to be gravitating towards Bitcoin.

"There are some oddities in the perspective with which we see the world. The fact that we live at the bottom of a deep gravity well, on the surface of a gas covered planet going around a nuclear fireball 90 million miles away and think this to be normal is obviously some indication of how skewed our perspective tends to be, but we have done various things over intellectual history to slowly correct some of our misapprehensions."*Douglas Adams*

Agreeing on a Set of Ideas

The goal of the Bitcoin network is to reach *consensus*, a general agreement on the state of the system. Bitcoin's breakthrough innovation was utilizing unforgeable costliness to reach global consensus without relying on a central authority.

Bitcoin can be understood as a game that anyone can join. Like all games, it can only be played if it has rules, certain ideas which are internally consistent. Otherwise, it wouldn't be a game; it would be chaos.

"Before any game can be played, the rules have to be established; before the game can be altered, the rules have to be made manifest. [...] All those who know the rules, and accept them, can play the game—without fighting over the rules of the game. This makes for peace, stability, and potential prosperity—a good game. The good, however, is the enemy of the better; a more compelling game might always exist."*Maps of Meaning* Bitcoin's consensus rules are just that: a set of ideas, codified into validation rules, acted out by nodes on the network. Changing this core set of ideas is akin to changing what Bitcoin is, and the decentralized nature of the network makes changing them extremely difficult. There is no central authority to dictate changes, making unanimous adoption of a new set of ideas virtually impossible. Anyone who changes the rules, even if he thinks such a change is for the better, will start to play a different game, with only those who join him.

As Bitcoin's creator famously said: the nature of Bitcoin is such that once the first version was released, the core design was set in stone for the rest of its lifetime.

Undoubtedly, Satoshi had certain ideas in mind when he created Bitcoin. Many of these ideas are articulated in his writing, and even in the genesis block. Most importantly, however, his core ideas are codified in Bitcoin's consensus rules:

- fixed supply
- no central point of failure
- no possibility of confiscation or censorship
- everything can be validated by everyone at all times

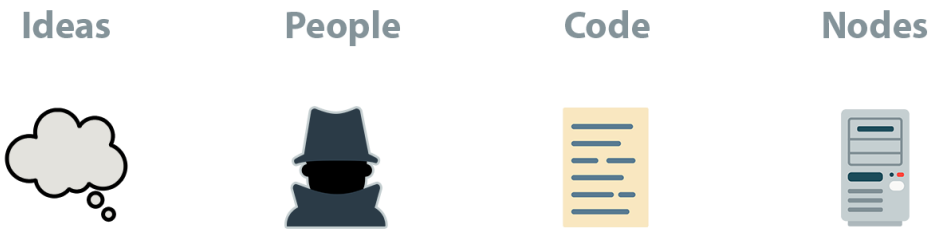
This set of ideas is embedded in the rules of the network, and you have to adopt them to participate. In essence, a network like Bitcoin encodes a social contract in its software: ideas which are shared by everyone on the network.

Spreading ideas

All great things start small, and Bitcoin was no exception. In the beginning, it was one node, one piece of software, one person, one set of ideas. On 31 October 2008, the Bitcoin whitepaper was published. Two months later, on 3 January 2009, the genesis block was mined.

"The Times 03/Jan/2009 Chancellor on brink of second bailout for banks."*Bitcoin's Genesis Block* It took only two days until a second person was intrigued enough to join the network. Hal Finney ran the software, connected to Satoshi's node, and the Bitcoin network was born. Soon, other people picked up on the idea, ran the software, and set up their nodes to join the network. The rest, as they say, is history.

The Bitcoin network is a complex piece of machinery. The constituents of the network—part technology, part biology—make it inherently difficult to describe and understand. While the following doesn't claim to be a complete description of the system by any means, I think it's helpful to focus on some constituents in more detail. In particular, I want to focus on the following four: **ideas**, **people**, **code**, and **nodes**.



Bitcoin's ingredients: two parts software, two parts hardware.

On the physical layer, the network is made up of interconnecting *nodes*. Bitcoin's consensus rules are embodied in its software, i.e. the *code* which is

running on its nodes. Ultimately, *people* are choosing which software to run, a decision which is shaped by the set of *ideas* they hold.

The possibility of running self-sovereign nodes is part of the reason why Bitcoin's consensus rules are so hard to change. As mentioned above, there is no central authority, no entity to trust. Changes have to be adopted voluntarily by everyone. People are free to run any version of the software, be it out of conviction, laziness, or contempt.

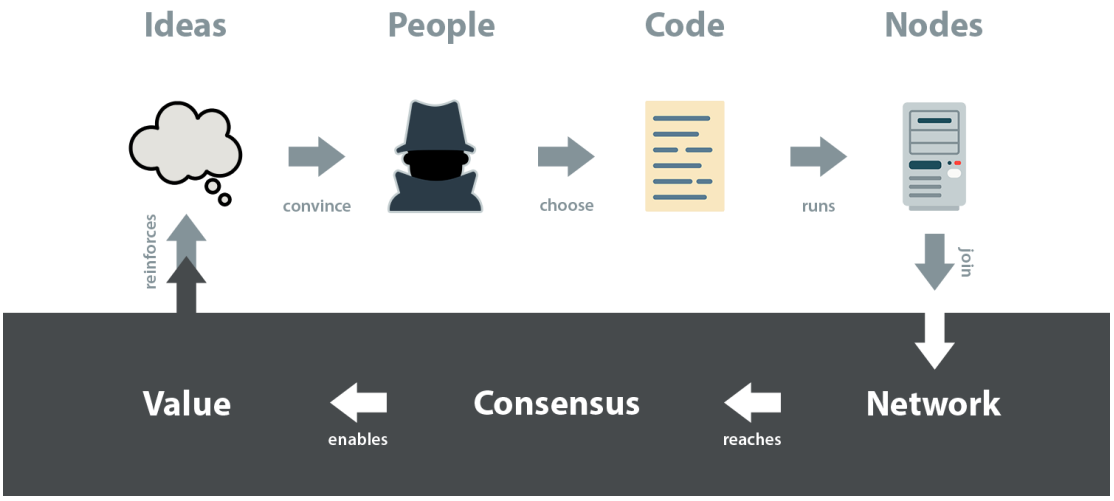
Bitcoin is a system "based on cryptographic proof instead of trust," to quote the whitepaper. The implication is that *you* are the authority and *you* have to verify everything for yourself from scratch. Out of this, consensus emerges.

"Freedom brings men rudely and directly face to face with their own personal responsibility for their own free actions."*Frank Meyer, In Defense of Freedom* As soon as consensus is reached on the network, *value* comes into play. That bitcoins—or any monies, for that matter—have value, is in itself an idea that people need to be convinced of.

For Bitcoin, this process took almost 500 days. When the network was in its infancy, bitcoins weren't worth anything. They were mined and sent back and forth between curious cypherpunks. However, the moment Laszlo exchanged 10,000 BTC for two pizzas, Bitcoin went from zero to one. In an instant, the network became valuable in a tangible way.

Ever since this moment, the following *idea-value feedback loop* is at play:

- Bitcoin's set of **ideas**—its value proposition—is attracting people.
- Those **people** freely choose which code to run.
- The selected code runs on individual **nodes**, dictating their behavior.
- Nodes join the **network**, connecting to peers who share their ideas.
- The network reaches **consensus**, enabling agreement on who owns what.
- The **value**, in turn, is based on the set of ideas enforced by consensus rules: the embodiment of its value proposition.



Idea-value feedback loop.

This idea-value feedback loop, the re-enforcement of ideas through value creation, is the mechanism behind Bitcoin's gravity. Everything in this cycle influences everything else—whether it is software, hardware, or wetware. This loop is what ultimately captures people, and since Bitcoin's core set of ideas is virtually fixed, it has some surprising effects on the sets of ideas held by people.

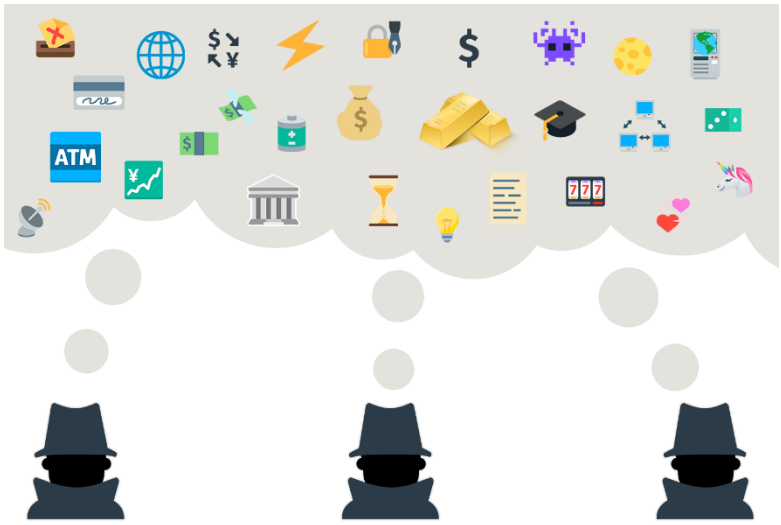
Bitcoin's Gravity Well

As we have seen above, Bitcoin is an opinionated piece of software, creating an opinionated network. The result of an opinionated network is that it attracts opinionated people.

Arguably, most early adopters of Bitcoin shared its core set of ideas. As Dan Held points out in *Planting Bitcoin*, Satoshi carefully chose the initial group of people: cryptographers and cypherpunks, who understood the technical components Bitcoin is made of.

There are many paths which might bring you close to Bitcoin's gravitational pull: you might have an interest in cryptography, information security, or financial technologies. You may hold certain political or economic beliefs. You might be a gold bug, free speech advocate, or a speculator. You may need to use Bitcoin out of necessity. Whatever the reasons for your initial contact with Bitcoin, there is a certain probability that you are pulled in. Satoshi alluded to this multi-dimensional attractiveness in one of his emails to the cryptography mailing list.

"It's very attractive to the libertarian viewpoint if we can explain it properly. I'm better with code than with words though."*Satoshi Nakamoto* One way to illustrate this is by visualizing a landscape of ideas. Since the number of all possible ideas is basically infinite, we will have to focus on a small subset. And since we are talking about Bitcoin, we will focus on the small universe of ideas spawned by asking the question of what Bitcoin is.



What is Bitcoin?

Ask three strangers what Bitcoin is, and you will probably get three very different answers. Any answer is necessarily shaped by past experience, political and economic beliefs, and an individual understanding of the world. Your personal set of ideas, your world view, defines where you are on the landscape of ideas.

The landscape has sets of ideas which clump together: *narratives*, which help to explain what Bitcoin is. One person might think of Bitcoin primarily as digital gold, focusing on the store of value aspect of Bitcoin. Another person might think of Bitcoin as a payment system, focusing on the medium of exchange aspect of Bitcoin. Yet another person might think of Bitcoin as a way to automate more complex social constructs, focusing on automation of contracts and similar ideas.

"Nobody can know everything. The complexity of society is irreducible. We cling to mental models that satisfy our thirst for understanding a given phenomenon, and stick to groups who identify with similar narratives." *Dan Held* These narratives, these sets of ideas, describe both what Bitcoin *actually* is—at least in part—and what people *think* it is. These narratives will necessarily evolve over time as our understanding of the system and the system itself evolves. Neither ideas, nor people, nor Bitcoin, nor the world at large are static things. Our visions of Bitcoin have changed, and will continue to do so in the future.

Whatever Bitcoin is, it acts as a *gravity well* in this universe of ideas. If your set of ideas overlaps with those embodied by Bitcoin, you are close to its gravity

well and captured easily. If your set of ideas is opposed to Bitcoin's, you are far away from its gravitational pull and remain unattracted.

What is Bitcoin?

Consequently, Bitcoin is attracting opinionated people who share certain ideas and ideals. "Birds of a feather flock together," as the saying goes. In this case, many nerd-birds and cypherpunks flocked around Bitcoin early. Not particularly surprising.

What is surprising, however, is the side-effect of an opinionated network: it influences people. Since the set of ideas embodied by Bitcoin is fixed, it is the set of ideas held by *people* which has to align—not vice-versa. The last ten years have shown that Bitcoin is very effective in changing minds. So far, no single mind was particularly effective in changing it.

"So the universe is not quite as you thought it was. You'd better rearrange your beliefs, then. Because you certainly can't rearrange the universe." —Isaac Asimov To repeat an old TFTC trope: Bitcoin will change us more than we will change it, as I have learned myself.

Attraction and Repulsion

But what if your set of ideas does not overlap with Bitcoin's? What if you wish to change Bitcoin's set of ideas, not convinced of the futility of this endeavor? What if you are downright repulsed by some of its ideas?

"The miracle of physics that I'm talking about here is something that was actually known since the time of Einstein's general relativity; that gravity is

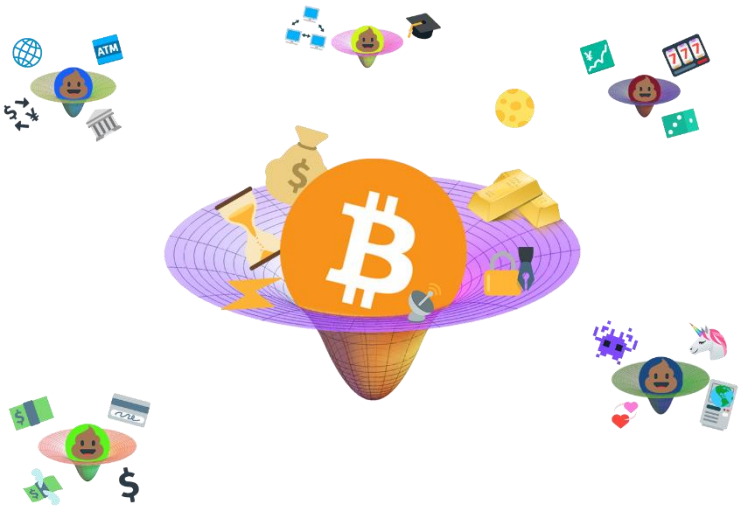
not always attractive. Gravity can act repulsively."*Alan Guth* If you are truly repulsed by Bitcoin's ideas, you might end up drifting away into space, joining the interstellar void where nocoiners float around.

If you want to change Bitcoin's ideas in a fundamental way, you might end up creating another gravity well. This is easily possible because of Bitcoin's openness. Its open source code, permissionless network structure, and lack of formal organization of any kind allows anyone to copy, modify, and run the code without asking for permission.

As outlined above, changing the core rules of Bitcoin results in a new game—different from the game everyone else is playing. To not play alone, you would have to convince other people to play with you. If you want to have the same number of people to play with, you will have to convince *everyone* on the network that your set of ideas is better than the one held by everyone else. And since this is mostly a financial game, strong network effects are very beneficial; it is in your best interest to convince everyone.

Failing to do so will create a competing system; either by creating a new network or by splitting off from the existing Bitcoin network. Since all new projects are inspired by Bitcoin, the set of ideas necessarily overlaps; sometimes almost exactly.

"Tracking narratives is a good way to help people understand that there are, in fact, a menu of beliefs competing for their affiliation; [...] Trying to identify where one narrative ends and another begins is a challenging task, as ideas tend to have permeable borders."*Nathaniel Whittemore* Since creating new gravity wells is (a) possible and (b) relatively easy to do (copy Bitcoin's code, change a few parameters, launch the new network with a couple of friends) there was an explosion of alternative coins in the last few years. While most of these altcoins are outright scams, some try to find a niche, attracting people who share its new or modified set of ideas.



Different ideas are captured by different gravity wells.

Being sucked into one of these gravity wells—and thus into an idea-value

feedback loop—is the reason for much of the toxicity we see in Bitcoin and elsewhere. The direct link between holding beliefs (ideas) and holding assets (value) is a multiplying factor which can result in ever deeper entrenchment.

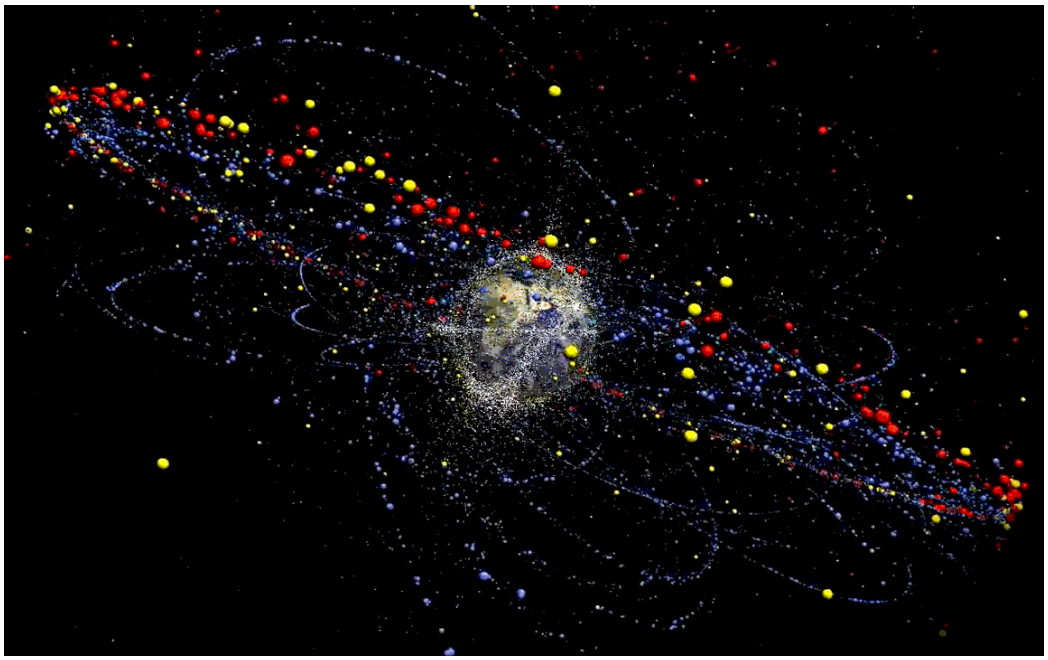
"Everyone knows nowadays that people "have complexes." What is not so well known, though far more important theoretically, is that complexes can have us."*Carl Jung* One could argue, as Carl Jung did in relationship to complexes, that *blockchains have people*. At the root of every gravity well is a set of ideas and a group of people which are had by them.

Once captured, a difference in technicalities can easily become a difference in ideologies—and vice versa. Giving up on ideas is difficult in any case, but if your net worth is intractably linked these ideas it becomes ever more difficult.

Orbits and Collisions

The formation of any gravity well isn't exactly a smooth ride. Just like stellar and planetary formation is violent at times—suns swallowing planets, planets bumping into each other, and moons being smashed to pieces—the formation of Bitcoin's gravity well had some violent events too.

I plan to explore some of these events in the future, but for now, let's just acknowledge that there are other projects orbiting Bitcoin and that there have been collisions in the past.



An artist's impression of Bitcoin and its satellites. Source: KQED Science

Whether all other projects will be swallowed by Bitcoin or die on their own, or whether some will find stable orbits, is yet to be seen. What can be observed today, however, is that most networks are competitive. To quote Eric Hoffer: "the gain of one in adherents is the loss of all the others."

What can also be observed, since it has happened multiple times over the last couple of years, is that projects which fail to deliver on their value proposition are quickly losing most of their adherents and also their value—the former due to disillusion, the latter due to market forces. Value, and speculation on future value, is an integral part of the idea-value feedback loop. If ideas don't materialize or fail, real (and speculative) value is lost, which is effectively killing those ideas and the networks which embody them.

However, as long as people hold different sets of ideas, and as long as a project in Bitcoin's orbit embodies this set of ideas, people will flock to it. Whether those ideas have merit will be decided by time, the open market, and ultimately, reality. Horrible ideas don't work at all, bad ideas not for long, and solutions which aren't substantially better than the status quo won't thrive in a free market.

The best ideas, however, might be discovered by the biggest networks and will be assimilated, if assimilation is possible. If Bitcoin can eat it, it will eat it.

Feeding on Ideas

As mentioned above, Bitcoin's core set of ideas is fixed from day one. However, this doesn't imply that Bitcoin can't be improved. It can and *should* be improved, but it has to be improved in ways that don't destroy the essence of Bitcoin. Such improvements are happening all the time, which is why we can send payments to script hashes, have segregated witness, and can pay small amounts quickly and cheaply on the lightning network.

The technicalities of improving Bitcoin—and the important difference between a soft and a hard fork—are well worth exploring, but are beyond the scope of this article. Without going into more details in regards to the nature of these improvements, Bitcoin undoubtedly *is* improving, and thus its feature set is changing and expanding.

In terms of gravitational pull, this means that Bitcoin is gaining mass. The set of ideas which describes Bitcoin is expanding along with its feature set, potentially capturing more people and swallowing competing projects and ideas in the process.

The idea of cheap payments, for example, has re-emerged thanks to payment channels on the lightning network. While still in its early stages, other projects built on this idea will lose their merit if the lightning network is successful on a large scale.

Privacy is another idea which is at the root of several competing projects. If future privacy enhancements in Bitcoin prove to be successful (Schnorr signatures, lightning, whirlpool, wallets supporting CoinJoins), these projects might be swallowed by Bitcoin as well.

"And the earth opened her mouth, and swallowed them up, and their houses, and all the men that appertained unto Korah, and all their goods. They, and all that appertained to them, went down alive into the pit, and the earth closed upon them: and they perished from among the congregation."*Book of Numbers* I'm not saying that *all* other projects will perish, necessarily. But networks thrive because of network effects: the winner takes most, if not all.

The Value of Conviction

Whenever people are debating ideas, tribalism is the norm, not the exception. Whether it is politics, sports, iPhone vs Android, or pineapple on pizza, people identify with the camp that is closest to their ideas and ideals.

While the validity of ideas are sometimes hard to measure, either because their consequences are very indirect (politics) or subjective and not truly consequential in the grand scheme of things (pineapple on pizza), networks like Bitcoin come with a direct measurement: value.

While this value can be distorted by both manipulation and speculation, it is a reliable and (almost) direct indicator of both conviction and validity of ideas. If more people are convinced by a network's set of ideas, more people will hold its native token as an asset. And the more those ideas align with reality, the more real-world value is generated by the network, convincing more people and deepening the convictions of those already convinced.

Bitcoin has the largest gravity for a reason: it works since day one, solves real problems for real people, generating real value. It works because its set of ideas aligns most closely with reality. It is valuable because people believe in its value proposition, and with good reason: Bitcoin is the largest, most secure, most robust network for permissionless and digital value transfer to date. And it is growing.

Whether you are already convinced by Bitcoin's ideas or are diametrically opposed to them, Bitcoin will continue to not care. Its gravitational pull will

continue to increase, swallowing ideas, people, code, and nodes in the process.

Conclusion

We have seen that Bitcoin embodies a certain set of ideas in its consensus rules and overall architecture. Changing Bitcoin's core set of ideas is virtually impossible, which is why its core design is "set in stone" since day one.

The idea-value feedback loop is what creates Bitcoin's gravity. People coming close to this feedback loop have a certain probability of being captured, which forces them to align their own set of ideas with Bitcoin's or "fork off."

Understanding that any unchanging system will change its participants is helpful in understanding both attraction to and repulsion by Bitcoin. Since changing the core set of ideas is not an option, new projects embodying new sets of ideas are launched, creating new gravity wells in the process.

A different idea-value feedback loop is the basis for each gravity well. Tribalism and loss-aversion help to explain some of the toxicity between competing projects and communities, since falling into any feedback loop will taint the world view of anyone captured by it.

"For one can fall victim to possession if one does not understand betimes why one is possessed. One should ask oneself for once: Why has this idea taken possession of me? What does that mean in regard to myself?"*Carl Jung* Both the world and Bitcoin are dynamic things, making any set of ideas we currently hold insufficient for a permanent, complete view of either. Bitcoin can and does change, even if its essence is virtually unchangeable. No matter our individual beliefs, we must not get too attached to any narrative, or to any set of ideas.

Bitcoin's dominance is no accident. Its set of ideas managed to convince the largest group of people, generating the most value in turn. However, exploring other ideas can be a good and healthy thing, if pursued genuinely. Time and the free market will decide which ideas align with reality. Bad ideas will vanish, and good ideas will be absorbed.

In a world where people hold a combination of ideas and valuable assets, a feedback loop which links and reinforces both is a powerful force of attraction. Whether you just started to feel Bitcoin's gentle pull or you've been a hodlonaut in close orbit, Bitcoin's gravity will continue to increase. I am convinced of that idea, and I hope to have planted a seed of conviction in you as well.

Further Reading

- Unpacking Bitcoin's Social Contract by Hasu
- We can't all be friends: crypto and the psychology of mass movements by Tony Sheng
- Visions of Bitcoin - How major Bitcoin narratives changed over time by Hasu and Nic Carter
- The Many Faces of Bitcoin by Murad Mahmudov and Adam Taché
- Bitcoin: Past and Future by Murad Mahmudov and Adam Taché
- Crypto-incrementalism vs Crypto-anarchy by Tony Sheng
- Bitcoin Culture Wars by Brandon Quittem
- Schrödinger's Securities by Nathaniel Whittemore
- Market Narratives Are Marketing by Nathaniel Whittemore
- Quantum Narratives by Dan Held

Acknowledgments

- Thanks to Hasu, whose incredible feedback helped to shape large parts of this article. His writing on Unpacking Bitcoin's Social Contract was my inspiration for writing about Bitcoin's gravity.
- Thanks to Nathaniel Whittemore for his writings on narratives and feedback on earlier drafts of this article.
- Thanks to Ben Prentice for proofreading the final draft.
- Graphics based on the fxemoji set cc-by Sabrina Smelko
- Dedicated to the bravest space cat of them all (* April 2017, † April 2019).

Translations

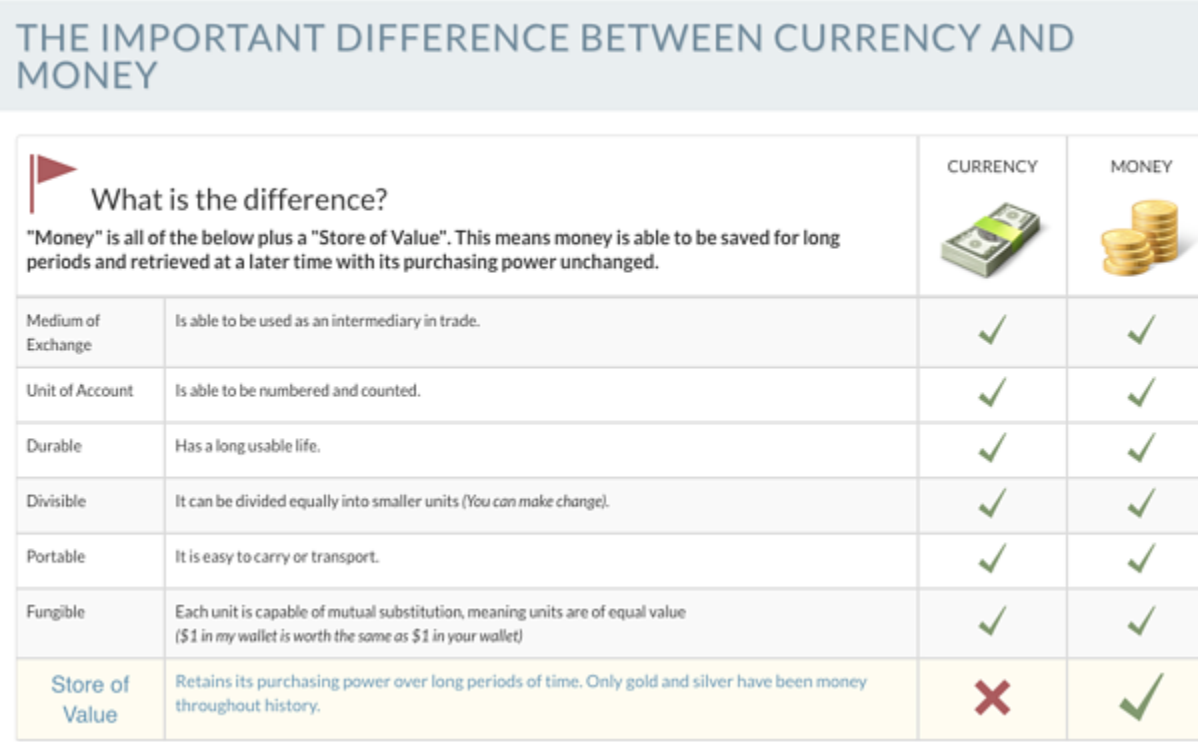
- Turkish translation by @deniz_zgur

Bitcoin - The Unseizable Asset

By Rayne Steinberg May 2, 2019

Posted May 2, 2019

You often hear that Bitcoin specifically, and crypto generally, is digital gold...but what does that mean? When most people talk about gold and its value, they are talking about how it is a superior form of money when compared to fiat currency (I have previously examined the relationship between Bitcoin and Gold prices here). The chart below summarizes the difference between currency and money:



Source

Everything lines up, except for the store of value argument, which gold proponents have always asserted is the yellow metal's killer feature. The store of value argument usually focuses on inflation - notably, issuing governments have inflated and eventually debased every fiat currency throughout history. This focuses on the "theft of inflation," but we often overlook a much more direct form of value destruction - outright theft or confiscation of property by the government. Bitcoin, unlike gold, may offer unique attributes that remedy the ever present possibility of asset seizure by force.

Property Rights throughout History

When we talk about property, it is important to understand what we mean. There are broadly three types of property regimes: common, centralized and private. When we think about property, we are generally thinking about it in the private sense:

The recognition and enforcement of private property rights are the founding pillars of a free-market economy. Private property means that individuals have absolute, exclusive and permanent rights on what they legally own: they can do whatever they like with their property, nobody can interfere with their decisions, and there is nobody to whom these rights must be returned after a given time period. Thus, under this regime each individual engages in unfettered voluntary exchange, subject to his/her compliance with the freedom-from-coercion principle (no violence and no cheating are allowed), and insofar as he/she respects the private property of the other individuals. Put differently, the legitimacy of private property and the freedom-from-coercion principle specify the moral foundations of a free-market economy. By contrast, the illegitimacy of private property and the limits to private property define the features of the centralised economies, regardless of the political format –dictatorship or social democracy. This idea that "individuals have absolute, exclusive and permanent rights on what they legally own" is the essence of Bitcoin and crypto. If you secure your Bitcoin correctly, it cannot be seized or stolen or confiscated. If you do not understand private keys or the statement "not your keys, not your Bitcoin," take a minute and watch Andreas Antonopoulos explain. Can the same be said about gold?

Property Rights in the Land of the Powerful Centralized Governments

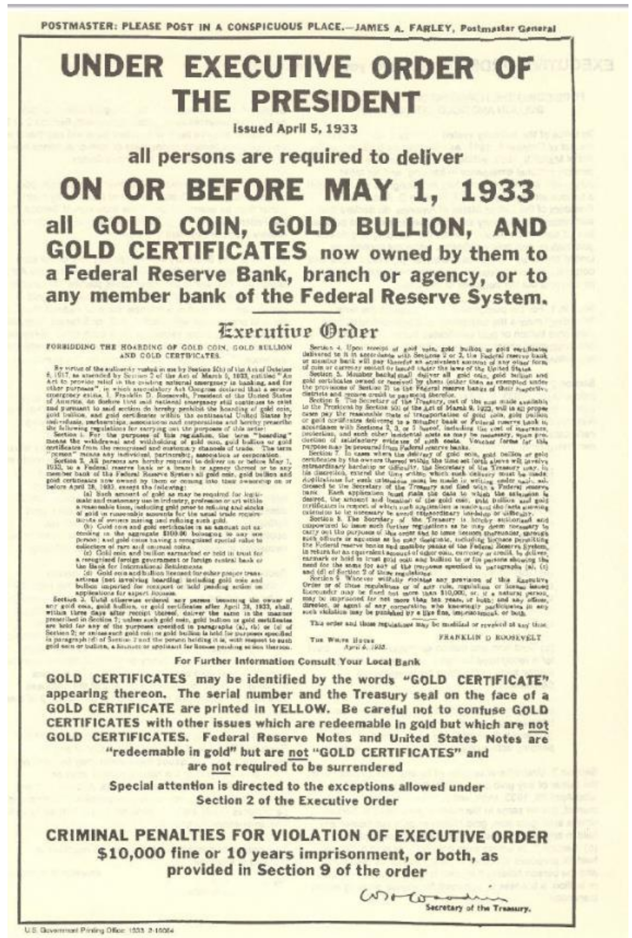
When it comes down to it, the first thing we have to look at is how powerful centralized governments have behaved when it comes to property rights in general. If we just look at the 20th century, it is rife with examples of governments seizing what they want, when they want it. In 1938, the Nazi party forced Jews to register their property before they seized it. This activity is not limited to the distant past or easily recognizable totalitarian regimes. The US has an increasingly flexible relationship between what the government can and cannot do when it comes to asset seizure. Time after time, the US government has further encroached on the rights of private citizens, taking their private property in more and more blatant manners. From the 1970's evolution of the Racketeering Influence and Corrupt

Organizations (RICO) Act, to the Comprehensive Forfeiture Act (Introduced by 2020 Democratic presidential frontrunner, Joe Biden). This trajectory of property rights erosion has continued to the present day. But, how does all of this relate to gold?

Executive Order 6102

We do not have to speculate about the generic degradation of property rights as it refers to gold ownership in the US; we have a concrete and chilling example. On April 5, 1933, President Franklin D. Roosevelt signed Executive Order 6102, "forbidding the hoarding of gold coin, gold bullion, and gold certificates."

Source



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

UNDER EXECUTIVE ORDER OF THE PRESIDENT

Issued April 5, 1933

all persons are required to deliver

ON OR BEFORE MAY 1, 1933

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

Executive Order

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

For Further Information Consult Your Local Bank

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

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

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

Secretary of the Treasury.

The order required all persons to deliver all but a small amount of gold to the Federal Reserve in exchange for $20.67 an ounce. Private ownership of gold was restricted one way or another, until the full repeal of these laws by President Gerald Ford, in 1974. The reasons given for these laws? "Hard times had caused 'hoarding' of gold, stalling economic growth and making the depression worse." Does any of this sound familiar? Is it that unreasonable to think our government would use extraordinary measures to carry out desired policy regarding the economy? Bottom line: gold was made illegal to possess in one of the freest countries in the world for over 40 years. How is that for your store of value?

Die Hard Bearer Bonds and Bitcoin

In the 1988 classic Die Hard, John McClane (Bruce Willis) defends Nakatomi Plaza from Hans Gruber (Alan Rickman).

Source What people may or may not remember (I feel like I'm dating myself with intimate Die Hard knowledge...sigh), is that the target of Hans Gruber and Co., was the hoard of $640 million in bearer bonds housed in the Nakatomi vault. Bearer bonds are securities whose ownership is determined by the "bearer" or possessor of the security. The instrument was employed to allow a feasible plan where the gang could get away with stealing that much money and spending it "realistically," without authorities catching them (there are whole areas of the internet debating the merits, feasibility and accuracy of such a plan). While spiriting away nearly a billion in value in 1988 required the suspension of disbelief, that reality is here now, in the form of Bitcoin. Bitcoin and other cryptocurrencies allow one to hold a theoretically infinite amount in their heads with no physical indication of its existence at all. While central authorities argue that the only reason to do this is to avoid legitimate government oversight, the myriad examples above demonstrate many instances of governments' abusing their monopolies of force to extract private property from citizens. No property has been immune to this seizure, including gold. Here, Hans is trying to evade law enforcement for theft. But does one's desire to have their assets be unseizable mean your goal is necessarily illegitimate? If history is any guide, an inability to seize or discover property is the true killer feature of crypto and the Achilles heel of gold and physical assets.

Why Blockchain is Not the Answer

By Jimmy Song

Posted May 7, 2019

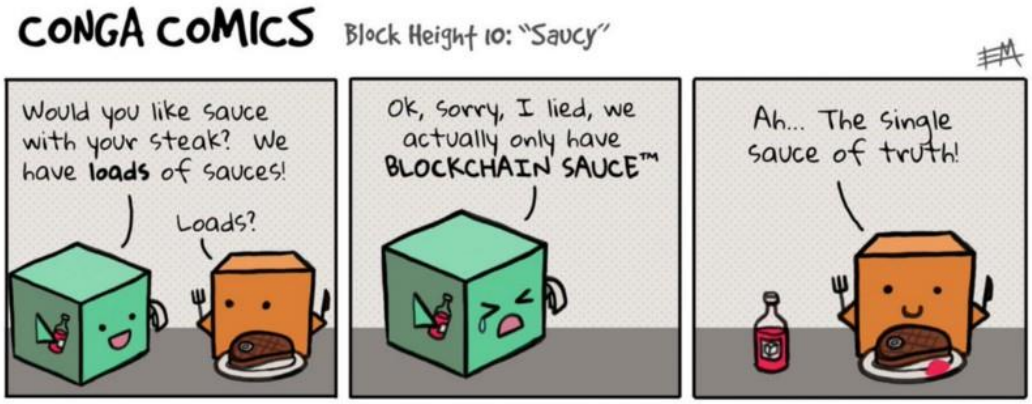
There's a persistent myth that blockchain tech is brand new and that if only given enough time, somebody will make something that's useful for something other than money. This is what I call the "blockchain, not Bitcoin" syndrome and in this article, I'm going to dispel the myth that uses for blockchain are just around the corner, that they're going to add decentralization to all the things, and that it's some revolutionary new tech.

The concept is about as bankrupt as the company whose logo which this imitates.

Blockchain not Bitcoin is 5 years old already

Corporate obsession with blockchain started in 2014, shortly after Bitcoin got on their radar. Instead of paying attention to the revolutionary, innovative, decentralized and digitally-scarce money that is Bitcoin, they instead took a concepts from the software and called it "blockchain".

Multiple industry groups were found at this time, like Hyperledger and R3 as well as companies like Digital Asset Holdings that tried to create a market around this tech.



What they had in common was the use of the word blockchain as a panacea for a bunch of problems in all sorts of industries. In typical corporate fashion, they took the word "blockchain" and bastardized it to mean whatever they wanted it to mean.

Ignorance meets hype

The life that the word "blockchain" took on around 2015 was incredible. Tons of people, especially people that weren't technical, often with only a vague sense of how Bitcoin worked, were saying things like "I believe in the technology, but I don't believe in Bitcoin". This was apparently the "consensus" response for business-types that wanted to seem like they were current on the technology.

You can understand why for two reasons. First, Bitcoin's reputation from 2011 to 2015 or so, and to some degree today, was unsavory. Bitcoin was associated with activities like buying drugs, paying for an ad on backpage or even being an anarcho-capitalist/libertarian/Ron Paul crazy. Second, by praising the technology, an executive could appear to be on the leading edge of something that's too technical for others to question effectively.

In other words, endorsing "blockchain" and not Bitcoin gave many business-types the appearance of expertise and knowledge about the topic without all the unsavory connotations associated with Bitcoin at the time. What's clear from the subsequent actions is that they had no idea what blockchain was and seeded the consequences of their own ignorance.

Their ignorance led to mediocre engineers with very little understanding of incentive systems, game theory or even public key cryptography to masquerade as blockchain experts. These "experts" bamboozled business-types into believing that the solution to the biggest problem for a particular industry could be built with a blockchain, some developers and some money. But we're getting ahead of ourselves. Before the full fledged "blockchain, not Bitcoin" syndrome caught fire, plenty of fuel in the form of hype preceded it.

Blockchain: the Panacea for All Ills

This pretense of knowledge led to books like *The Blockchain Revolution*, which promised fixes to pretty much every sector in the economy while giving just enough tantalizing technical concepts in vague enough terms that many executives felt the adolescent fear of missing out on the new technical trend of "blockchain technology".

To be fair, many were taken in by promises of solutions to real problems for their industry. For health care, "blockchain" would somehow make patient history available to care providers at exactly the right time without violating patient privacy. For law, "blockchain" would somehow create perfectly fair contracts without the need for expensive lawyers. For supply chains, "blockchain" would somehow prove whose fault it was that some parts were substandard or that not enough parts were delivered. For art, music and TV, "blockchain" would somehow reward the creators what they were due while combating piracy and taking out the middle men. For online

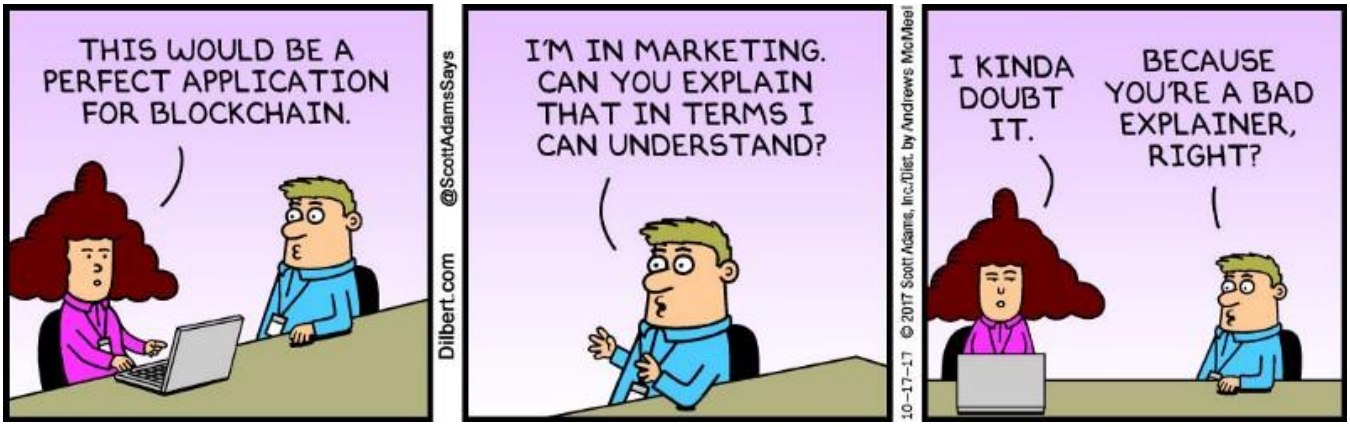
ads, “blockchain” would somehow make tracking accurate, reduce fraud and take out the many different middle men that collectively take a large portion of the profit. We could go on and on and on about the impossibly difficult problems that “blockchain” supposedly would solve.

It’s not a coincidence that these promises correspond to giant problems in each industry. Blockchain became a blank canvas onto which any problem could be painted as being solvable. Literally hundreds of startups and industry consortiums, many using ICOs, promised to solve the biggest inefficiencies in every industry using “blockchain”.

Many of these startups were created by veterans of a given industry who thought that the only missing piece was developers to write the blockchain system that would solve everything. They reasoned that they had the expertise to know what the problems were and that getting a few blockchain experts would be all that would be needed to make their industry so much better and create tremendous profit for themselves.

The Reality of Blockchain

This would work if only these developers could deliver on what the industry veterans wanted! How hard could it be to make a flawless, auditable, decentralized, encrypted database that execute terabytes of smart contracts quickly and efficiently using oracles that check each other using zero-knowledge proofs? Surely a few lines of code in Solidity could create a scalable, provably correct, maintainable system that would solve the biggest pain points of industry X, right? Well, no.



No, because no such explanations exist

Blockchain became a meaningless buzzword that meant “solving the biggest challenge in industry X” using fancy jargon to convince people that the challenge could be met. The reality was far different. What most of these

startups discovered is that blockchain is not a panacea. They ran head first into problems that we've known for a long time like the oracle problem, or the consensus problem, or the analyzability of Turing-complete contracts, or the free rider problem. It turns out blockchain, far from being a panacea is actually a hindrance to creating these solutions because of the requirement, at least nominally, of decentralization.

To make matters worse, the developers tasked with creating these systems were often completely ignorant about user and node incentives and possible exploits in an adversarial environment.

The Utter Failure

The results of such shenanigans are sadly predictable. When you promise more than you can deliver with mediocre talent in a technology that few people understand, you're not going to be able to deliver much. Most of these efforts have accomplished nothing. The few that created proof-of-concepts have not progressed to full-fledged products. The few products that have launched have very little traction (less than 2000 users per day is considered a complete failure for an app or website).

Despite all this, ICOs touting decentralized blockchains for industry X, enterprise blockchain efforts to optimize Y and even public blockchains for some service Z continue to be touted as the future. Several different arguments generally come up when this discrepancy between promises and results are pointed out.

How can you be sure nothing will come out of blockchain technology other than Bitcoin?

It's true, it only takes one counterexample to disprove my thesis that blockchain is really only useful for sound money. However, without bastardizing the word blockchain, the essence of what blockchains provide is decentralized, authoritative, expensive to alter data. This is not a surprise as these properties are exactly what you want for sound money like Bitcoin.

Unfortunately, what non-monetary projects generally need, given that it's software for an industry that's regulated, changing and growing, is a centralized, upgradeable and scalable system. Each need is made greatly more difficult when combining with a blockchain. In other words, blockchain is the wrong tool for the job.

Even if by some miracle a popular app is created on a blockchain, a centralized equivalent without the extraneous blockchain will be cheaper, faster, more reliable, more maintainable while having the exact same single points of failure as the "decentralized" blockchain-y version. Or put another way, any popular dApp is destined to lose against a centralized competitor on cost, speed, features and scale.

So many people are working on this! Something has to come out of it.

Lots of people working on something doesn't mean desires magically turn into reality (see: alchemy, cold fusion, flying cars, etc).

That's even overstating the point. Flying cars are at least possible. What most of these projects are working on are square circles or perpetual motion machines: decentralized services that have centralized control, that is, logical impossibilities.

I can hear my critics now, "Jimmy is against experimentation, entrepreneurship and trying new things!" This is a classic bait and switch

tactic. Experimentation is fine to start. Pouring more money into failed experiments is just putting good money after bad. These "blockchain" experiments have a history of being futile and have little basis in reality. They are wastes of capital and human effort and don't lead to any useful goods or services. All they do is allow charlatans to rent-seek.

Lots of money has gone into it! Someone is going to come up with something!

Certain engineering challenges are simply not a matter of funding, they are a matter of innovation. What's worse, when a company is handcuffed by being required to use a particularly cumbersome technology like blockchain, there's even less chance of anything coming out of it. This is the classic error of a solution looking for a problem. And no, more money won't magically find you a profitable market problem for which a blockchain happens to be the most optimal solution.

Conclusion

"Blockchain, not Bitcoin" is not a new idea. The past five years have produced nothing with this so-called "blockchain" technology and we're unlikely to see anything in the next five. The only thing that blockchain seems to be good at is promising to fix the biggest problems while delivering very little and consuming tremendous capital.

Blockchain is a solution looking for a problem. Too many people have been taken in by “blockchain” and pretend to see clothes on a naked emperor. The imaginary clothes may seem like perfect solutions to the biggest problems of their industry. Unfortunately, wishful thinking is not reality.

Sorry to be the bearer of bad news, but the emperor has no clothes. Blockchain without Bitcoin is a big nothing burger.

Thanks to Neil Woodfine, chandra duggirala, Vijay Boyapati, Michael Flaxman, Ben Kaufman, and DOC.

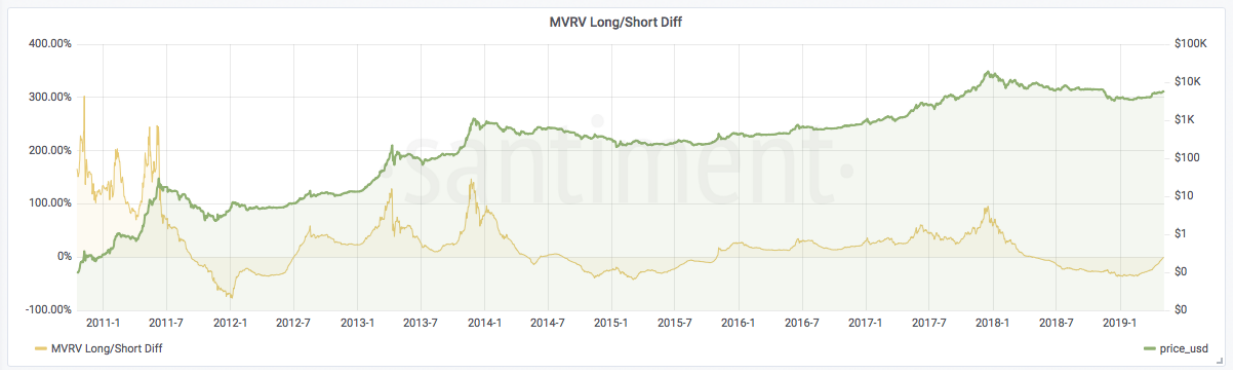
BTC Long/Short MVRV difference indicates an end of the bear cycle

By valentin

Posted May 7, 2019

The BTC Long/Short MVRV difference is almost at 0% at the moment, which historically has proven to indicate an end of a bear cycle.

What does that mean and what exactly is the BTC Long/Short MVRV difference?



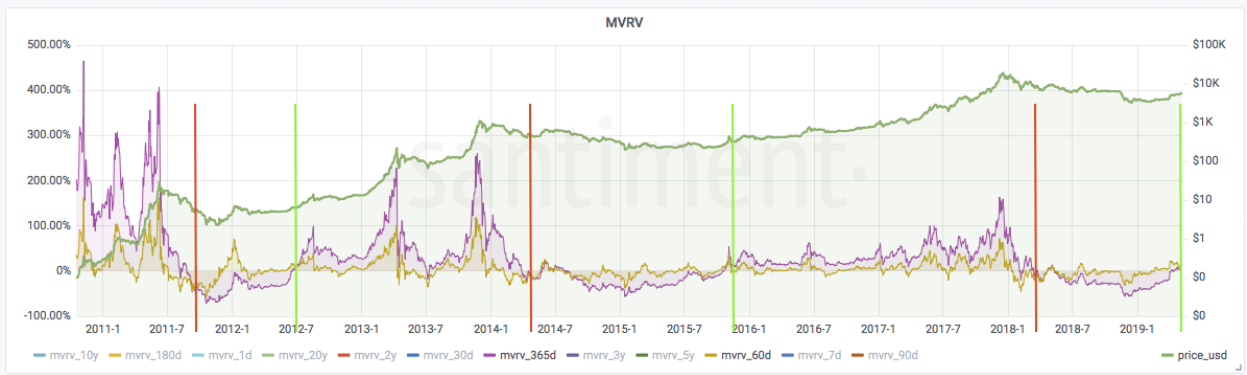
The MVRV Long/Short difference for the last 8 years. Green is BTC price on log scale.

May be you are familiar with the MVRV ratio, which was first developed by Murad Mahmudov and David Puell at the end of 2018: https://blog.goodaudience.com/bitcoin-market-value-to-realized-value-mvrv-ratio-3ebc914dbaee

The idea is to measure how much each BTC holder paid for his coins and compare it to the current price of BTC. If the ratio is above 1.0, then on average all BTC holders will get profit if they sell their coins now. If it is below 1.0, on average everyone will realize a loss if they sell. The bigger the ratio, the more sell pressure there will be on the BTC price.

At Santiment we extended this metric to a “Time-bound MVRV”, which is the same as MVRV, but takes into account only coins that moved in the last X days. For example we have 365day MVRV and 60day MVRV. These ratios will measure the average profit/loss of all coins that moved within the last 365 days and 60 days respectively. When we computed these 2 metrics we

observed something very interesting: during a bull market the 356day MVRV is bigger than 60day MVRV and during a bear market it is the opposite. The explanation could be that the short term traders are usually profiting when the market goes down and sideways, while during a bull run the long term holders are the ones that will have the final call - ultimately when the long term holders start to sell, that will be the end of the bull run. Another nice thing about the time-bound MVRV is that it automatically filters out lost coins.



365day (purple) vs 60day (yellow) MVRV. Lines on the inflection points. Red is bear cycle. Green is bull cycle.

Having all the above in mind we developed a single indicator that we call MVRV Long/Short MVRV difference, which captures this phenomena. The indicator will bottom at the bottom of the bear market and will top at the top of the bull run. As you can see from the first image above, when the indicator crosses 0, the price of BTC grows steadily. The tricky point is to identify the top of the ratio.

We are still researching this indicator and so far we've been able to beat a buy'n hold strategy using it as it gives us a good indication when we should sell. If you want to get access to this metric go to https://santiment.net/dashboards/ and requests access.

Why learn to program with Bitcoin's Lightning network?

By Pierre Rochard

Posted May 7, 2019

Send and receive payments

Enabling payments in your software is often a business necessity

Common consumer web application use cases include:

1. Receiving SaaS revenue
2. Payments between marketplace participants, including escrow
3. In-app purchases for premium features

Until now, the only choice for developers has been integrating proprietary, trusted, centralized, third-party digital credit systems like PayPal or Stripe.

Bitcoin's Lightning network offers developers an open source, trustless, decentralized, self-hosted digital cash system.

What is Bitcoin's Lightning network?

The Bitcoin digital cash system uses proof-of-work over time to provide transaction finality. This proof-of-work function is currently paid for by new cash emission and transaction fees. Full verification of every transaction is necessary for users to trustlessly determine that the expected cash emission schedule to 21 million bitcoins is correctly being followed. To keep the cost of full verification reasonable, the system's consensus rules have a number of resource-usage limits.

Bitcoin's scaling challenge is to maximize the efficient use of its limited resources. One approach is to transfer cash by privately updating one transaction many times "off-chain" before publicly broadcasting the last version of the transaction for final settlement "on-chain".

Off-chain updates to transactions instantly transfer cash, and the cost of on-chain transactions are amortized over many off-chain updates. Lightning is an off-chain scaling protocol, often called "layer 2" or "state channels". Peers

on the Lightning network send cash payments to each other by updating Bitcoin transactions.

Lightning uses smart contracts (spending conditions) embedded in Bitcoin transactions to prevent cheating by a malicious peer broadcasting a superseded version of a Bitcoin transaction.

Payments are instant and inexpensive, with a few manageable trade-offs:

- Your server should have high uptime. For almost all web applications, this was already the case.
- You must secure a hot wallet. For services that already send cash with on-chain transactions, this is not a new requirement. To minimize risk, cash can be regularly transferred from the hot wallet to a cold wallet.
- You must continuously backup Lightning data. This is a new requirement as on-chain wallets only need to be backed up once, but it is easy to implement. Almost all applications already have data which needs to be continuously backed up.

With these conditions met, Lightning is a subset of the Bitcoin digital cash system and thus shares its trustlessness and sound monetary properties.

For most software developers, using off-chain Lightning payments to enable sending and receiving cash in their application is a strict improvement over using on-chain transactions for the same purpose.

Digital Cash

Legacy solutions are trusted, centralized credit systems

Lightning is a trustless, decentralized cash system

- No counter-party credit risk
- No personally identifiable information is required
- No need to securely store other people's credit card numbers
- No charge-backs

Open Access

Lightning is self-hosted

- No need to "apply" for an account
- No unexpected account closures
- No bank holidays

- No geographical limitations

You don't need to ask for permission to use the Lightning network

Open Source Bazaar

The Lightning protocol and implementations are open source and being developed in public. Any developer is welcome to contribute to the lightning-rfc GitHub repository, which is home to the protocol spec:

lightningnetwork/lightning-rfc *Lightning Network Specifications. Contribute to lightningnetwork/lightning-rfc development by creating an account on...* github.com

Discussion of changes is open to the public, you are free to participate as much or as little as you want.

There are no executives or salespeople forcing their decisions on developers, but a business perspective is very helpful for developers working on a cash payments system.

Bitcoin Has No Intrinsic Value—and That's Great.

By Conner Brown

Posted May 8, 2019

Intrinsic Value. Bitcoin skeptics love to talk about it. Their argument is typically as follows: "Bitcoin cannot be used as a money because it does not have any intrinsic value as a commodity. For something to be a viable money, it must first be accepted and used for some other commodity purpose intrinsic to the item then slowly become a money over time. For example: because gold can be used in jewelry and electronics, people naturally stockpile it to store value."

Previously, Bitcoiners have made several compelling arguments against this on the grounds that 1) intrinsic value is subjective and 2) Bitcoin does have intrinsic value as a good for censorship resistant payments. Here I will argue that Bitcoin skeptics are right. Bitcoin has no "intrinsic value" as a commodity, but that's a great thing for Bitcoin (and the rest of the world).

Inside the Mind of a Skeptic

Intrinsic value is an old idea. Even Aristotle wrote about the importance of money being "intrinsically useful and easily applicable to the purposes of life, for example, iron, silver, and the like." It's no wonder that this idea has persisted—commodity value has been essential to humankind for thousands of years and is directly evident to the layman.

Despite its ancient origins, intrinsic value is not directly linked to monetary functions. A good money needs to be many things—portable and easy to trade, scarce and durable to store value, fungible and divisible as a unit of account—but an alternative commodity use is not one of them. So why do many critics claim money needs intrinsic commodity value?

There appear to be two main reasons.

Appeals to History

Many skeptics denounce Bitcoin's lack of intrinsic value simply because they are accustomed to stores of value doubling as commodities. Put simply—they are living in the past. Many have made this argument about previous

technological improvements by wrongly assuming that previous trends would hold true.

The fact that all previous forms of value had a physical form does not mean a new store of value must also be physical. People were making similar arguments about physical shopping during the rise of the internet. Here is a hilariously bad takefrom a Newsweek contributor in the 90's, arguing that because we've always had physical sales in the past, physical sales will not be replaced by the internet. Bitcoin skeptics claiming money needs to be a useful physical commodity will seem equally ridiculous a decade from now.

In fact history shows that commodity value is far from a requirement for a money. Nick Szabo explains in the beginning of his classic piece"Shelling out: The Origins of Money" that societies have used otherwise "useless items" for storing and communicating value. These glass beads had many strong monetary properties and were used for trading throughout Africa and parts of North America, but they had little use as a commodity. The Rai stones used by the Yap people are another example of a store of value without commodity use.

Figure One: Glass Beads formerly used as money among tribes in Oklahoma.

Appeals to Authority

Today, many who voice concerns about intrinsic commodity value trace their arguments to Austrian economists such as Menger, Mises, and Rothbard. These writers strongly emphasize the importance of money and its impacts on society. For them, commodity value and money have been inseparable since their earliest writings. One of Menger's seminal works, *On the Origins of Money*, begins by describing money as "the fact of certain commodities becoming universally acceptable media of exchange" (p. 1). Mises later built upon this understanding. In *The Theory of Money and Credit,* Mises writes, "we may give the name commodity money to that sort of money that is at the same

time a commercial commodity; and the name fiat money to money that comprises things with a special legal qualification" (p. 61).

Following in the mental footsteps of previous Austrian economists, many critics apply these outdated frameworks to attack Bitcoin. Niels van der Liden, one of the first Bitcoin skeptics (when a bitcoin was 77 cents!), rejected Bitcoin for this very reason. He claimed it would not work because "nobody could do anything with them but trade them." Therefore, he concluded they had no use as commodities and would not work as money.

While commodity and fiat monies were the only two possibilities for early Austrian economists (outside of credit instruments), times have changed. In our digital age, the distinction between commodity and fiat money has lost its value. It should be immediately apparent that Bitcoin does not fit neatly into this dichotomy—it has no use as a physical commodity but also does not exist through any legal decree. We can now hold and trade digital money wholly independent of the simple force of law. Instead, Bitcoin's monetary properties are guaranteed with rules and logic embedded into its coded DNA. Through this purely digital existence, Bitcoin lives as a money free from the restraints of the physical world.

Solving the hard money paradox

In fact, if the skeptics had done their homework, they would realize that Mises was a Bitcoiner at heart as well. He recognized the problems inherent in commodity money but saw gold as the best of bad choices. In *The Theory of Money and Credit*, Mises laments that even a monetary system based on gold is still subject to "considerable disadvantages" regarding "not only the fluctuations in the supply of money and the demand for it, but also fluctuations in the conditions of production of the medal and variations in the industrial demand for it" (p. 238).

Mises correctly points out that commodity uses of money create price distortions as fluctuating industrial demands push and pull on the shared supply. Hard money has always been associated with unique physical attributes—good for money, but also other industries. In this regard, gold's incredible versatility across many different industries magnifies this harmful effect.

The physical world also brings other monetary restraints. Something found in nature cannot be routinely distributed over time. Here, Bitcoin's predictable, periodic emission allows for supply calculations decades into the future that

are not possible outside the digital world. A physical item's supply also cannot be audited. At any moment someone could find previously unknown amounts of gold and radically dilute ownership without current holders knowing about the sudden changes in supply—similar to how cowry shells were secretly inflated by European traders to the detriment of African tribes. With Bitcoin's digital nature, anyone can audit the entire supply and know the exact amount created at any time.

With these advances, it's silly to cling to the Austrian economists giving advice for their unique historical moment. Those writers were not laying down universal constants. Even they realized their limits and hoped for better forms of money than precious metals. New circumstances require new theoretical foundations—and Bitcoin gives us just that.

Bitcoin as the key to unlocking captured utility

In our present day, it just so happens that the best stores of value are also those that have some element of utility as a commodity. The key distinction here is that gold, real estate, or any form of commodity money is not a store of value **because** of its utility as a commodity, but **despite** that utility!

When someone decides to hold gold or any other asset for a monetary purpose, they make a clear and conscious choice to use it for its wealth storage properties instead of as a useful commodity. Rather than creating electronics parts or jewelry, holding a gold bar puts gold's monetary properties to work. While this decision may appear innocuous, this can bring harmful economic consequences. Large numbers of people storing their value in a specific commodity with hopes of wealth storage often leads to extreme waste and speculative bubbles.

Real-estate is a particularly egregious example of this effect. Today, speculators chase "golden concrete" to protect their wealth. Developer Michael Stern explains "the global elite is basically looking for a safe-deposit box" and many have decided to invest in Manhattan properties to store their funds. By doing this, they are using their luxury apartments for **saving instead of for living.** As a result, journalists noted "according to the Census Bureau, throughout a sweeping stretch of midtown—from Forty-ninth to Seventieth streets, between Fifth Avenue and Park—**nearly one in three apartments is completely empty at least ten months a year.**" Similar trends are spreading through large cities worldwide. As *The Guardian* reports, "[t]he trend for the world's super-rich to invest in prime London property as a way to safeguard their wealth, without the need to secure a rental income, has

meant the **number of empty homes in Kensington and Chelsea rose 22.7% over the same period and 8.5% since 2015.**" As the elite continue to pour wealth into these commodities, bubbles begin to rise to the top. A recent report by UBS shows just how risky this has become.

Not only are properties sitting empty, using homes as a significant store of wealth destroys healthy market incentives for new housing development. San Francisco and the rest of the California housing market are obvious examples of this phenomena. Below is a map illustrating San Francisco's zoning regulations. All areas shaded yellow are limited to a building height of 40 feet.

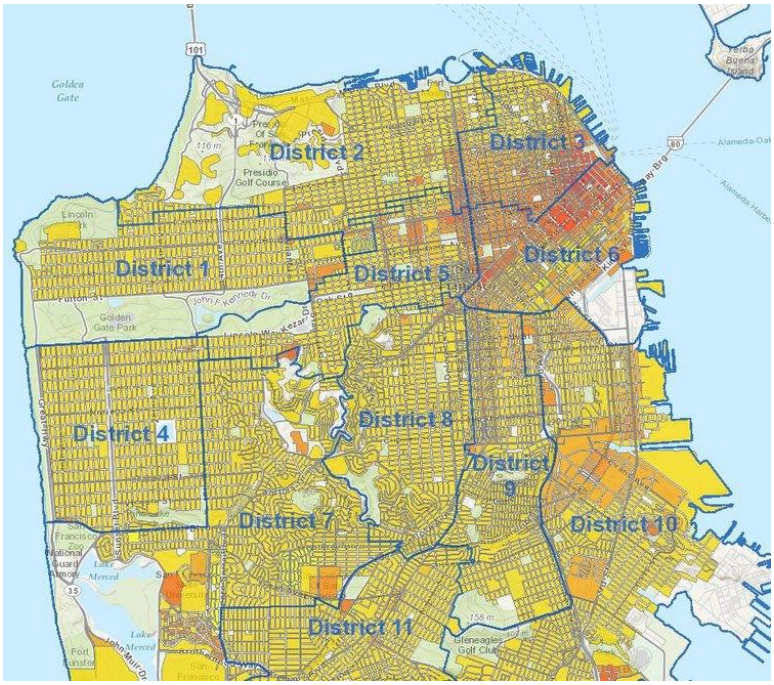


Figure Two: A map of San Francisco's local zoning laws.

These regulations are a clear impediment to building new affordable housing to meet demand. Given the repercussions on the average residents and rent prices, why do they exist? One large cause stems from existing homeowners lobbying for artificial restrictions on supply to preserve their wealth. A recent report by the Legislative Analyst's Office for Californianoted that "residents may see new housing as a threat to their financial wellbeing. For many homeowners, their home is their most significant financial investment. Existing homeowners, therefore, may be inclined to limit new housing because they fear it will reduce the values of the homes." Because the average buyer does not have a reliable store of value in their money, homes are considered by many to be the best place to safeguard one's wealth. This naturally causes homeowners to then lobby to constrict home supply so their precarious wealth is not diluted. **In this sense, the real-estate markets only have store of value properties through artificially generating scarcity.**

Bitcoin would not solve this problem entirely, but it gives potential homebuyers an alternative way to securely store wealth over time. Allowing

people to rethink their financial decisions may ease the pressure against building new homes. With new affordable development, cities would be able to increase their density and improve the quality of life for all residents. For example, research modeling suggests that if San Francisco were able to increase its housing density, this could significantly reduce the city's carbon footprint, increase the city's walkability, and improve the quality of community life—all while preserving the signature sunny California environment.

Even securing the network would be cheaper, with higher quality ASICs!

Gold is another great example. As individuals sell their gold to buy bitcoins, gold that was previously held for its wealth storage properties can be put to work in electronics, medical devices, and aerospace pursuits. It can even be eaten! Gold stored around the world can be used to benefit society through cheaper and higher quality products—and make previously impossible endeavors much more affordable. With Bitcoin we can actually afford to go to the moon. So when you hear goldbugs extol its amazing societal uses—they are right—but they are really making a case for digital gold. By acting as a global store of value, Bitcoin unlocks that stored commodity utility that we've had to set aside because our world has always lacked a pure money.

Final Thoughts

Instead of locking up useful resources to store wealth, Bitcoin gives humans the ability to store wealth free from the opportunity cost inherent in storing commodities. This global, permanent, and accessible store of wealth is forming a solid bedrock for future economies around the world. As funds move from other asset classes towards Bitcoin, this newfound supply will create better access for affordable housing, rejuvenated urban environments, higher quality consumer goods, and more.

Yes, Bitcoin has no intrinsic value and for that we should be thankful.

A special thanks to Karina Kauffman, Dan Held, and the Bitcoin Observer for their incredible help.

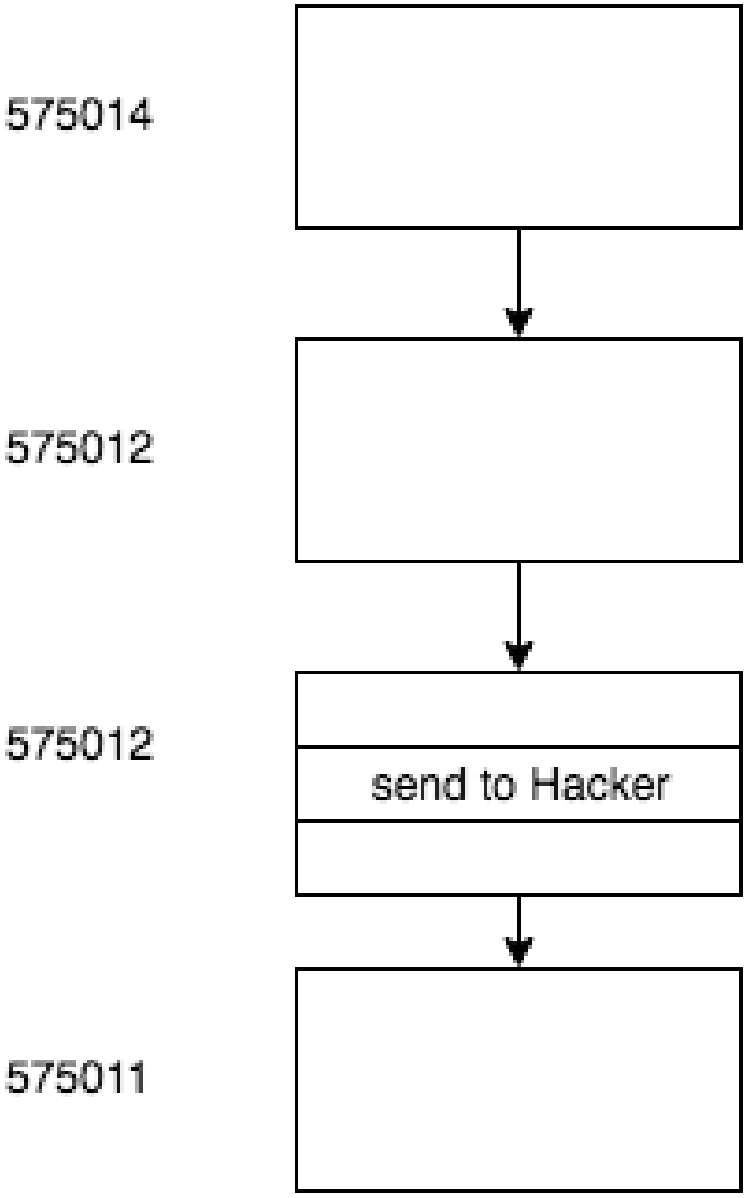
How to bribe miners to re-org?

By Tamas Blummer

Posted May 8, 2019

Organizing a re-org to revert a Bitcoin transaction was recently considered but not attempted Binance. They could have done it, would they had better understanding the technology and POW economics. I describe how to bribe miners so they unite for a re-org.

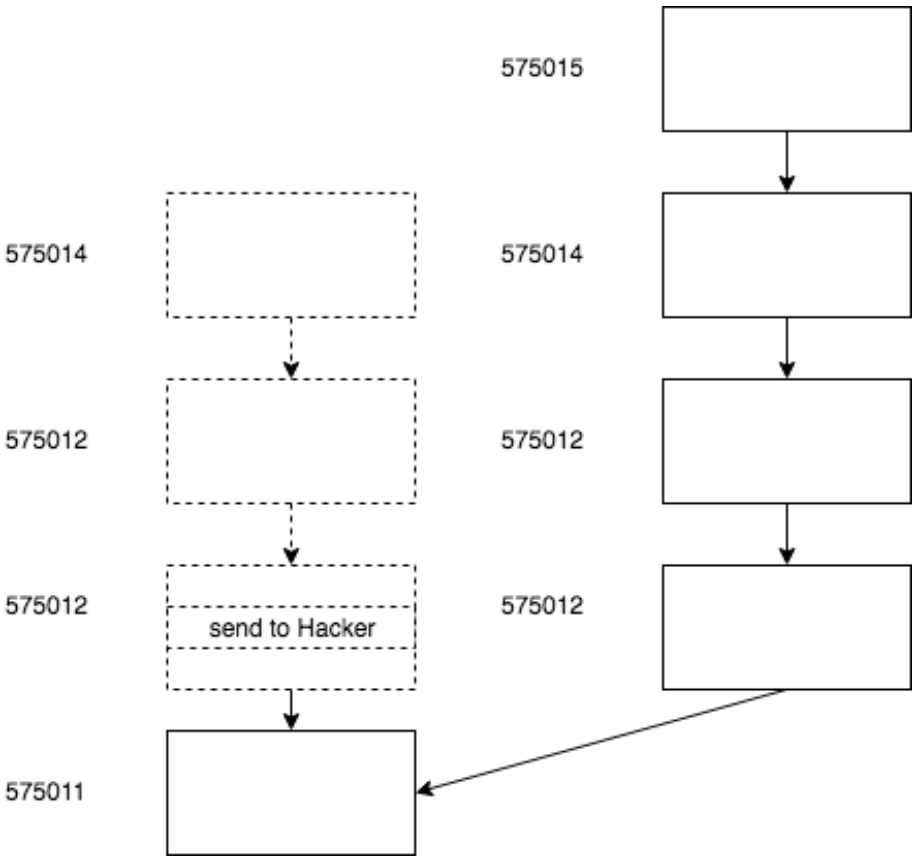
A bitcoin transaction economically matters only if it is recorded in the chain of blocks with most work.



There are already 111 blocks built on top of the block containing the Binance hacker's transaction by the time of this writing. It is safe to say now, that Binance lost 7000 Bitcoins.

Block 575011 contains the hacker's transaction and further blocks were mined as usual on top of it.

Bitcoins lost to the hacker could be re-claimed if miner would build an alternate continuation of the chain that roots before the block that contains the hacker's transaction. That alternate continuation would not contain the hacker's transaction and would have to grow faster than the current one, so at some point it exhibits more work and all Bitcoin clients re-org to it. After the re-org the hacker's transaction would ceases to exist in the memory of the network.



The earlier versions of blocks 575012 and higher would then cease to exist in the memory of the network.

Re-orgs to an alternate chain with higher work are nothing special for the network, but its regular method of resolving the race between independently working miner. Re-orgs that replace the most recent block are quite frequent.

A re-org is costly for the miner who mined on the side that ceases to exist, since the miner loses the Bitcoins mined in those blocks. This is the main reason why miner are keen to extend the chain and avoid creating alternatives.

Binance CEO considered to offer the stolen funds to miner who build an alternate chain of blocks. He can offer those funds in the alternate chain since they would remain in his control there. He rejected the plan as he thought it was impractical. It is impractical if considered within the bounds of collusion between his friends and network, but would have been possible if he was prepared, knowledgeable and quick.

How to bribe the miners

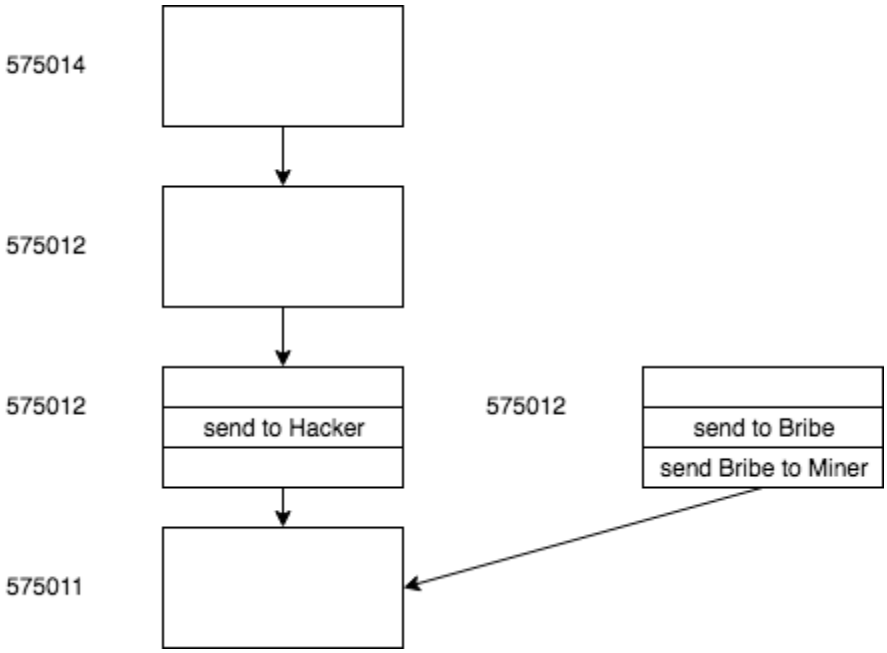
Besides calling friends Binance CEO could have done the following as soon as the breach is noticed:

1. Create a transaction that spends a big chunk of the stolen funds from their last controlled address to a bribe address and publish the transaction on their web site.

2. Publish the private key of the bribe address on their website.

The transaction is worthless in the current reality since the funds are at the Hacker's address, but is perfectly valid in an alternate reality that starts with an alternate block 575012.

A miner who builds an alternate 575012 can include the transaction published on the website and also another transaction that moves the bribe to his own address, since he also knows the private key for the bribe address.

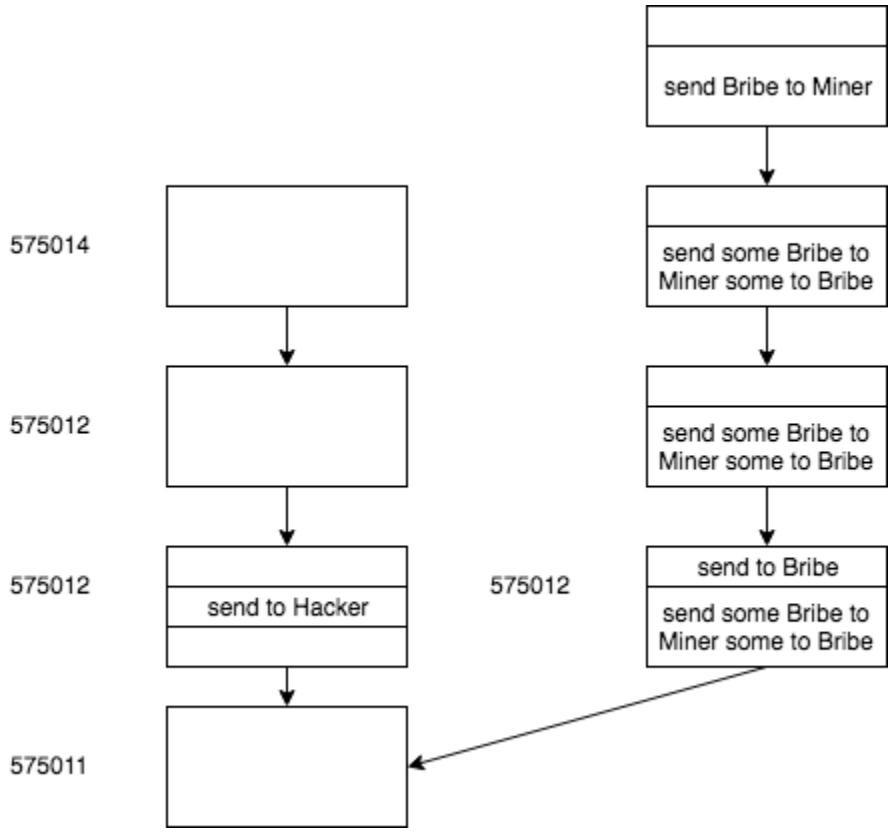


It is rational for a miner to mine that alternate reality if the bribe is higher than the amount of Bitcoins he mined since Block 575011 **and** there is a sufficient chance that the alternate reality will attract more work than the current chain.

Note that the miner can significantly increase the chances of the alternate reality taking over by not taking the entire bribe but leaving sufficient amount for the next miner.

A sufficiently hight bribe and not too greedy split of it can build a coalition for the alternate reality quickly and more efficiently than calling friends as any miner is invited and could be attracted to join.

Eventually the chain of miner splitting the bribe could overtake the current chain and in the new reality after the re-org Binance would own the rest of the stolen funds and miner who participated in the rescue would have earned much more than usual.



I know that above rescue is technically feasible. It would work if those who can lose funds are prepared to offer a bribe and miner are prepared to act on it and make rational choices. Chances of success still diminish exponentially with time.

Exchanges could commit in advance to use this procedure in the unlikely event of losing funds, so miner are also prepared to act swiftly on the offers.

Consequences?

Consequences of miners acting on a bribe could be severe as the re-org can disrupt regular transaction processing and diminish trust into the block chains immutability.

Damages would be proportional to the length of the re-org. I think damage would be negligible if the rescue maneuver is executed within hours as a re-org of a few blocks is not an event in the technical sense and would not noticeably delay regular transaction processing.

Addendum

After publishing above, I participated in a few public discussions and the most prominent objection against the described procedure was that the hacker could counter the bribe on the original chain. While this is technically correct, it neglects that miner who would take that offer would become complicit and target of lawsuits. Even anonymous miner were vary of taking

those coins as they could not be sold in short term to cover their electricity cost, also being associated with coins in high interest could dox them.

Tweetstorm: Ari Paul on the reorg and it's feasibility

By Ari Paul

Posted May 7, 2019

- There's a bit of superficial discussion happening (mostly dismissal) of CZ of binance's exploration of reorganizing the blockchain to reverse binance's recent hack. Here's why such a rollback is plausible in a future case (whether we want it to be plausible or not.)
- 2/first, I'm not commenting at all on what I want to happen or what's good for bitcoin. I'm going to argue reorgs in these scenarios may be a natural result of the game theory for bitcoin that Satoshi created.
- 3/this hack was relatively small, but consider Bitfinex's previous hack of 117k+ BTC, which was 30+ days of block rewards. If Bitfinex could create a smart contract to programmatically incentivize miners to re-org 3 days of the blockchain, the simple economic incentives work.
- 4/ then the question is coordination. A reorganization requires 50%+ of hashpower, but doesn't require conscious coordination. If no one miner had more than 1% hashpower, and all were truly anonymous, might raw incentives serve to coordinate a reorganization?
- 5/ I'm not aware of how you could structure such incentives entirely within the bitcoin network itself. The logic of the smart contract would, I think, have to refer to whether a re-org has occurred. The incentives might have to be provided on another layer or network.
- 6/ but I'm probably missing some simple clever in-network incentive structures. Regardless, there's a pie of BTC value that could be programmatically cut to incentivize the reorg for any and every miner, considering only mining economics.
- 7/ if the exchange is incentivized to attempt this, and all rational miners are incentivized to take the deal, why wouldn't the re-org happen? Only one answer I believe - we have to hope the miners act uneconomically in the short-term due to altruism, or non-mining incentives.
- 8/ many miners *are* incentivized by things other than mining math. They have other economic incentives like the value of their ASICs or BTC on balance sheet. It would come down to miner incentives in the reorg payoff vs devaluation of their ASICS or BTC.

- 9/ for any one small miner, they could sell their BTC at market, so more decentralization is actually *worse* in this regard since it makes miner BTC holdings more liquid (smaller relative to market liquidity.) same might apply for secondary ASIC market.
- 10/ in a world where miners don't have to own their ASICS and don't generally hold a bunch of BTC, there would be really clear economic incentives for the re-org to happen. But what about the real world where miners do own ASICs?
- 11/ here it might be a prisoner's dilemma, I'm not clear on the right game theory model. Collectively miners might be hurt by the re-org devaluing their hardware, but every individual miner is incentivized to re-org. Re-org is binary though, different from typical prisoner's.
- 12/if the exchange could think of a way to reward every miner that supports the re-org more than those who oppose it, that might be enough to cause the reorg by turning this into a classic prisoner's dilemma.
- 13/is this a bad thing for Bitcoin? Maybe. One way to think about all of this is just as a cypherpunk free market rising organically from Satoshi's competitive mining game theory solution for BFT. It's just economic actors playing the game.
- 14/what result might this have? For average users, probably none. Average transactions would almost certainly be included in the re-organized chain. So this would probably only be relevant to giant, "fast" transactions separated from the legal system. exchange withdrawals.
- 15/does our twitter conversation on this topic matter or is this just shouting into the wind and it's all up to miner incentives? Twitter actually matters a little here, since we're effectively increasing the cost of the reorg to miners.
- 16/by strengthening the social consensus around immutability, we imply a large devaluation in BTC price should such a reorg occur, which incentivizes miners who own ASICS or BTC not to reorg in marginal cases.
- 17/as part of that social consensus building, I expect the self-appointed social media bitcoin priests to attack this thread. It's kind of their job to vigorously support the immutability social consensus. Have at it you self-appointed social consensus guardians 😀
- 18/a final thought inspired by the brilliant Adam Back (but disagreeing with him.). Past data is useless here. Incentivizing a reorg is a hard

coordination problem that fairly simple new tech may solve.

- 19/another final thought again inspired by Adam. Most of the logic in this thread could be changed if node operators ran software that didn't blindly follow the longest chain. Such software may be provided eventually, some Core devs have worked on it.

Tweetstorm: Jimmy on the reorg

By Jimmy Song

Posted May 8, 2019

It's too bad cz didn't try to reorg.

Why? I think it would have failed spectacularly and would have completely disproven the miner centralization concerns leading to an enormous price spike. Bitcoin is antifragile. It does better after disordering events like a reorg attempt.

No, You Can't Just 'Rollback Bitcoin'

Yet Another False Narrative

By Eric Olszewski

Posted May 9, 2019

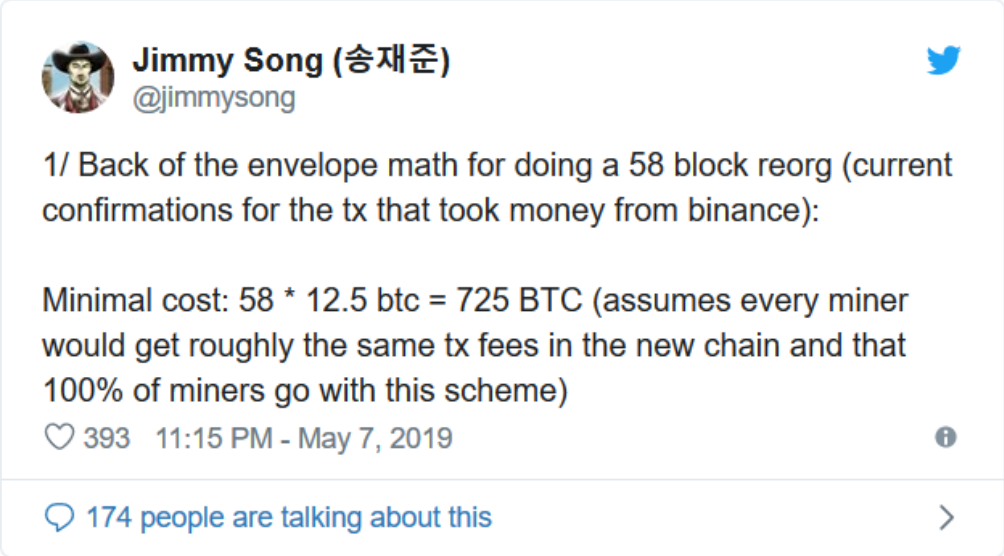
A few days ago, Binance, one of the largest cryptocurrency exchanges, faced a hack in excess of 7000 Bitcoin (~ $42M at the time of this writing). Details on the hack, here.

With so much value stored in these exchanges, it's unsurprising that they are getting regularly hacked. And it's somewhat hysterical to hear about someone losing their Bitcoins to an exchange hack given that one of the main values of Bitcoin is the ability to be in complete control of your own wealth. And as far as the majority of the Bitcoin community is concerned, these people knew the risk that they were taking.

Lucky for the individuals who were affected by the hack, Binance stepped up and used a contingency fund to refund all affected users. Regardless, this was small potatoes compared to things like the Bitfinex hack of 2016 where 120,000 BTC were stolen or the infamous Mt. Gox hack of 2014 where over 850,000 BTC were stolen.

And yet, someone in the community thought that miners could be incentivized with a percentage of the stolen funds to re-mine from the point of the hack, omitting the transactions which stole the funds.

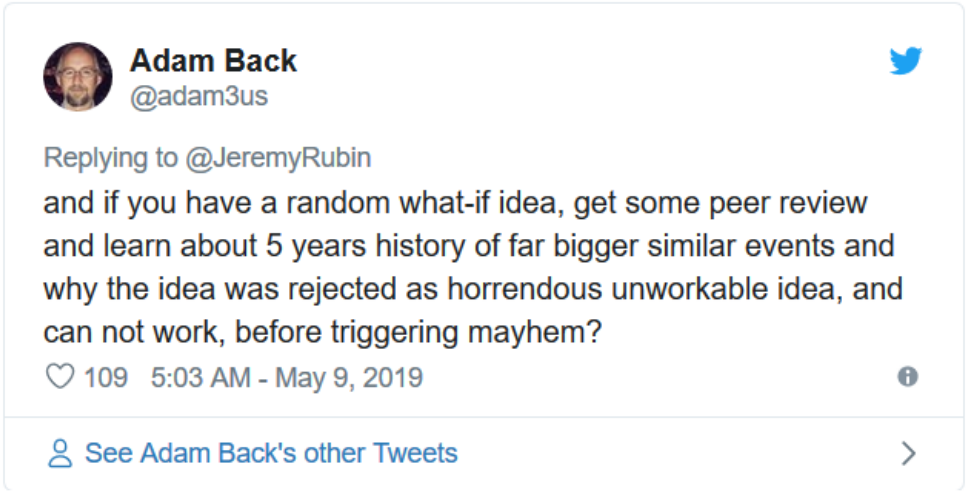
With the justification for this sort of reasoning being that each Bitcoin block takes 10 minutes to mine and pays out 12.5 Bitcoin, so, Binance could just pay miners more than what they made mining the previous blocks to re-mine them, and omit the hacker's transactions. And while such measures may be lucrative to miners, these are only in the short term—Jimmy Song gives a good overview on how this becomes less and less so as time progresses.



Not to mention that if this were to occur, that it would undermine Bitcoin's censorship-resistance and damage the network's value. This would likely tank the price of of Bitcoin, as well, and subsequently hurt the miners who performed the reorg to begin with.

While something like this **could** certainly happen, the fact that it was asserted as something which could easily be pulled off with short-term incentives for miners shows how many people are completely oblivious to Bitcoin's history.

While a reorg which removes past transactions is not against the initial Bitcoin design, its ramifications on the value of Bitcoin would likely be cataclysmic. And I highly advise everyone new (and old) in the space to look back at Bitcoin's history before asserting it's future.



Note: As much as I hate exchanges, Binance did an incredible job of handling things and being transparent throughout the process. Major kudos to them and CZ for admitting their faults and communicating updates as they surfaced.

A modest proposal regarding Bitcoin mining

Nic Carter

May 9, 2019

From the editor… This is satire, just want to be clear.

Join us, or pay the price.

Following the sad loss of funds suffered by Binance, the well-loved crypto exchange, the Bitcoin community rallied around the embattled exchange and wisely proposed that Binance institute a reorganization of the Bitcoin blockchain in an attempt to steal back the funds, or at least confiscate them from the hacker.

However, due to miner unreadiness and the shameful trolling by certain regressives and malcontents, Binance was not able to marshal a reorganization in time. Those stolen funds are now buried under an impossibly heavy hash weight and cannot be recovered.

To prevent this in the future and protect our blockchain from griefers, hackers, and the alt-right, I propose a set of countermeasures to ensure that

Bitcoin remains ethical, compliant, and bailout-friendly, as intended by its creator, Craig Wright.

Introducing the BMSRO

Bitcoin mining at present is a global, anarchic industry with no barriers to entry. From 2009-present, individuals merely had to plug in a computer and start hashing away without asking anyone for permission. Otherwise-wasted power is often purloined and mining is sometimes done without government consent, as in Venezuela. Mining must be rendered more compliant, and miners must have a central body informing them when to reverse fraudulent transactions.

Today, I am delighted to announce the **Bitcoin Miner Self-Regulatory Organization** (BMSRO) which will remediate these woes. By demonstrating compliance, a commitment to rapid chain reorganizations, and serving as a single point of contact for governments, the BMSRO will take Bitcoin mining from a dangerous backwater to a safe, modern, and cooperative industry.

The chief activity the BMSRO will engage in will be the facilitation of deep reorganizations of the Bitcoin blockchain, to punish fraudsters and hackers who steal coins. Inspired by the excellent work at the EOS Core Arbitration Forum, the BMSRO will enable exchanges to submit Reorg Requests to member miners who will collectively agree to reorder the transaction history. This requires significant cooperation, so we will need to get a critical mass of miners on our side first—at least 51%. We believe that miners will join us thanks to the same economic incentives that drive Bitcoin. By introducing regulatory moats, the BMSRO will enable miners to create barriers to entry in their industry, protecting the hardworking incumbents from competition.

How will the BMSRO affect you? If you are a regular user, you won't have to change much—but you can rest assured that your network will actively seek out and reorg crooks and fraudsters. At last, a safe and crime-free network. Below, we've included guidance for major stakeholders.

Guidance for miners

If you're compliant, clean, and happy to cooperate with other miners, your business won't change. All miners will have to register their business with the SRO and announce their participation before beginning to hash. Previous hashers will be granted conditional amnesty if they agree to fully comply with the SRO's mandates on an ongoing basis, subject to a probationary period.

Miners should submit their self-identification to our CAO (Chief Anarchy Officer) with the **ITH-1 form** (Intent To Hash). ITH-1 approvals are subject to on-site audits, meeting environmental suitability guidelines, and passing background checks. Full form in Appendix A.

Other conditions of SRO membership include:

- Member miners must, in an expedient manner, process the latest Reorg Requests from exchanges who have lost funds. Failure to do so will lead to expulsion from the BMSRO and punitive actions, including the confiscation through reorg of your last 12 months of block rewards (failing to take part in the BMSRO is classified by our Ethics in Bitcoin board as a hostile act).
- All miners must include the latest hash of the Miner Accord in each coinbase output. The miner accord specifies permissible miner behavior and the inclusion of the hash indicates their willingness to participate in arbitration decisions.
- All miners meeting the hash thresholds who are classified as Medium or Large miners on ITH-1 must appoint a mandatory compliance officer who will manage the on-site audit process and the environmental sustainability of the mine. Acceptable sources of energy include solar and wind, but not nuclear because it's scary. Dirty miners will have to buy carbon credits.
- Is your randomness good enough? Miners classified as Large under ITH-1 must appoint a CEO – Chief Entropy Officer. They will be tasked with sampling hashes to ensure randomness. Good randomness is hard to obtain; we suggest using our official BMSRO Certified Randomness Feed. Alternatives such the NIST Randomness Beacon are also acceptable.

Guidance for users

- Do not store critical information (timestamps, hashes of important documents, supply chain information, proof of provenance) on Bitcoin. Bitcoin is **not** your playground. It is a strictly mutable ledger and should be treated as such. Know that due to the many deep rollbacks the BMSRO expects to facilitate over the coming years, information included in Bitcoin ought to be treated as unreliable and nonfinal.
- Practice strict KYM (Know Your Miner) policies. Do you know who is mining your transaction? It could be anyone—vagabonds in Sichuan monetizing otherwise-wasted hydropower, ISIS, North Korea, or even 4chan. Did you know that under the Bank Secrecy Act of 1970, a failure

to vet the miner who is including your transaction in a block could be a federal offense? Ensure that you have a clean line of communication with your miner and that you trust them to behave appropriately and censor the correct transactions.
- Be advised that the militant wing of the BMSRO—the Subcommittee for Correctness in Bitcoin Transacting— actively ensures compliance by monitoring users. If you express skepticism of the BMSRO's objectives, wear a UASF hat in public, or "troll" our member organizations on Twitter, expect a two-week ban from transacting with any of our member miners. On your second offense we will include your information and your offense in the OP_RETURN so everyone will know of your malfeasance. However, due to our ongoing challenges with immutability, we expect these public shamings to be reorged out at some point.

Guidance for exchanges

Fear not—hacks will soon be a thing of the past. If you join us, you will be able to submit expedient Reorg Requests to the Arbitration Forum the very moment you notice something awry. We will manage the miner coordination and ensure that, pending approval by the Ethics in Bitcoin Board, malicious transactions are reversed. The EiB Board, consisting of three white dudes in their 30s from Brooklyn, has worked out a consistent and fair ethical framework that should prove acceptable to people the world over.

- Connect with your local miner! Exchanges should have very close relationships with their miner counterparts and abide by KYM (a stated policy position of the BMSRO is to lobby regulators to institute mandatory local KYM). You trust your miners to order your transactions, why not codify that relationship with a contract? You deserve recourse if they don't follow one of your official Reorg Requests.
- OTC desks and traders—if you make a bad trade or a fat finger, we encourage you to submit a Reorg Request (although our member exchanges will get priority in the Reorg Queue). We promise the deepest and most compliant network of miners and will be happy to help reorder transactions in the blockchain such that you do not have to suffer.
- We suggest you vertically integrate. Why trust a third party miner to reorg on command when you can simply mine yourself and take full responsibility for your transactions? This way, you can impose full stack compliance on your users. And if you register as a miner, you will get to enjoy all the benefits of arbitration without the exchange fees.

BMSRO governance

As an organization dedicated to uniting the innovation of the present with the prudence of the past, we have designed our governance processes accordingly. Just as Bitcoin's innovation must be married to the recourse of credit networks and the benevolent American oversight of SWIFT, we will unite old governance mechanisms with the new.

In this light, we will marry liberal democracy—the greatest innovation the world has ever seen—with futurism and neat algorithms. As such, members of the BMSRO advisory council, the Ethical Correctness Board, and the Arbitration Forum will be elected by members through cubic voting. That's like quadratic but with the third exponent. (We wanted quadratic but apparently that's encumbered by IP).

I hope you'll join me. If you don't—we'll reorg you anyway.

Towards a more compliant, safer, and predictable world,

Nic Carter Inaugural Chief Anarchy Officer The Bitcoin Miner Self Regulatory Organization

---

Differentiating Against Bitcoin

By Sourabh

Posted May 11, 2019

What factors will investors consider important when comparing other cryptocurrencies to Bitcoin? [Image source]

When Satoshi Nakamoto released Bitcoin, it naturally garnered interest among cypherpunks trying to create digitally native money. By using Proof of Work and its difficulty readjustment mechanism to solve the double spending problem, Satoshi managed to put Bitcoin significantly ahead of previous cypherpunk attempts at digital money. Along those lines, it is understandable why the Bitcoin community is irritated with most altcoins today; they simply do not differentiate against Bitcoin meaningfully enough to warrant attention.

While I sympathize with the core beliefs of this thinking, it does leave lingering questions. Along which dimensions could a cryptocurrency compete against Bitcoin today? Did Satoshi get every cryptocurrency design choice right? As a believer in free markets, I am in favor of honest cryptocurrency competition. Not to mention the fact that fierce competition through a truly free market strengthens the ultimate winner of the cryptocurrency market.

At this time, differentiations have been proposed along many vectors, ranging from privacy to on-chain governance. For the most part however, these differentiations are marginal and insufficient to disrupt Bitcoin on their own. In the end, I believe there are two differentiations against Bitcoin that could provide meaningful competition against Bitcoin: a cryptocurrency's adaptability and its ledger assurance model. This blog will take a look at some of the most popular differentiations available: programmability, privacy, throughput, monetary policy, adaptability and ledger assurance, and

examine whether they provide enough of a competitive advantage to compete with Bitcoin in the long term.

Programmability

Programmability is perhaps the most well known form of differentiation in crypto. The main idea behind programmability is that it makes developing dApps much easier. In turn, the utility generated by dApps drives monetization.

In the case of Bitcoin, the sole purpose of Bitcoin's script is to provide a simple way to signify the authorization of a value transfer. Satoshi said it best: "The nodes only need to understand the transaction to the extent of evaluating whether the sender's conditions are met." Bitcoin's script was intentionally limited to predicates because Satoshi did not believe that programmability would be the key driving force behind making Bitcoin more money-like.

On the other hand, programmability advocates argue that the additional utility from more programmability will drive monetary premium. While true to some extent, additional programmability also exposes a cryptocurrency to a greater attack surface, as seen with Ethereum's DAO hack. Ultimately, the marginal utility gained from additional programmability must also be compared to the marginal attack surface created by it.

Moreover, from a monetary perspective, it is not a given that utility is the critical driver of monetary premium to a cryptocurrency. Although utility does play a role in bootstrapping some forms of money, monetary premium is ultimately driven by other factors, like network effects, durability, reliability and liquidity. A good example of this is gold. For the most part, during gold's monetization, there were few practical uses for gold. Despite this, gold had common acceptance throughout the world, could be easily stored and verified, remained scarce throughout history, and thus was widely used as money.

It is also worth noting that while Bitcoin's script limits programmability to boolean evaluations, it does not necessarily limit its extensibility. For example, recently proposed BIP-schnorr, BIP-taproot and BIP-tapscript have recently been proposed by Pieter Wuille in order to modify script to allow for Schnorr signatures. These BIPs would structurally change script without increasing programmability while also increasing the efficiency and privacy of transactions. In sum, Bitcoin's script provides more than enough extensibility to improve Bitcoin's ability to function as a money without taking on risk associated with additional programmability.

Another way of looking at it is that transactions only occur when the sending party agrees on conditions under which they will transfer value. Script seeks to serve that use case solely. In turn, script's predicate based nature fits this model perfectly, and provides plenty of room to grow. As noted earlier by Satoshi, ideas for script include multisig for custody solutions and hash time lock contracts for Lightning have provided tremendous value to Bitcoin's ability to function as money without having to fully engage with the programmability-security tradeoff.

In conclusion, although Bitcoin's script demonstrates the usefulness of programmability to a cryptocurrency's ability to function as money, it isn't clear how additional programmability infuses enough additional "moneyness" into a cryptocurrency for it to differentiate meaningfully against Bitcoin.

Privacy

At first glance, it appears that privacy would be a strict improvement for a cryptocurrency to pursue given Bitcoin's complete transparency. However, a closer look reveals some problematic tradeoffs.

First, increased base layer privacy reduces auditability, which is important because it helps users quickly verify that Bitcoin is functioning as expected. A great example of this was the recently disclosed Zcash bug: printed coins may exist in the shielded pool and we'll never know for sure whether coins have been counterfeited. This is a truly disastrous outcome for a cryptocurrency. Ultimately, auditability ensures that everyone can verify that their currency is not counterfeitable and is crucial for scarcity and social consensus.

Second, privacy coins often require users to trust innovative cryptography that is much more experimental than the well established primitives of digital signatures and hash functions. As a result, privacy coins further push users to trust a handful of cryptographers to maintain the cryptocurrency. Again, this is a tradeoff, where users gain privacy at the expense of trust.

Third, privacy does not need to be built into the base layer. As a comparison, the Internet can provide a fair degree of privacy through Tor's onion routing to obfuscate network activity and TLS for encrypting communications. A similar story is happening in Bitcoin, with Wasabi wallet "fungiblizing" individual users' bitcoin via Chaumian coinjoin through the transaction layer and proposals like Dandelion for hiding transaction origination in the network layer.

Moreover, it would be very cumbersome to implement privacy at the physical layer of the Internet. Although physical layer privacy may have been ideal, it presents challenges that are simply easier to address at other layers of the Internet. In the end, the Internet's physical layer focuses on one job: providing a reliable physical medium through which information can be transferred.

Finally, we do see some issues prop up with privacy coins at a performance level. For example, the privacy coin Monero cannot be pruned, could be vulnerable to tracability attacks and has a much larger transaction size compared to Bitcoin. This is a direct result of the complexity involved with implementing privacy. In the end, the cumbersome nature of building privacy is akin to a fully private physical layer of the Internet: ideal, but with substantial and potentially unnecessary performance tradeoffs.

On the other hand, one can make the case that the Internet faces privacy issues today as a result of not taking the time to properly build privacy lower in its protocol stack. As a result, today's Internet users do not have privacy by default, and most users do not end up benefiting from the tools available that help make using the Internet more private.

In sum, privacy offers a differentiation against Bitcoin that provides a valuable characteristic of money to users and a critical property of money, but with some very important and potentially avoidable tradeoffs.

Throughput

If a new cryptocurrency were to appear that improved throughput without engaging in any tradeoffs, it would be an instant hit. Of course, in a world without free lunches, this is not possible. Throughput is measured in transactions per second, and is inversely proportional to transaction size and directly proportional to block size.

In the transaction size case, it's unlikely that a new form of digital signatures will come around that Bitcoin would not be able to adopt through a softfork. For example, Schnorr signatures could be implemented in a whole new differentiated cryptocurrency, but it's also possible to integrate them into Bitcoin through a softfork.

In the block size case, Bitcoin's network will need greater bandwidth across the network and social consensus to support a block size increase. This is due to the fact that block size increases substantially reduce Bitcoin's security model; as fewer users would be able to independently validate Bitcoin's state, it becomes much harder for more people to be able to trust the currency itself. As such, there is a direct tradeoff that is constantly being made here by

all participants of the Bitcoin network: low bandwidth requirements and less throughput in exchange for enabling more users to run their own full node.

In the end, differentiation on the axes of transaction and block size would be marginal at best and would likely not be enough to usurp Bitcoin. While this form of differentiation could be useful, its costs to decentralization mean that it would not be enough on its own to overcome Bitcoin.

Monetary Policy

One of the most fascinating facts about Bitcoin is that it has a fixed money supply in the long term and its nth order effects on society. However, there is still some uncertainty with regards to how Bitcoin will function in a post-block reward world.

At this time, the game theory is out on what will happen as transaction fees start to take over as the chief subsidizer of the network. We don't have a good understanding of what the impact of Lightning Network will be, how users will behave and how miners will view the network in the future. While there may be problems a few halvenings from now, none of them can be addressed now by coming out with a new coin with a different monetary policy.

In the end, at this time there is little reason to experiment with this issue at this time. Although there are interesting discussions ongoing in this vector, at this time, there just isn't enough information available at this time for other cryptocurrencies to meaningfully differentiate on this axis.

Adaptability

For cryptocurrencies, adaptability is the ability of a cryptocurrency to make necessary changes to its protocol to protect itself. Another common term for this is governance, and it is critical to a cryptocurrency's ability to build trust and Lindy effect among its users. Hasu gets to the crux of the importance of governance in Unpacking Bitcoin's Social Contract: "You can agree you're in a terrible situation and you can agree you want to change it, but the resulting social contract is only as strong as it is credible. Without a stable institution to enforce it, a contract loses the trust of the people and falls apart." As such, creating a reliable adaptable systems could be a critical differentiation factor against Bitcoin.

In general, the tradeoffs of adaptability have to do with increasing upgradability in exchange for steadiness and conservatism of the rules within a system. In Bitcoin's case, governance is largely informal and bottom up, and

much of it occurs through BIPs. This process is covered extensively by Jameson Lopp in his article Who Controls Bitcoin Core? In the article, Lopp points out that Bitcoin develops more like a language does over time: "Languages emerge spontaneously; the consensus over the meaning of words is organic rather than dictated by dictionaries. Much as dictionaries describe the phenomenon of a language rather than define it, so do Bitcoin implementations describe the language of Bitcoin with code." As such, we can understand Bitcoin's adaptability to be very difficult to change singlehandedly, memetic based, and conservative. In exchange, it is much harder to force sweeping changes upon the network.

One popular method to counteract this lack of adaptability has been proposed is on-chain governance. Although potentially useful, on-chain governance does present challenges to cryptocurrencies. For starters, it is inherently anti-meritocratic. Those with large holdings of the currency gain influence over those with skill. For instance, imagine a world in which one group had exclusive control over Bitcoin's development. We might see constant work hash function changes (demanded by users who don't want to deal with those pesky ASIC manufacturers) or block size increases (which help miners and merchants in the short term at the expense of the health of the network). Instead, Bitcoin's far more meritocratic process of approving and rejecting ideas has been more effective and secure, albeit slow. Altogether, formal governance is directly antithetical to Bitcoin's goal of decentralization.

In addition, on-chain governance directly increases the attack surface of "corporate takeover" attacks where a group buys influence within the project. At a minimum, formal governance allows for lobbying for certain developments within the cryptocurrency, resulting in stakeholders picking winners and losers through the development of the cryptocurrency. Instead of letting ideas compete in the open, governance provides mechanisms that can be hacked by savvy parties. And as a result, governance presents political risks to the security of the cryptocurrency itself.

In their piece, A Conflict of Crypto Visions, Arjun Balaji and Yassine Elmandjra summed up Bitcoin's stance on formal governance: "Because the specifics of law and governance are complex and unknowable, the constrained vision opposes fully formal on-chain governance: implementation of "law as code" becomes heavily subjective and unlikely to account for the unpredictable changes in the real world." Essentially, it's impossible to know how or what governance will be used for in practice. As seen here, governance can be

viewed as an unnecessary introduction of politics to something that ideally would be void of politics in the first place.

That being said, formal governance does have potential for allowing for increasing the adaptability of a cryptocurrency. By providing a formal framework through which disputes are resolved, governance may help keep a community unified while allowing it to remain nimble. This can be tremendously helpful for a new cryptocurrency, especially as it tries to bootstrap trust among users in an attempt to compete with users' well established trust in Bitcoin. All told, by providing credible governance, a cryptocurrency accomplishes several critical tasks: first, it bootstraps its own trust within holders by elevating their importance above that of anyone else within the given cryptocurrency's ecosystem, second, it meaningfully differentiates itself from the informal governance king in Bitcoin, and third, it further integrates its technical and social systems, making for better adaptability.

Finally, it's worth noting that Bitcoin has demonstrated adaptability in times where the agreed upon social consensus rules were insecure in the short term. CVE-2010–5139, also known as the Value Overflow Incident and CVE-2018–17144 demonstrated that Bitcoin can make changes when fundamental aspects of its security are challenged. In a way, adaptability varies on a spectrum from security risk to upgrade profitability.

In total, adaptability, whether its through on-chain governance or not, presents a tradeoff between political attack security surface in exchange for upgradability and reduced forkability. It does not stop truly motivated forkers, and does reduce the meritocracy associated with debates in a cryptocurrency's community. As it stands today, Bitcoin dominates the informal governance axis of the cryptocurrency industry. Given that governance plays such a critical role in the social contract of a cryptocurrency, it will be interesting to see which cryptocurrency's governance systems prove to be successful in the years to come.

Ledger Assurance Model

This is likely the most meaningful way to differentiate against bitcoin. An idea invented by Permabull Nino in his article Assurances in Crypto, ledger assurance is the security and reliability guarantees generated through consensus mechanisms like Pure Proof of Stake, Proof of Stake + Proof of Work, and Bitcoin's pure Proof of Work along with its difficulty adjustment mechanism. It will be interesting to see what tradeoffs are uncovered in this

subfield of cryptocurrency because it is basically a currency's security model against double spending attacks.

To sum up the idea behind Permabull Nino's ledger assurance models: all monies can be summarized as ledgers that assure their users of their balance through accounting practices and respective legal systems. In the case of fiat, we have sophisticated accounting systems for individuals and businesses to keep track of their money and laws and regulations to help facilitate transactions between adversarial parties. Bitcoin provides people with accounting by allowing them to track their individual accounts through the blockchain, and provides mechanisms to transact through its digital signature system and Proof of Work. In sum, because Bitcoin provides significantly improved ledger assurances over fiat, it will eventually win the battle of monies. (Note, Murad Mahmudov discusses this idea in a recent RHR in depth. Link here.)

One popular ledger assurance model is Proof of Stake. Instead of rewarding blocks to the strongest worker, it rewards blocks to the strongest staker. As a result, Proof of Stake provides low energy consumption and complete finality. In doing so, it sidesteps two oft-cited criticisms of Proof of Work: energy abuse and vulnerability of having Proof of Work's game theory exploited. That said, there are drawbacks to Proof of Stake. It is naturally oligarchical and disposes itself towards technical and complexity problems. It is practically impossible to fair launch from scratch a Proof of Stake currency (i.e. either a Proof of Work bootstrapping period or long term ICO required). Additionally, given the variety of implementations of Proof of Stake, it isn't clear what Proof of Stake is at this time.

Another potential ledger assurance model could be a hybrid between Proof of Work and Proof of Stake. Such a hybrid would likely live somewhere between Proof of Work and Proof of Stake tradeoff spectrum. Again, given the variety in Proof of Stake implementations, it is unclear how such a currency would work at this time.

All this isn't to say this design space isn't worth exploring. As more information comes to light about the security of Proof of Work, alternative consensus models could provide better ledger assurance. For example, if it is determined that the economics of Proof of Work is doubtful, then another consensus mechanism might uncover tradeoffs to mitigate the issues with Proof of Work. If a superior model were to arise that provided Bitcoin-like guarantees and addressed any potential problems with Proof of Work, it's likely that cryptocurrency would compete strongly with Bitcoin.

Smart Contract	Privacy	Transactional	Store of Value	Governance	Level 2
POW | POW+POS | POS					Level 1

Everyone thinks you want the best of each category in Level 2. The reality is that you want the best of Level 1, as winning at this level creates a much larger "moat" - Level 2 can be conquered after Level 1. However - still not sure about standalone POS.

Differentiation at Level 1 will be much more interesting than other forms of differentiation. Source

Another important point worth acknowledging about this space is the importance of social scalability as a tradeoff within the ledger assurance model differentiation. As Nick Szabo writes in Money, Blockchains and Social Scalability, "the secret to Bitcoin's success is that its prolific resource consumption and poor computational scalability is buying something even more valuable: social scalability."

Proof of Work, and its counterpart, Proof of Stake, can be thought of as being on a sliding scale between social scalability and computational and energy efficiency. Where pure Proof of Stake is highly political and relies heavily on a wide variety of design choices, Proof of Work is objective, and whose only design choices involve the difficulty adjustment mechanism and selection of a hash function. On one hand, pure Proof of Work provides unlimited social scalability, and on the other, Proof of Stake or its introduction limits social scalability while gaining energy efficiency.

In the end, ledger assurance models are the primary drivers of trust within monies. And it is trust that ultimately matters in the competition of monies. Ledger assurance models confer finality and provide users with a sense of security. In addition, ledger assurance models must account for social scalability. In sum, because ledger assurance simultaneously involves building trust among users and allowing for social scalability, cryptocurrencies that heavily differentiate on this axis successfully will have a much greater chance of competing with Bitcoin.

Conclusion

At this moment in time, differentiating against Bitcoin is really hard. Barring a Satoshi level innovation in a new cryptocurrency model, there just isn't much of a justification to experiment with a vast majority of the cryptocurrencies available today.

Some differentiations like programmability, monetary policy and privacy present tradeoffs that provide marginal benefits to the core functionality of a cryptocurrency, but have significant downsides. At this time, Bitcoin dominates most of these tradeoffs by selecting for security and decentralization. In total, these differentiations can be treated as red herrings; easy on the eyes, but impractical in practice.

In the end, ledger assurance systems and adaptability may just be the axes along which cryptocurrency can differentiate against Bitcoin. At this time, it is unclear what the post block subsidy (and future) problems will look like, how to implement other ledger assurance models and hard cap monetary policy will tend to outcompete inflationary currencies in the short term. In sum, these two vectors present interesting fields of research through which cryptocurrencies can meaningfully differentiate themselves against the Proof of Work and organic governance king, Bitcoin.

Cryptocurrencies differentiate in the present through their governance and ledger assurance models, and over time by building liquidity, acquiring development and entrepreneurial talent, and increasing belief in their security. Ultimately, the long term differentiations take time and no one can come close to matching Bitcoin's Lindy-based security. And while all differentiations are linked, a new cryptocurrency will only be able to compete with Bitcoin in the immediate term by finding niches within the differentiations of ledger assurance and adaptability.

I want to shout out Hasu, Nic Carter and Murad Mahmudov. Conversations with them and their notes helped me write this article.

51% attack - apparently very easy? refering to CZ's "rollback btc chain"

How to make sure such corruptible scenario can never happen so easily?

Conversation from Peter Wuille, Greg Maxwell, Fernando Nieto

Posted May 11, 2019

Peter Wuille

I was shocked to see binance CZ comment to literally "roll back" the bitcoin chain by just "calling" in some favors from "friendly" Asian miners .

This ONE person could effectively do it??? I mean are we all in a bubble, in some kind of utopia then, to think that the chain's decentralization makes it "bulletproof" and resistant to collusion by miners?

(1) This is fundamental question: How are our highly regarded and brilliant Devs of bitcoin explaining such situation where only a handful of persons´ interests could essentially be enough to do a majority 51% attack?

(2) And secondly, are there active debates about how to mitigate such situation in the future, what technical aspects implemented in the btc chain (or to be implemented) could be helpful?

This huge mining farms are essentially very disturbing. it is like in proof of stake , where the "richest" has most power. And in the PoW mining case , its similiar just that the "biggest hardware" has most power.

we have to try somehow to eliminate such easily corruptible scenarios, right?

in todays digital world, there are plenty of collusion examples of even more than 1000 different persons involved.

Handful of colluding majority miners would be a piece of cake, right?

Thank you for explaining to me this issue . I hope sincerely that this is taken up by our awesome dev community, or maybe I am just misunderstanding everything.

Peter Wuille

Disclaimer: I believe this question may be primarily opinion-based and not very appropriate for this site, but there are a number of technical misunderstandings that can be clarified along with it, so I'll give it a shot.

There are many nuances involved here, and I fear that a large part of them didn't reach as much of an audience as the exchange announcing "we decided not to do it". I believe this was a poor choice of words, as the decision they made wasn't whether or not to roll back the chain; only whether or not to offer a bounty for doing so. I personally believe it would be very unlikely that the alternative would have actually resulted in a deep rollback.

Let's analyze the situation from a number of perspectives.

If we only consider miner's actions, is it theoretically possible for them to roll back the chain? Yes. If you're wondering if there is a small number of mining company CEOs in the world, which, if all together convinced, with complete disregard for their own financial interests, the health of the network, or legal repercussions, could decide to roll back the chain to a point before the theft, the answer is yes. This is the reason why people care about mining decentralization, and permissionlessness of entering the mining market. However, unless it's not just a majority of the hash rate that is on board with this, but actually close to all the network's hashrate (a substantially harder problem, as there are many small miners in addition to the few big ones), this would likely have take days or even weeks (if it's close to 50%), a time during which many things can happen - including a public outcry and a UASF-style fork to prevent the rollback from being accepted by the ecosystem. If considered over an even bigger timescale, events like this may even incentivize people and businesses to become miners, in order to reduce the influence of large pools.

Assuming miners maximize short-short term profit, would it be financially interesting to rollback? No. Even if we assume that everyone in the network is acting selfishly to try to maximize their own (short-term) profit, and ignores the protocol rules and the possible repercussions from doing so, it is not. By the time the information about the theft became known, the transaction was already confirmed several hours before. During those hours, miners had

created dozens of blocks, which together earned several hundred BTC in subsidy and fees. The exchange would need to offer at least that amount to the affected miners, to compensate them for the income they'd lose from rolling back those blocks, before it would even be worth discussing. Let's call this the rollback cost R. As the stolen amount was in the thousands (let's call this S), that seems like a reasonable option. However, nothing prevents the thief from using (part of) the stolen funds to do the same. Every BTC offered by the exchange above R can be countered by an equivalent amount offered by the thief. And then it becomes clear that the thief has the upper hand: the exchange can at most gain S-R by a rollback, but the thief stands to gain S by not having a rollback. A theoretical possibility is a bidding war between the exchange and the thief, where both increase the amount paid to make miners act in their favor. The end game of this is that the exchange offers S-R, the thief offers slightly more and keeps R, and miners are paid S-R by the thief, and no rollback happens.

What would happen in the real world? Theoretical models are interesting to study, but in reality many more practical considerations exist. I believe those too are generally in favor of no rollback:

- Coordination between distrusting miners (especially close 100% hashrate) is hard, and would take time. The more time it takes, the less advantageous a rollback becomes (see the above point), and the more damage would be done to the ecosystem (see the next point).
- An hours-long (in the very best case) or a weeks-long (in the worst case) rollback would monumentally hurt the ecosystem, and likely undermine the public's confidence in the system to the extent that it would severely reduce the profitability of many parties involved (including miners and the exchange itself!).
- Even ignoring all the above, miners may not be willing to take a bribe to rollback because of legal reasons if they're publicly known (which they mostly currently are). They may equally not want to take stolen money as a bribe, so this cuts in both directions. This point becomes weaker if the mining ecosystem is more decentralized, but that would also make coordination harder.
- As I pointed out above, in the extreme scenario where such a rollback is actually happening, the public has time to react. If a sufficiently large group of economically relevant parties in the network refuse to accept the rollback, miners have no choice but to go along with that. This is a last-resort option, and likely damaging to the ecosystem on its own, but it is an option.

So to summarize: in theory there are absolutely ways in which a rollback could happen, and it's good to be aware of those. In reality, the security of the system relies on economic incentives already which are nontrivial to analyze. It however seems very unlikely that in the case of a theft a deep rollback is a reasonable outcome.

Gregory Maxwell

You might want to elaborate on your short term profit formula to consider that R depends not just on the existing blocks but on the share of honest hashrate. E.g. In the simplified theoretical model R is infinite after confirmation with >50% hashrate honest. At just under 50% honest it's finite but much larger than the number of blocks that need to be replaced. Only at 0% honest does R equal just the cost of blocks that need to be replaced. Coordination challenges alone assure that some hashrate would behave honestly.

Gregory Maxwell

(adding some color) Some discussion I saw suggested that people promoting this believed they only needed to achieve >50% hashpower, which caused them to overestimate the feasibility. Reorging with only slightly over 50% would take weeks– even months, creating massive disruption if successful, and virtually guaranteeing an effective public initiative to block it. In such an event once the rollback began, users would advise each other to use the 'invalidateblock' debugging command to make their nodes ignore it. [I also had multiple users ask me to review patches ahead of the fork that would have blocked it, I told them I thought they were over-reacting and that this was a nothing burger. :)– but a patch would only be needed before a fork existed, and clearly people were ready to start responding to this only on the basis of twitter chatter]

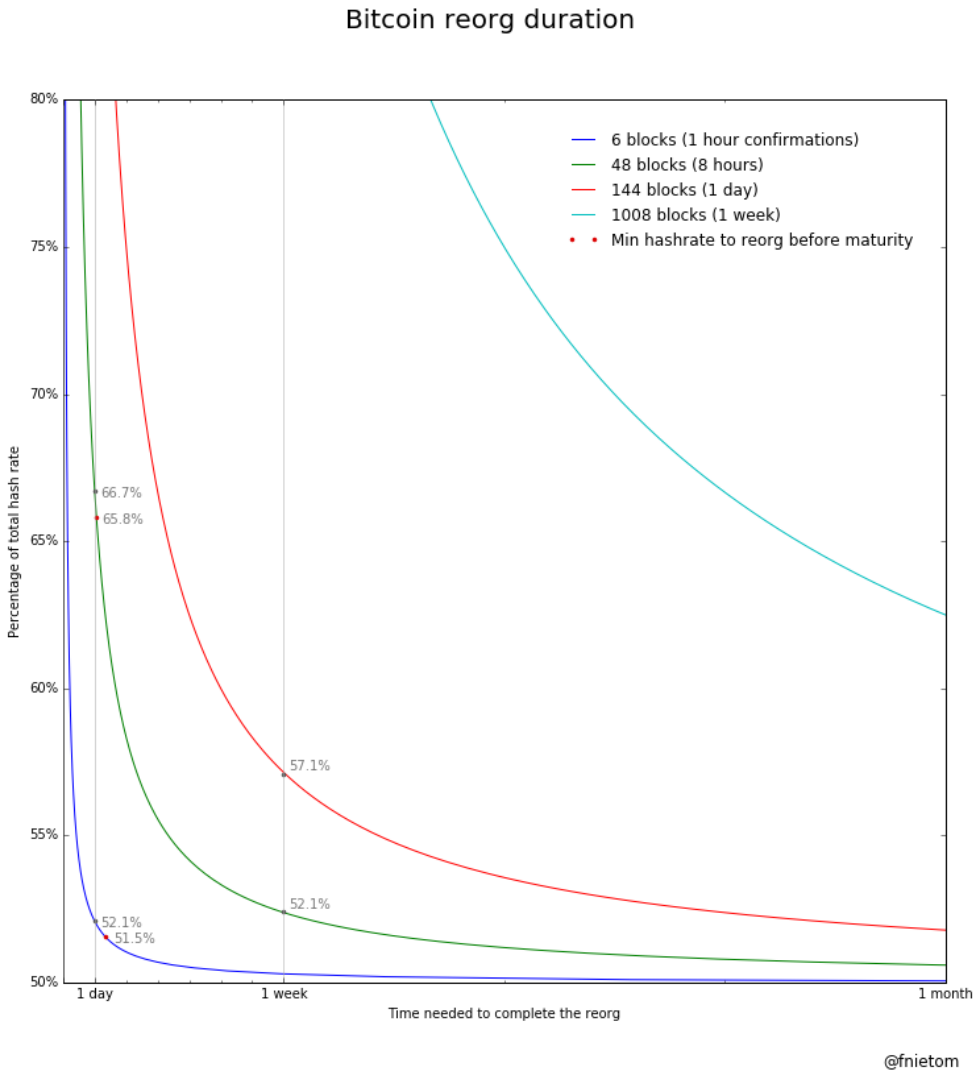
Fernando Nieto

here a are a few things to take into account when we consider the probabilities of a reorg to be successful:

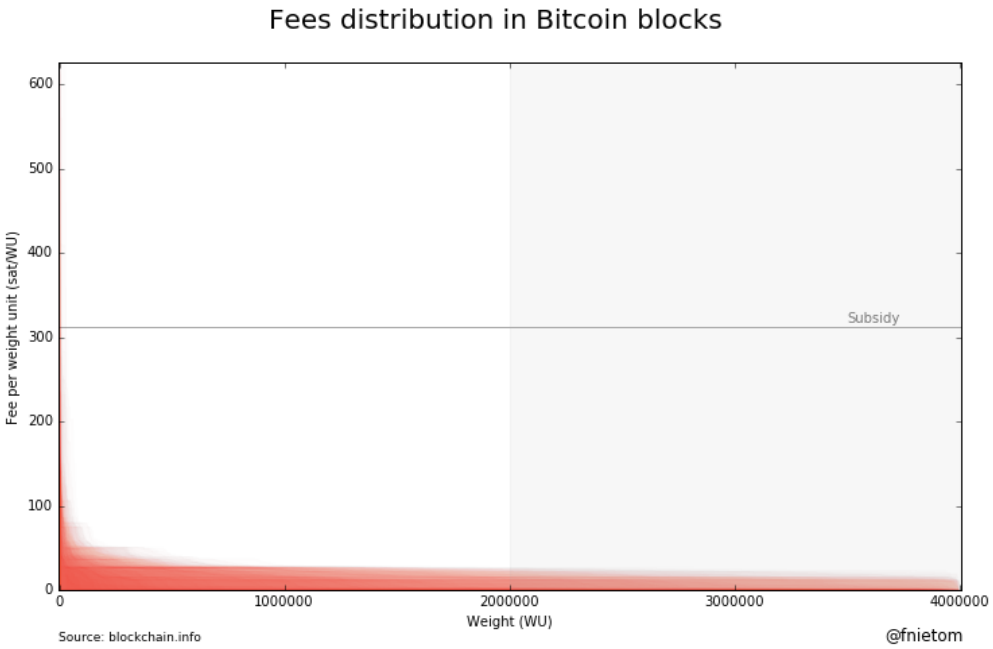
1. If the reorg is shallower than 100 blocks (COINBASE_MATURITY), the attacker can minimize the amount of direct victims. But if we are talking about a deeper one, not only the payments he wants to revert

may have been spent, mixed with other inputs and all those coins owned by other innocent people, this would also apply to coinbases earned by honest miners. The longer it takes to perform the reorg, the higher the amount of victims and their value at stake.

2. The attack may take a long time. The fraction of miners participating (via direct control or bribes) and the amount of blocks to revert will determine how long. For example, to revert just 6 blocks (1 hour worth of confirmations) before coinbases start maturing, the attacker will need to get immediate control over 51.5% of the hashing power. If he falls short of that percentage or requires more time to convince some of the miners, it will take him over 33 hours and reverting more than 100 blocks in total, so rewards from the first blocks may have been spent already.



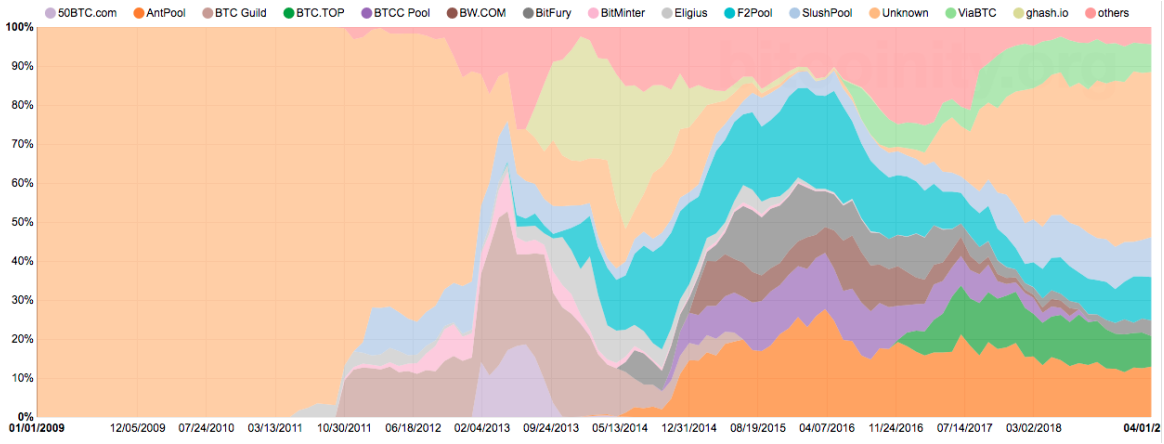
3. If the attack uses existing mining capacity, during the time it takes to reorg the chain, the capacity on the longest chain would be reduced to less than half of the usual capacity. You can expect this to have an impact on fees and miner rewards, as the offer for transaction confirmations is not able to satisfy demand users will have to fight for the reduced space available. Higher rewards on the honest chain will put additional pressure on miners carrying the attack. It's difficult to predict how high they can go in the middle of all that FUD, with many people rushing to move coins to trade. enter image description here



4. A significant reorg doesn't affect just direct victims, every bitcoin holder would be affected due to a diminished confidence in the system, a reduction in Bitcoin utility and a drop in the price of the coins as a consequence. PoW is a trust-minimized market signal enabling us to scale social consensus. But, if somebody builds a heavier chain with a lower value, breaking PoW trust-minimization, users can choose not to follow it and make a UASF, invalidating the reorg:
5. `$ bitcoin-cli invalidateblock "blockhash"`
6. Coins in both chains are only as valuable as their chances to become part of the winning one. Miners coordination, unusually high fees in the longer/honest chain and UASF risk during the reorg attack are all factors against reorg-coins having as much value as those in the honest chain. This makes even more challenging to use reorg-coins to bribe miners.

How can we make reorgs even more difficult? @LukeDashjr provided the first two of these ideas, that would help us achieve stronger immutability:

1. If users set individual checkpoints in their nodes, this would discourage reorg attempts and split the chain if one happens, leaving it for market to discover the value of each chain when PoW consensus assumptions break down.
2. Use pool swapping rule introduced by BFGMiner to prevent miners from wasting work on stale blocks. If one pool implements a reorg policy (even if it is trying to earn bribes), miners will refuse to ditch previously validated blocks and switch to a pool working on the newest block.
3. @TheBlueMatt's BetterHash mining protocol would have a similar effect, making practically impossible for mining pools to enforce an ordering of transactions, hence removing their ability to censor some of them.
4. The more independent miners, the more difficult it will be for anybody to coordinate them and try to 51% attack the network with existing mining capacity. Currently over 40% and growing.



Cryptocurrencies & Their Effects On Monetary Policy

By Deniz Özgür

Posted May 14, 2019

Abstract

The programmable economy is a natively “smart” economic system that supports and/or manages the production and consumption of goods and services, enabling diverse scenarios of exchange of value (monetary and non-monetary). Beyond the hype, beyond the expectation lies a digital future ahead of us with great speed of adaptation both by individuals and the institutions. This report briefly explains blockchain and how cryptocurrencies work; examines pros and cons; mentions some of the most powerful implications on financial institutions and potential effects on monetary systems; and lastly announces technology projections and predictions of research companies.

What is Blockchain ?

An insane contradiction and confusion lead people to become quite radical about distributed technologies. Depending on who you ask, blockchains are either the most important technological innovation since the internet or a solution looking for a problem. Here is the definition of blockchain: A blockchain is a decentralized, distributed and public digital ledger that is used to record transactions across many computers so that the record cannot be altered retroactively without the alteration of all subsequent blocks and the consensus of the network. But what does this really mean? Let’s break this definition down. First, a digital ledger is a digitalized collection of transaction records. When something is “decentralized and distributed,”

there's no central service center or supercomputer hosting and storing these records. Rather, the records, or digital ledger, are separated, or distributed, into millions of identical copies and on different machines (known as nodes).Second, "public" means that the digital ledger is open to the public, as opposed to being held by a particular entity. This also means that all the machines or computers in the blockchain network have access to add transactions and update all the copies on other machines. In a 2017 Harvard Business Review article, Marco Iansiti and Karim R. Lakhani define blockchain as *"the technology at the heart of bitcoin and other virtual currencies,"* and *"an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way."*

Towards Bitcoin

There is this misconception that blockchain and crypto currencies came out of nowhere. Originally built upon some strong economical, philosophical and technological concepts, even though 2008 is known to be a milestone, digital currencies have 30 years of past starting from Digicash (1989) enabling users to make untraceable, anonymous transactions. It was perhaps too early for its time. Later that attempt, history has witnessed E-Gold (1996), which was a digital currency backed by real gold. The company was plagued by legal troubles, and its founder Douglas Jackson eventually pled guilty to operating an illegal money-transfer service and conspiracy to commit money laundering. That acquisitions never seem to put out the fire because only 2 years later in 1998 B-Money and Bit-Gold was developed by two famous cryptographers Wei Dai (B-money) and Nick Szabo (Bit-gold) each proposed separate but similar decentralized currency systems with a limited supply of digital money issued to people who devoted computing resources.

Economic Crisis & Bitcoin

What didn't kill us literally made us stronger. A devastating crisis for the world economy resulted in massive unemployment and market collapse. But what were the factors which led us to rethink the economy? Let us look at a few:

1. Selfish Interest of Banks: The investment bankers, traders and executives took excessive risk without proper market study. They just wanted to drive in profits, without pondering on the ways in which it could be done. The risk to reward ratio did not fit, but they took the chances anyway. The bonus culture prevalent that time led the bankers to sell as many products as they could. They did not focus on building a

long-term relationship with their customers. The Incentives and Bonus which came with each sale clouded their judgment. Loans were issued to even poorly rated credit borrowers. These were the people who had a bad reputation in the market regarding repayment of loans and handling their own finances. The bankers were only focused on giving out loans, and thus even the bad elements got involved in the process. Securitization of high-risk assets was done. Also, these securities were kept off the balance sheet. Investors took a heavy risk in these securities. But perhaps they were not really aware of this, thanks to the credit rating agencies. The bankers chose sales targets over sustainability. There was a difference in interest.The role of credit rating agencies is to give information on riskiness, safety and quality of securities issues. Some of the very famous credit rating agencies were handling this job for the big banks these days. Now they had incentives on giving ratings to these securities. In order to develop positive sentiments, they gave a positive score to even very high-risk securities. Perhaps they had realised that none of those securities was of any value, but they had to look at their own profits as well. This led to the banks issuing more securities and investors taking the risk.

2. Lack of Financial Education: Another very important factor was the lack of education among the masses. When loans were issued, the interest rates used to be low. In time these rates changed and the people who took these loans could not understand this variation. The new interest rates were higher than what they were initially asked to pay. When borrowers realised they could not pay their loans at these rates, they defaulted. Even the bankers did not fully understand the terms and conditions of the deals they made and the risks they took. One classic example would be the Housing Bubble which popped and many banks went into bankruptcy.
3. Monetary Policies and Lack of Regulation: Monetary policies are what determine the interest rates and the circulation of currency which

influence the economy as a whole. Many individuals mortgaged at a certain interest, and when these rates rose, they defaulted. The regulations were not so strong, particularly in the US and the banks were free to do what they wanted. Glass-Steagall Act was introduced in 1933 after the Great Depression. This Act led to the separation of commercial banking and investment banking. Prior to this, both the functions were carried under the same roof. The Act was revoked before the 2000s and the banks returned to their old ways. Commercial banking and investment banking was merged again, leading to banks taking greater risks. It was a careless gesture which led to the doom of economy. In conclusion, this chain of continuous negligence and concession has shaken the trust to central authorities as well as any intermediaries. It made people question the economic mechanism which intuitively was the responsibility of government and central bank. Just like when discussions on separating politics and religion took place a hundred years ago, now it was time to have individual sovereignty on money management. What is even more noteworthy, people started to become more aware about their financial ignorance and even blamed the education system.

“Those crashes, these bailouts, are not accidents. And neither is it an accident that there is no financial education in school. [...] It’s premeditated. Just as prior to the Civil War it was illegal to educate a slave, we are not allowed to learn about money in school.”— Robert Kiyosaki”

Without Policy, No Control! How Does It Work?

There are three main concepts Bitcoin and most of the following crypto currencies are built upon: Decentralization: There is no central entity governing the system. Every participant of the network contributes to keeping it alive. This removes security holes, because even if a single, big party gets hacked, the other members of the network aren’t affected and the overall system recovers. Shared memory: A record of all transactions between all parties on the blockchain is stored on every computer in the network. Forever. And everyone can see it. This makes the

network secure against fraud and data loss. Cryptography: Through a set of complex algorithms and math problems, all transactions and participants are protected by encryption. There are tradeoffs between these features and different projects interpret them in different ways, but in the end, these three elements are what defines not just Bitcoin, but all blockchains. When it comes to Bitcoin in particular, the combination of these blockchain features serves two core functions: storing value and enabling direct, financial transactions from one user to another. These functions are part of any working currency, Bitcoin just aims to make them better.

1. Trustless Transactions In a government-issued currency, the trust that enables you and me to exchange $1 bills at constant value is delegated to the government. We hope no matter what happens, the government will make sure we get our $1 worth of goods. Whether that's an apple today or a car in 50 years, no one knows. When we process money through banks, we trust that the government has trusted in them to extend that guarantee, and so on. "The Bitcoin network enables that same 1-on-1 transaction power at constant unit value, minus the governments and the banks." Every user has an individual address, like a bank account you use today. It keeps a balance of how much value in Bitcoin you have and enables users to send money from one address to another. What's different is that users don't need the bank and can still expect the transaction to be secure. They don't even need to know each other. Hence the 'trustless' part. You don't need to delegate trust to any third party in order to exchange value for currency and vice versa.
2. Storing Value The way a government can guarantee a dollar will always be interchangeable for another dollar is by backing the sum of all dollars with a massive amount of assets. While governments do own a lot of those—land, real estate, landmarks, national treasure, and tons of commodities, like gold—their number one asset is that they can print the currency at will. It's called inflation.

Bitcoin's "supply formula"

Bitcoin tackles this need by more directly copying the economic model which has evolved around gold. The two are often compared because both have a limited supply. As with gold, it gets harder to create, that is mine, new Bitcoins over time. While nobody knows exactly how much gold is still to be discovered, the maximum supply of Bitcoin is detained in the open source code: 21 million coins, over 17 million of which have already been mined. The last Bitcoin will be created around the year 2140. With a fixed supply of money, but an infinitely growing population of humans, demand is bound to outpace supply sooner or later. In fact, it already has, which is why the price of Bitcoin has exploded so much. If population growth stagnates at some point and everyone uses Bitcoin, the price might stagnate too. But as long as it doesn't and more people keep joining the currency network, the price goes up. That makes holding Bitcoin a great store of value for those, who have some.

"Bitcoin's value proposition is not digital currency—90% of existing money only exists as digital currency; Bitcoin's value proposition is its methodology in guaranteeing the trustworthiness of digital currency."

How About Fractional Reserve Flexibility?

Talking about value, one should remember how arrangeable money supply giving a useful flexibility to the central banks. What has been called expansionary monetary policy, quantitative easing or fiscal stimulus to the economy all refers to that clever tool but almost instinctively hides the meaning from society to cover the obvious intervention. Godfrey Bloom, addressing the European Parliament during a joint debate, said it way better than I ever could:

"[...] you do not really understand the concept of banking. All the banks are broke. Bank Santander, Deutsche Bank, Royal Bank of Scotland—they're all broke! And why are they broke? It isn't an act of God. It isn't some sort of tsunami. They're broke because we have a system called 'fractional reserve banking' which means that banks can lend money that they don't actually have! It's a criminal scandal and it's been going on for too long. [...]We have counterfeiting—sometimes called quantitative easing—but counterfeiting by any other name. The artificial printing of money which, if any ordinary person did, they'd go to prison for a very long time [...] and until we start sending bankers—and I include central bankers and politicians—to prison for this outrage it will continue." Don't get me wrong: There is nothing wrong with making economical arrangements. There is nothing wrong with fractional reserve banking if having entire authority also means to have the responsibility to take the controlling action. There isn't even anything wrong with good old regular banks to store your wealth somewhere more secure than in your sock drawer. However, what has been proposed here is basically a self-controlling, living mechanism which sustains perfect information opportunity among the voluntary participants.

Grandchildren Of Bitcoin: Altcoins

Following the success of bitcoin, there have been more than 1630 (according to Coinmarketcap data) other cryptocurrencies created, they are collectively called “Alt Coins” since they serve as an alternate of bitcoin in the digital currency world. The main motivation of their core developers was to advance Bitcoin’s flaws such as scalability, the amount of energy and time consumption during its transaction verification process which is called Proof Of Work. Not without mentioning, those reasons keep people to develop applications, generate use cases and more importantly, evolve their businesses with distributed technologies. In 2011, an important question was arisen: What if your set of ideas does not overlap with Bitcoin’s? What if you wish to change Bitcoin’s set of ideas, not convinced of the futility of this endeavor? What if you are downright repulsed by some of its ideas? Criticising the obvious weaknesses of the old father, who will take the throne instead? Those who wanted to change Bitcoin’s ideas in a fundamental way, draw their own path which is called forking in software ecosystem. With forking, Bitcoin’s open source code, permissionless network structure, and lack of formal organization of any kind was basically allowing anyone to copy, modify, and run the code without asking for permission. Although most of the projects failed to generate a unique approach to Bitcoin and their set of ideas necessarily overlaps with it; in most cases they were almost the same.

New Term Has Arisen: CryptoEconomics

As more and more networks and alt coins came alive, theories and models are needed to understand the issues facing contemporary communities. Crypto-economics as a discipline is an attempt to create models that allow

the analysis of interrelationship in increasingly complex frameworks of human interaction in distributed systems. Most commonly accepted public blockchains are a product of crypto-economics. The term “Crypto-Economics” has been defined in several different ways. Most commonalities in definitions for the term crypto-economics include the use of cryptography and incentive design to created networks, applications, and systems. Further, crypto-economics is interdisciplinary. We already know economics examines how individuals and groups respond to incentives. Connecting it to traditional economics, crypto-economics is mostly associated with mechanism design, a sub-discipline of economic theory and mathematics. Crypto-economics is what makes blockchains interesting, what makes them different from other technologies. As a result of Satoshi’s white paper, we have learned that through the clever combination of cryptography, networking theory, computer science and economic incentives we can build new kinds of technologies. These new crypto-economic systems can accomplish things that these disciplines could not achieve on their own. Blockchains are just one product of this new practical science. Blockchain networks are in need of economics especially with the incentives listed below, which exists in every blockchain but in various shapes:

1. Tokens: The actors who actively participate and contribute to the blockchain get assigned cryptocurrencies for their efforts.
2. Privileges: Actors get the decision-making rights which gives them the right to charge rent. Eg. Miners who mine a new block become the temporary dictator of the block and decide which transactions go in. They can charge transaction fees to include transactions within the block itself.
3. Rewards: Good participants get a monetary reward or decision-making responsibility for doing well.
4. Punishments: Bad participants have to pay a monetary fine or they have their rights taken away for behaving badly

With those incentives, some obvious subfields of economics are adapted through cryptographers. As we almost always see economics, supply and demand curves are also very popular here as well. Deciding on the total supply of the coins (or tokens), their releasing mechanisms, burning strategies (to withdraw the money from the market) with the ultimate goal of creating a self-organizing living organism which serves as an economic environment with participants fully informed and motivated. Soon after, digital currency design required people to study game theory to search for the motivations of the contributors and built the action-result mechanisms.

Nodes (devices in the network representing individuals), miners and authorities (if any) are expected to behave on their best interests while never sacrificing the maintenance of the network. Free and competitive market mechanisms is replicated in public blockchain systems while private chains give priority to institutional organization and authority delegation. If crypto economics of a network is poorly designed or executed, individuals have every right to shift towards a greedy strategy. In order to widen the perspective of building the perfect maintenance for participant one should consider the subjects of economics that are listed below:

1. Game theory
2. Mechanism Design
3. Consensus Mechanisms
4. Network Effects - Behavioral Economics
5. Governance - Political Economics

Investment In Blockchain Technology

A technologic phenomenon has never given that much priority to finance and economics. Not because designing consensus systems strictly requires economics, but because allowed millions for open market investments. Thousands of people flocked to the cryptocurrency markets hoping to catch the hype occurred in October 2017. They have learned investment tools before learning the blockchain itself. Fraud-Proof characteristics of transactions, transparent ledgers, borders trade opportunity, lack of regulative dominance, scarce coins, seamless development of technology and high adaptation rates lead to a bubble for 5 months and resulted inevitable loss afterwards. On the bright side, attracted attention never goes away and that hyped is rather perceived as the true potential of an egalitarian cyber movement. Blockchain history, at that times, witnessed the transformation of a traditional funding method called IPO (Initial Public Offering) into ICO (Initial Coin Offering) which offered international funding framework for those who expect high ROI with enchanted growing and marketing potential in an unregulated environment to avoid taxes. While some of the leading blockchain startups today are the products of those ICO’s, 95% of them were scam. Cryptocurrency investment, no matter how volatile it is, has madly expanded throughout the years of spreading from ear to ear. Leading cryptocurrency exchanges already started to dominate the market even though their level of security and objectivity is still questioned. Binance, the biggest exchange founded in 2017, has been hacked in May 2019

and 7.000 BTC is stolen. What is even more interesting, CEO offered to reorganize the chain to rollback before the hack and almost for a week people sharply criticized him daring to manipulate the network. With the increasing costs, CEO took a step back and apologized but that incident remained some solid questions behind: How safe are we? How come the strongest exchange is that helpless against hacks? Eleven years after 2008 and are we still missing something? Those, we won't be able to answer in near future.

Cryptocurrencies: The Future Ahead

The most debated topics today in blockchain space has much to say about what lies in future. Any comment about the upcoming years should be investigated through three main problems: volatility, scalability and competition against incumbent money's network effects. Starting with the volatility hurdle, this is one of the most talked about issues with cryptocurrencies. High volatility is bad because it prevents a cryptocurrency from being a good unit of account or store of value. As we know from the economics, this feature is compromised by definition from high volatility. This is bad because if the volatility of a money is very high then the agent who accepts this money as payment runs substantial financial risk from the volatility, this overall makes the money in question far less appealing for real world agents. One potential solution is the hope that as cryptocurrencies become mainstream and secure user adoption, they will become stable in the markets themselves. This we call "maturity dampening effect". The argument often given for this thesis is as follows:

"Cryptocurrencies are still infant technologies. There is high uncertainty about their future use and adoption, hence, high volatility is entirely natural because small updates in market information will cause large shifts in market expectation. Once the dominant cryptocurrencies emerge and become adopted by all those who will use them, they will reach a saturation point which will make their price become more stable." Another solution is the creation of stablecoins, cryptocurrencies that have volatility reducing design

structure built into them. A stablecoin that relies on using USD or another currency as its unit of account would be a far less revolutionary outcome than that of a real independent cryptocurrency. Another issue is scalability. At the moment all decentralised cryptocurrencies cannot scale effectively because of the current technology limitations. By scale effectively people mean increase the amount of transactions by a large magnitude with negligible effect on speed of transaction and cost of transaction. The difficulty in large part comes from the cryptocurrencies who choose to stand by the commitment to decentralisation of the network with a permissionless blockchain. Many cryptocurrencies such as XRP have managed to scale effectively, however, this comes at the cost of a centralised network. That bears one questions: Since we only manage to scale the network with centralized structures, will the institutions dominate blockchain and use it for their benefits? Community surely resists that idea. Lasly, cryptocurrencies are definitely competing against the network effects of incumbent moneys. Money is only useful if enough other people accept and use it. It is one of the most classical examples of network effects—the greater the number of participants the more valuable the network (normally increasing in a non-linear fashion). Therefore, motivations behind cryptocurrency adaptation should be investigated. One reason why a cryptocurrency might be used instead of something like the dollar, is if there was a large scale financial crisis. For instance, if the dollar itself was called into question because of large government debt, then there may be a wide enough fear of national fiat that cryptocurrencies are turned to as alternatives. However, this would be then leaving the hope of powerful network effects to be established by apocalyptic events. Another reason for higher adoption might be from an ideologically motivated reason whereby people feel cheated by the current system and seek to try out of it by using cryptocurrencies. However, the practical cost of such an ideological position will be significant, buying groceries, getting paid all become much harder. Aside from this, the other option for cryptocurrencies might be to offer money for specific use cases, such as being used for the internet of things, or as an alternative to remittances rather than the all encompassing use cases that current currencies have. Some of these 3 challenges for current and future cryptocurrencies feed into each other. The uncertainty of any one cryptocurrency's acceptance in the future makes it hard to gain a large network, and this in turn makes it more volatile. The technical issues of scalability may reasonably be overcome. However, without the power of a government to help create a monopoly which is how most of money over time has been created, some of these challenges may prove to be insurmountable.

Conclusion

Bitcoin is is the marriage of economics and computer science; a digital deflationary currency and ledger run on a decentralised network, which was launched to replace the current inflationary fiat system, following the 2008 economic crash. Surely an economic phenomena rather than a technologic one with the consideration of mechanism design and incentive arrangements are at the heart of this innovation. The interpretation of blockchain as an experiment field for economics would even clears the doubts and fears out of the way which encourages economists to lead and take responsibility of bringing their open market theories into life. With abilities like control and flexibility, they are allowed to design replicable systems with millions of participant who have defined roles and incentives and more importantly economists can come up with real industry solutions. We should definitely get involved, definitely be decentralised.

Sources

- Accenture, “Tech Vision 2019: DARQ Power”
- Deloitte, “2018 Global Blockchain Survey”
- Deloitte, “Tech Trends 2019”
- Gartner, “Forecast: Blockchain Business Value”, Worldwide, 2017–2030
- https://www.forbes.com/sites/ginaclarke/2019/01/18/tech-trends-2019-what-do-blockchain-experts-make-of-beyond-the-digital-frontier/#4a0d211e114c
- https://www.idc.com/getdoc.jsp?containerId=prUS44898819
- IDC, Worldwide Semiannual Blockchain Spending Guide, 2017H2
- James Wester & Stacey Soohoo, IDC, “Blockchain:Worldwide Technology Market Update and Spending Outlook”, 6 Eylül 2018
- PwC, Building block(chain)s for a better planet
- PwC, A prescription for blockchain and healthcare: Reinvent or be reinvented
- https://blockgeeks.com/guides/what-is-cryptoeconomics/
- BIS Annual Economic Report (2018). Cryptocurrencies: looking beyond the hype (91–114)

Bitcoin's Security is Fine

Fears over the declining block reward are overblown

By Dan Held

Posted May 15, 2019

Published Block: 576165

Foreword

This article is part of a new series called "The On-ramp" by my company Interchange where we explore topics and ideas in crypto that financial institutions should know and understand. For those who don't already know, Interchange is a middle to back office accounting solution for crypto companies (ex: fund admins, OTC desks, fund managers). I'm one of the co-founders, and my role is business development, sales, and marketing. If you're interested in hearing more about our product, please feel free to reach out via our intake form.

TL;DR—This article comprehensively addresses concerns around Bitcoin's security model which is funded by the block subsidy and transaction fees. Key points:

- The larger the Bitcoin network grows, the more secure it becomes.
- Over the long term, an organic security tradeoff will occur between the block subsidy and transaction fees. As network effect becomes larger, demand for block space increases, thus decreasing the need for a block subsidy. We have empirical evidence that this is occurring, and future projections look optimistic.
- Bitcoin's block space is a scarce and unique commodity. It will continue to accrue demand.
- The bull market of 2017 wasn't millions of consumers suddenly using blockchains to transfer money around the world and seeking to minimize transaction, exchange, volatility, and coordination fees.
- The price elasticity of a Bitcoin transactor is high. Even in significantly higher fee environments Bitcoin block space demand will grow.

Block Reward

Approximately every 10 minutes, a new Bitcoin block is created, which contains newly minted Bitcoins (the "block subsidy") plus transactions (which includes transaction fees paid by the entity sending the transaction). The value of the newly minted coins plus transaction fees is called the "block reward."

Per Bitcoin's hard coded monetary policy, the amount of newly minted coins per block decreases over time, eventually reaching 0% in the year 2140 (also known as a disinflationary model). At the time of this article being published, over 83% of all Bitcoins that will ever exist have already been minted, and the current annual inflation rate is just 3.8%. Over 99% will be mined by 2040.

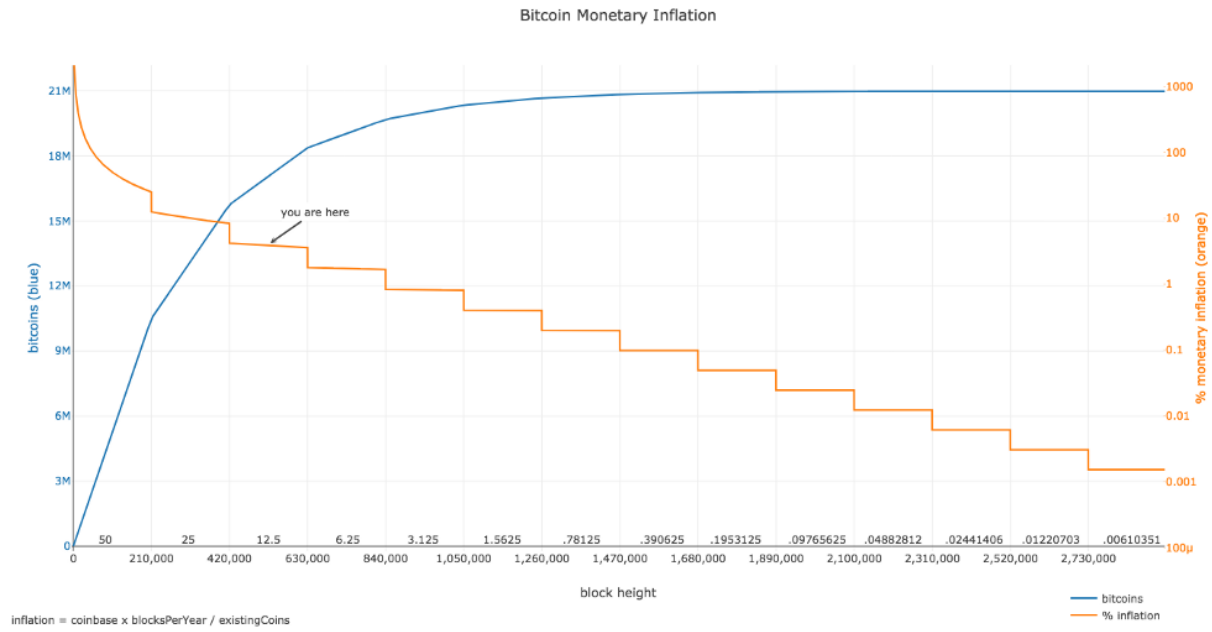
"Indeed there is nobody to act as central bank or federal reserve to adjust the money supply as the population of users grows. **That would have required a trusted party to determine the value, because I don't know a way for software to know the real world value of things.**If there was some clever way, or if we wanted to trust someone to actively manage the money supply to peg it to something, the rules could have been programmed for that." — Satoshi Nakamoto

Satoshi felt that setting a "proper" rate of inflation rate was impossible (due to the local knowledge problem) and that it introduced a political attack vector, so he decided to remove human decision making from the process. Each time monetary policy is changed or modified, human governance re-enters the system nullifying the certainty of monetary supply. This ultimately leads to less social scalability increasing the risk of network fragmentation and disagreements. A predictable monetary policy is key: Bitcoin's focus on long-term stability and transparency creates confidence for investors and developers.

In other words, the fixed monetary policy in Bitcoin effectively and directly addresses a property rights problem: Without a hard supply cap it becomes uncertain what share of the total future stock any particular holder owns; as a result, variable supply policies almost always dilute individual ownership shares of money over time. Because supply caps solve this property rights problem, then those currencies tend to have increased value.

I won't spend more time diving into Bitcoin's monetary policy, as I consider that a separate topic which requires an article exclusively (which I will be releasing sometime in the next few months).

So why does this matter? The block reward incentivizes miners to protect the network. As inflation trends towards zero, miners will increasingly obtain an income only from transaction fees. Some worry that transaction fees alone won't provide adequate compensation for the miners. In storing large sums of wealth, security and trust are critical.



https://plot.ly/~BashCo/5.embed?share_key=ljQVkaTiHXjX2W41UiqzCn
Created by BashCo

Bitcoin's Security Model

"In a few decades when the reward gets too small, the transaction fee will become the main compensation for [miners]."—Satoshi Nakamoto

Bitcoin's existing UTXO set (ledger) and new blocks are protected by game theory and physics. Bitcoin uses proof-of-work (PoW) to make changes to the ledger difficult, which eliminates trust and introduces an external cost for any would-be attacker. The miners buy hardware (capex) and electricity (opex) with the expectation of receiving their portion of the block reward based on work spent (hashes). The block reward financially incentivizes miners to behave properly.

As the price of BTC increases, the value of the block reward increases as well, which incentivizes miners to bring more hashrate online to mine. The higher the hash rate of a cryptocurrency network, the more expensive to 51% attack.

The security budget protects the network against 51% attacks which primarily occur on the tip of the blockchain, rather than an entire chain rewrite, which would require significantly more resources.

In the early stages of the network, Bitcoin miners are rewarded more heavily by the block subsidy than transaction fees. With Bitcoin's disinflationary monetary policy, approximately every 4 years the block subsidy drops by 50%. This creates both volatility and a price increase: if demand remains constant (or increases), the reduction in supply means demand is chasing less freshly minted Bitcoins hitting the market. This effect brings in new speculators, which is part of the beauty in its design, as the supply shocks bring greater awareness to Bitcoin.

"As the number of users grows, the value per coin increases. It has the potential for a positive feedback loop; as users increase, the value goes up, which could attract more users to take advantage of the increasing value."—Satoshi Nakamoto

While the two represent the same security budget, the block subsidy and transaction fees are very different. For the block subsidy, its value is both as a rational way to issue new Bitcoins and as a viral FOMO loop built into the protocol, which increases the number and network effect of believers in Bitcoin. It further stretches out the need for transaction fees to solely provide security. Hence why it's called a "subsidy."

Over the long term, an organic tradeoff will occur: as network effect becomes larger, demand for block space increases, thus decreasing the need for a block subsidy. While we don't know why Satoshi chose Bitcoin's issuance schedule specifically, we can speculate. Four years between halvenings is a long time to plan and build. In similar duration, we give a US President four years to make things happen for an entire nation.

With modeling done by Awe and Wonder we can see that around the year 2030 transaction fees will begin to consistently represent a healthy portion of the block reward. When transaction fees represent greater than 50% of the block reward for long periods of time (YoY), Bitcoin evolves to surviving more on transaction fees.

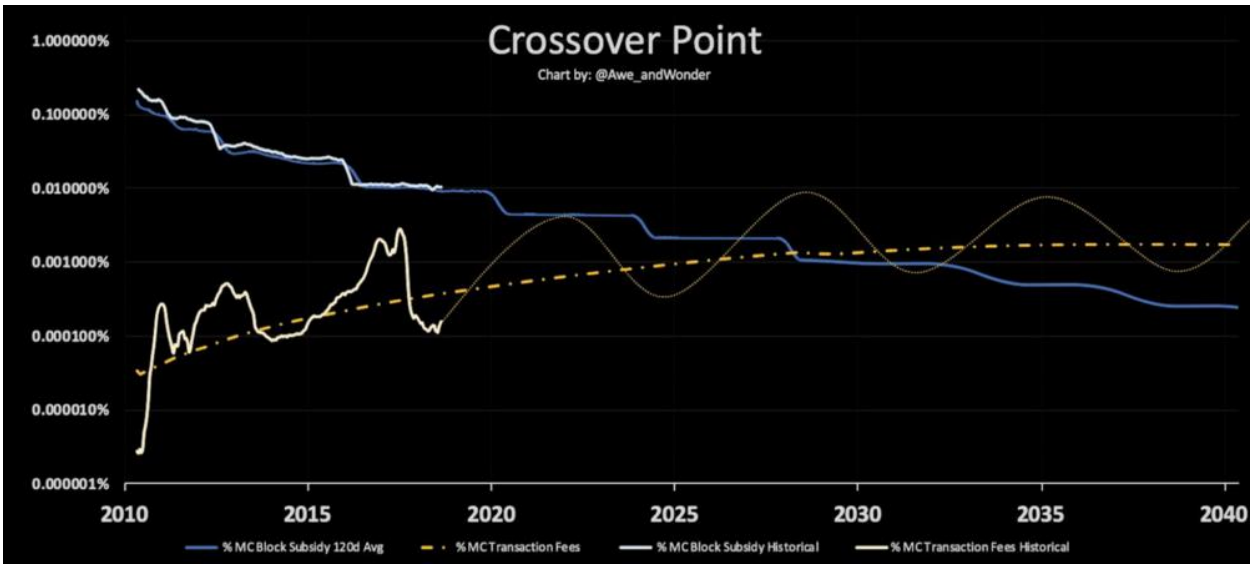


Chart and projections by Awe and Wonder

Critics often argue that transaction fees alone won't provide adequate security. But what is an appropriate security level? This is highly subjective since the amount of confirmations one would wait for depends on the transaction size and health of the network. However, despite the subjectivity, we should make an attempt to calculate it. At the MIT Bitcoin conference, Nic Carter presented several ways we could quantify an adequate security budget:

Threshold: At a given level of security spend, Bitcoin is assumed secure

Stock: Security spend should be indexed to the value of Bitcoin itself

Flow: Fees must be large relative to transactional volume

I personally believe security is best measured as a percentage of stock which eventually reaches a threshold level. Stock makes more sense than flow

because miners will increasingly be focused on long term operations as ASIC efficiency diminishes. Eventually, this reaches a threshold level that will be extremely difficult to disrupt by even the most wealthy states.

I hypothesize several hundred billion, in present value USD, would be an adequate security budget since it would be very difficult for a government to justify such a waste of an expense to just 51% attack the tip of the Bitcoin blockchain. They would also have to respond publicly for such an attack as their citizens (taxpayers), businesses, and banks will all be invested in Bitcoin.

Note that a 51% attack wouldn't "kill" Bitcoin, as you still cannot reverse historical transactions easily, the effort of which is calculated here.

"This may also increase the value of the fee market as demand to move Bitcoin should increase, creating more incentive for non-attackers to service the fee market"—Neil Woodfine

Finally, in the absolute worst case scenario of a sustained 51% attack, the thing that must be preserved is the UTXO set (ledger). If SHA256 must be abandoned, so be it. In that case, Bitcoin could fork onto a different mining algorithm that already has an established market—rendering all nation state mining equipment invalid. I want to be clear, this would be a last ditch effort, and by no means guaranteed to succeed, but the simple fact this could occur may dissuade a nation state from trying such an attack.

It's important to note that PoW achieves other goals than just minimizing 51% attacks, and increasing network effect, it also ensures that money is provably costly to create (Unforgeable costliness).

Bitcoin's block space is a scarce and unique commodity

There is no alternative to prime real estate

Getting a transaction mined can be seen as purchasing a portion of a block. By analogy, on average every 10 minutes, a fixed amount of land is created, people wanting to make transactions bid for parcels of this land. The sale of this land is what supports the miners even in a zero-inflation environment. The price of this land is set by demand for transactions because the supply is fixed and known. The basic premise is that if the network is being used/valued then it will reward miners for validation/protecting the network.

Some argue that altcoin block space is an equal substitute. However, there are many ways we can debunk that theory. Bitcoin real estate is prime real estate (ex: it doesn't matter how cheap land is in Midland, Texas, it'll never have the views or social network of San Francisco and therefore will have less

demand). The unique value of Bitcoin's block space is due to **security**, **exchange**, **volatility**, and **coordination** costs.

This following section borrows heavily from Donald McIntyre 's article " Observations About Paul Sztorc's Bitcoin "Security Budget in the Long Run" Essay " (I have his permission to use large directly quoted sections without quotations so the article could have more continuity)

Security costs: Bitcoin is the most secure cryptocurrency network due to the total accumulated hashes (energy). This will create a market for high value, highly secure transfers in Bitcoin, e.g. central banks, governments, interbank, corporate and other large value payment users, who will gladly pay very high fees. There is also a security feedback loop as other chains borrow Bitcoin's strong security by making on chain transactions, as we've recently seen with Veriblock.

Exchange costs: When senders and receivers want to store value in Bitcoin, but need to transfer them, there is friction to move from BTC to an altcoin, send it for a lower fee, and then pass it back to Bitcoin on the other side. Between exchange commissions (0.1–4%), spreads (since alts are less liquid), and transaction fees both ways, there will be an indifference point beyond which it will be better to pay for Bitcoin fees. If Bitcoin is a very good store of value, transfers will occur within Bitcoin precisely for the same reason it is a good store of value.

Volatility costs: Often people forget to consider volatility costs which depends on your holding period **.** Altcoins typically have higher volatility than Bitcoin which has the nasty effect of scaling with transaction size. A hypothetical example:

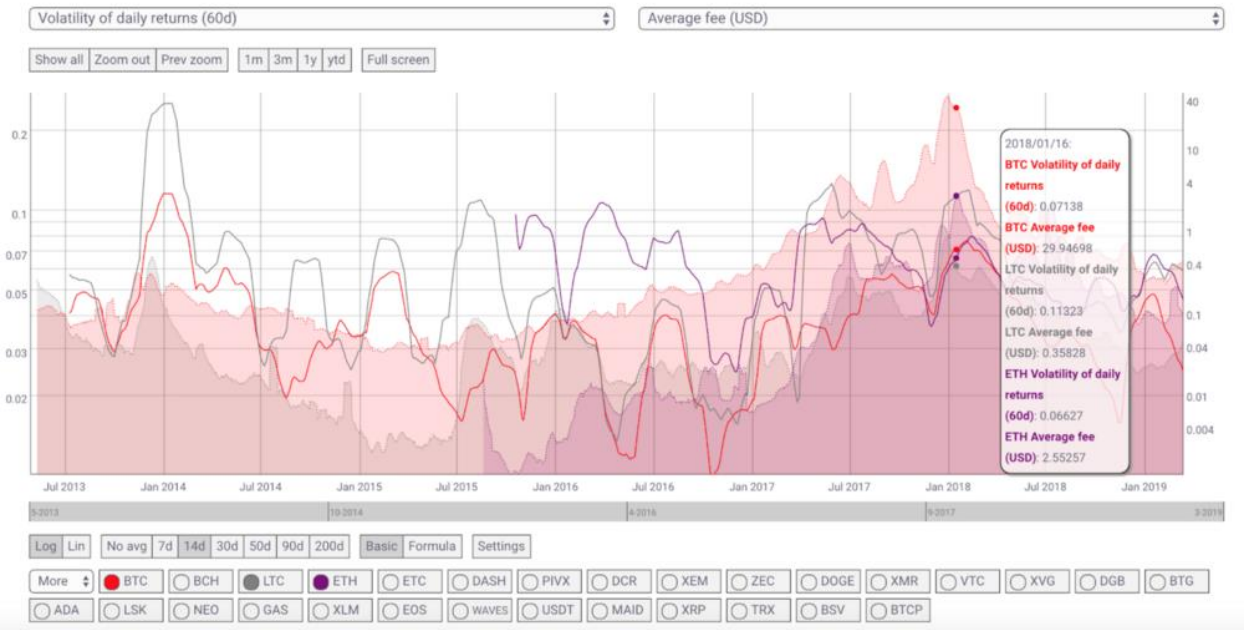
LTC: $10 payment + 10% vol + 0.01 fee = $1.01

BTC: $10 payment + 1% vol + 0.20 fee = $0.30

LTC: $100 payment + 10% vol + 0.05 fee = $10.05

BTC: $100 payment + 1% vol + $1.00 fee = $2.00

While Bitcoin fees hypothetically increased 5x, the volatility loss on LTC made the transaction fee ~ $10! Conversely, even if you make money on the volatility, you still will have to pay capital gains. Below is a chart which shows average fee and volatility for BTC, LTC, and ETH. Unfortunately, without an average individual holding period for multiple coins, it would be difficult to calculate the average cost of volatility.



Coordination costs: Not all coins will survive. There will be a limited competing block space market in the world. This is because our minds are limited and we will not think about 250 cryptocurrency names, transfer fees, the subsequent 250 prices, and go about selecting the cheapest one each time we move value (@NickSzabo4). Our brains will only support understanding the value of 2 to 3 coins at most, and we will be comfortable using them interchangeably up to a certain point (although there is a weak/unproven case to be made for obfuscating a plethora of coins behind proper UX/UI). Additionally, since Bitcoin HODLers have a strong affinity to only transact in Bitcoin (monotheistic), multicoiners will be forced to transact in Bitcoin (Tyranny of the minority). For example: Square, Bakkt, and Fidelity are only supporting Bitcoin at this time.

Finally, the Bitcoin core software is battled hardened with a mature ecosystem. This adds value to Bitcoin's unique block space since there are more developers and businesses that examine and rely on Bitcoin's code.

"Bitcoin is money. Multicoinery is barter."—Conner Brown

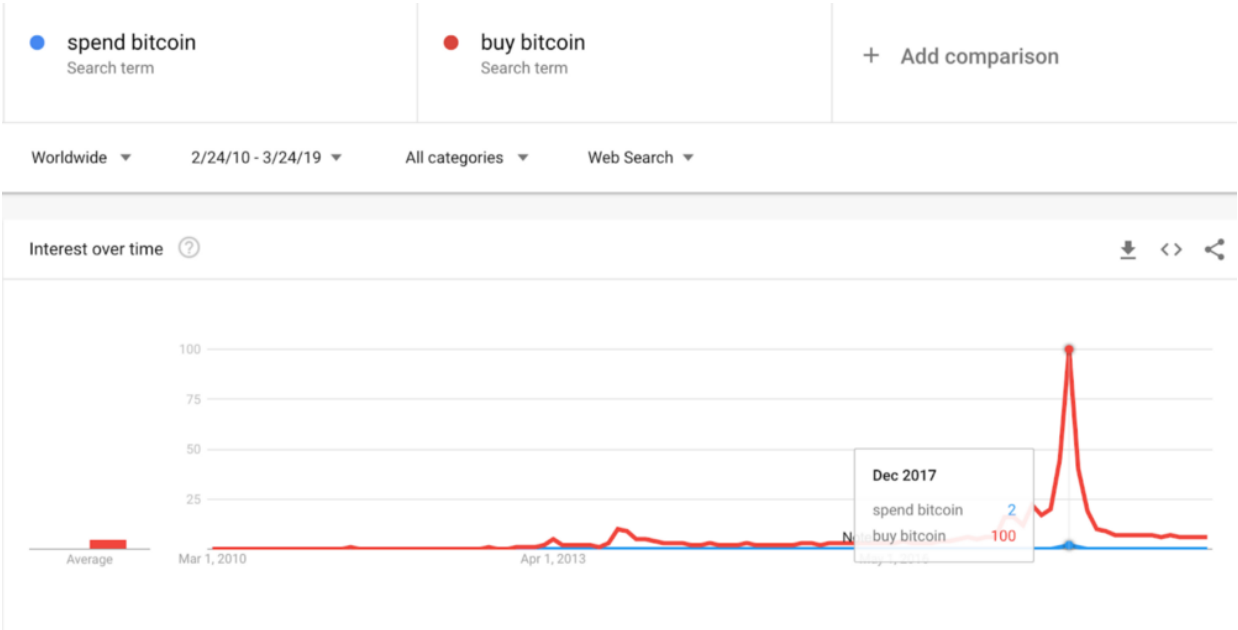
With all of these considerations above, there will be a limited amount of coins in the future, with a limited amount of block space and transaction capacity. This means that the cost of sending value will be distributed between the surviving chains in proportion to value and safety requirements. But in the end every altcoin is offering a lower security model with a higher risk.

"If one chain becomes the most secure by far, why would the majority of wealth and valuable apps not be secured by it?As more users buy into more

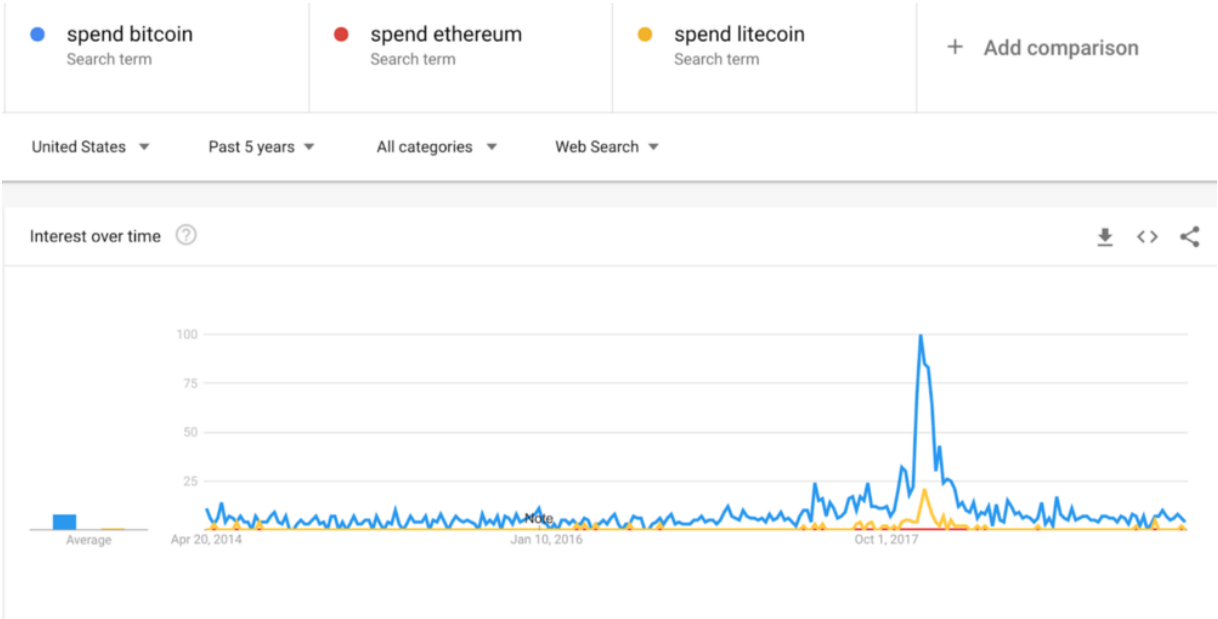
secure chains, their buying pressure will push up the price. The increased price will lead to increased security. From there, eventually usage, liquidity, and network efforts will compound on each other. These most valuable and secure chains should then be used to secure the most wealth and valuable dapps. Less valuable blockchains with the same security model of their more expensive counterparts will become less and less used as the gap in security grows. Sidechains, layer 2 systems, etc. will make the 'differentiating features' of alternate chains less and less relevant."—Alex Sunnarborg

"The sudden multiplication of altcoins and ICOs during the last bull run was a race to mimic the wealth creation that happened in Bitcoin. **It was not millions of people suddenly using blockchains to transfer money around the world and seeking to minimize those fees**. In other words, the coincidence of altcoin and ICO proliferation with the 2017 crypto bubble was a generalized gold rush (we were all trying to find gold/SoV) but not a rational pricing dynamic and arbitrage of block space through transaction fees."—Donald McIntyre

Although I have little data to back this statement up (and it's quite subjective), I think a large portion of payments were likely done for novelty. Paying for something with crypto is harder, more expensive, and slower than traditional payment methods. After all, Bitcoin's base layer is for building the strongest possible foundation for a new global monetary system–not creating another Venmo.



(If I had used the query "bitcoin" then "spend bitcoin" didn't even register on the chart)

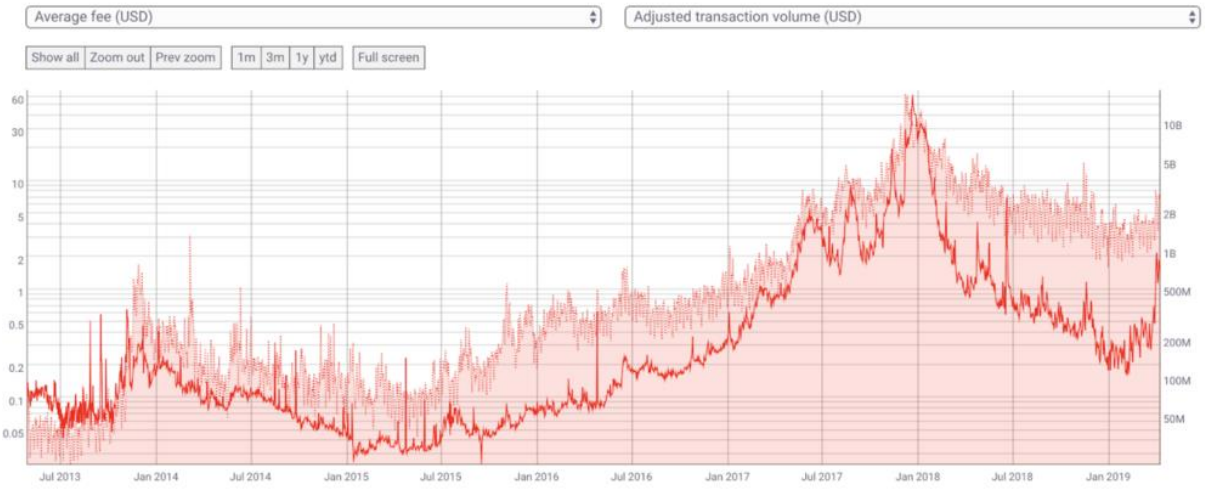


(Users aren't looking to pay for items with any cryptocurrency, otherwise we would have seen an up trend despite the price volatility)

Transactional Demand

"I'm sure that in 20 years there will either be very large transaction volume or no volume."—Satoshi Nakamoto

Another worry is that as fees become higher users will shy away from transactions to avoid fees. However, we've seen empirically this is not the case: as transaction/trading volume has increased, fees follow in step.



(log)

Price Elasticity

"Nobody goes there anymore. It's too crowded."—Yogi Berra

Consider the user experience for most North American, European, and Asian consumers/businesses (the majority of crypto participants). In most cases, any transaction fee has a higher level of friction than existing payment methods, so any fee is deemed "expensive" (vs cash or credit card).

"Think of the fees like insurance. You're paying for security."—Ari Paul

The price elasticity (for fees) of a Bitcoin transactor is largely due to the nature of the payment type being sent, an immutable SoV. During the point of highest congestion in 2017, the median fee was $38. And during that time period, we briefly saw blocks with fees being greater than the subsidy. For comparables we can look at cost of transacting a SoV:

Wiring Fiat

For US banks, the average domestic wire fee is **$30–40, and $65–80** for international (both incoming and outgoing fees combined).

Offshore ($7T Market)

"The **setup fee for opening an offshore bank account is between…. $1,935 to $3,745 for**[a bank account and an entity filing]"—Offshore Banking Primer

Real Estate ($250T Market)

"Buyers from **China bought 40,400 units totaling $30.4 billion between April 2017 and March 2018. They spent a median of $439,100 per purchase**"—National Association of Realtors

Average closing costs on a home are 2% of the value, or $8,000. I'm sure individuals will be fine paying $50 in the future to send an immutable payment with an asset that can't be easily taken away from them (unlike real estate which could be seized in a geopolitical quarrel at the snap of a finger).

Physical Gold Delivery ($7.5T Market)

Donald McIntyre requested information from the Bundesbank regarding their NY Fed transfer of 300 metric tons of gold ($12 Billion at the time) from NYC to Frankfurt. **It took 3 years and cost $4.8 million.**

With smaller sizes, gold delivery may require insurance, verified shipping, or physical protection during pickup/delivery, etc. Estimated to be around $10-$100 at a minimum.

Increasing Transactional Density

Nic Carter's MIT presentation highlighted two ways to improve transactional demand: increase economic or semantic density of transactions. Semantic Density is about having other blockchains imbed their data into the Bitcoin blockchain, like Veriblock. Economic density is about increasing transaction types on Layer 1, which are the following:

Privacy

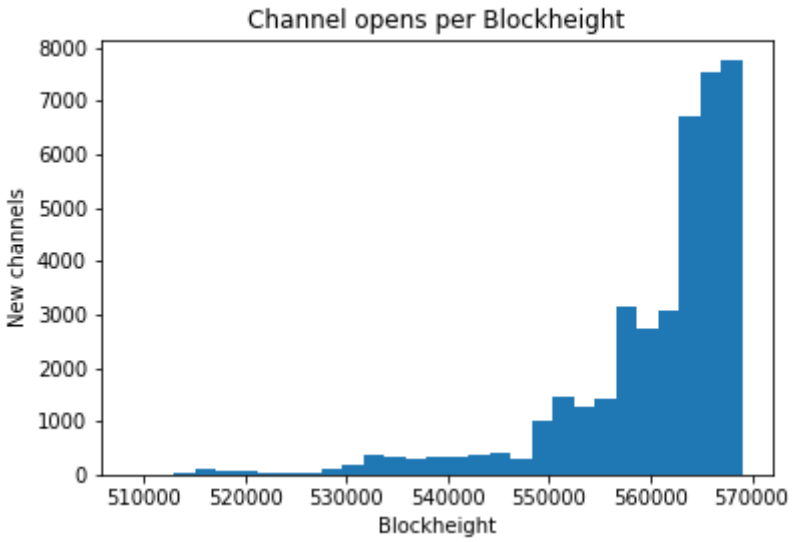
"Schnorr can enable the creation of new transactions types that break the heuristics widely used in blockchain analysis, and make it nearly impossible to pinpoint specific entities by simply looking at the blockchain while simultaneously allowing greater transaction density per block by aggregating signatures."—Lucas Nuzzi

Layer 2 (ex: Lightning)

As Bitcoin scales (Schnorr on Layer 1, Lightning on Layer 2, etc), it will become more and more efficient, driving higher on-chain usage. Jevon's Paradox intuitively predicts this—as cars have become more fuel efficient, more miles are driven annually. Layer 2 will support a massive number of cheap smaller transactions, whereas Layer 1 represents a more expensive settlement layer for large transactions (container ships vs cargo containers—Nic Carter). LN boosts on-chain fees by increasing the utility of each on-chain txn (by allowing each to do the work of many txns), and by therefore making high on-chain fees more tolerable to the end user.

As businesses and Lapps are built around the Lightning network, a big part of their opex will be channel management. That will ensure constant demand for Layer 1 settlement as these operators rebalance channels and optimize connectivity & capacity. On-chain, block space is premium, hence transactions are charged for the space it takes to register the transfer. Off-chain, liquidity is premium, hence transactions are charged for the amount being transferred over the channels (as it requires rebalancing). In other words, on-chain and off-chain transactions have different fee models that complement each other. On-chain, the fee is constant despite transaction value, whereas off-chain the fee is priced as a percent of the value transfer. There is a crossover point where high value transactions cost more to use on Lightning than Layer 1.

We've already seen evidence that Lightning is increasing layer 1 usage, even in its highly experimental form. There was a block created in February 2019 which was 25% full with lightning transactions to open a channel. This was detectable because Lightning uses the SegWit malleability fix, all LN channel opens are SegWit transactions.*



"The nodes in the lightning network gossip information about which (public) channels exist in the network, including a reference to the funding tx, which we check to make sure the announcement is real. Which is an underestimate as there are also some number of private/unadvertised channels."— Snyke

Quantum resistance

"The adoptionof quantum resistant techniques will also result in larger (and more expensive) transactions. Post-quantum crypto algorithmsrequire larger key sizes, which in turn increase the size of non-witness data in a transaction."—Lucas Nuzzi

Overall

We have empirical evidence that total fee revenue will slowly trend up to equal the block subsidy in the coming decades. Based on this data, fears that the transaction fee won't replace the block subsidy are definitively overblown.

The chart below shows transaction fees as a percentage of the block subsidy.

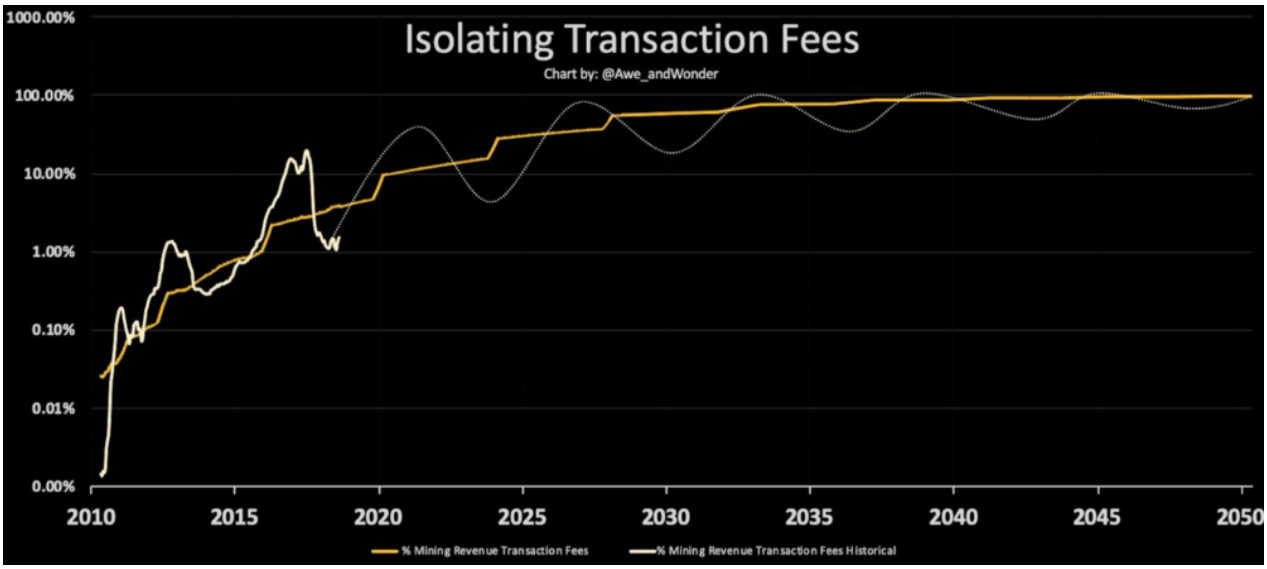
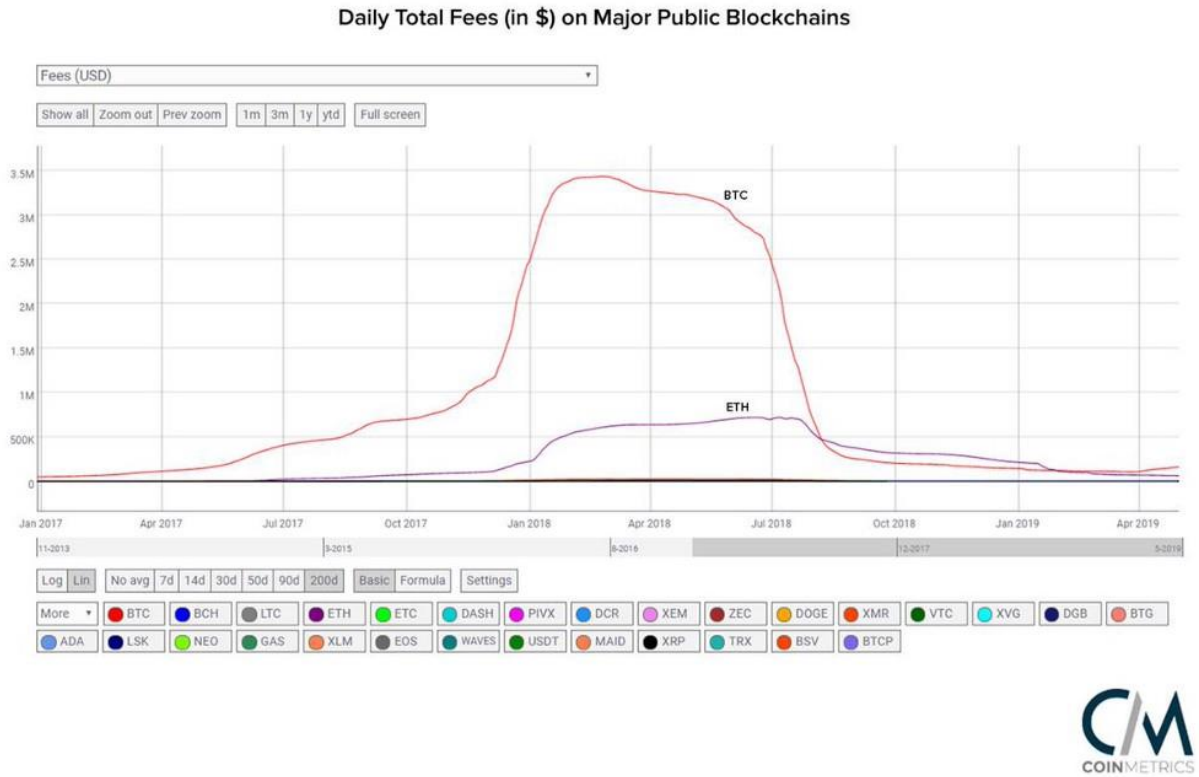


Chart and projections by Awe and Wonder

As Alex Sunnarborg pointed out, only Bitcoin and Ethereum have meaningful enough transaction fees to compensate miners in a no inflation environment. It is very unlikely that any other network will be able to compete.



Data from CoinMetrics, Chart initially compiled by Alex Sunnarborg

Security Stability

"The volatility of fees, which seem to behave nonlinearly as blocks become full. Might lead to corresponding big swings in hashrate."— Nick Szabo

Scarce block space is a good thing since we will see a backlog of transactions, which demonstrates future intent to reward miners, which in turn stabilizes the system. Congestion in 2017 demonstrated that the system can create and sustain a backlog.

A legitimate concern is that in a pure transaction fee security model, there will be volatility in cash flows. Transaction fees are market-centered, meaning that they go up and down adjusting to supply and demand. The base assumption is that cash flows from transaction fees will be unstable which makes the network less secure. Dan Mcardle sums it up nicely:

"As mining becomes highly commoditized with mature corporations, miners are unlikely to play short-run games, but will rather choose to mine continuously. Taking this further, as miners will likely vertically integrate with other services (ex: OTC) that become additional profit centers (meaning they're not as concerned about the possible games to play on a block-by-block basis)"—Dan Mcardle

Miners like stable cash flows, hence why they join mining pools. They don't play short term games trying to win a block, they socialize the winnings.

Given the worst case scenario where mining fees are unstable, it doesn't actually undermine the system, it just makes settlement time longer until fees grow large enough for mining to turn back on. Entities, by necessity of time preference, would increase fees in response, countering.

Moreover, the subsidy has already been incredibly volatile in real terms over the past few years and mining has remained strong and constant–even with 80% drawdowns in the value of the subsidy. This "instability" has not affected the network and mining will continue to become even more resilient to large swings as the market continues to mature.

In the future, miners might auction space in future blocks in advance which could have a stabilizing effect on their revenue (the same way farmers sell crop futures). The basic premise is that if there is increasing usage of Bitcoin, the free market for future block space will price it correctly.

Finally, if this is a major issue that isn't corrected by the market naturally, there are minor changes we can make in the protocol to smooth fee revenue.

However, this would make the base protocol more complicated, and the game theory behind it hasn't been adequately explored. For example:

"Other longer term low subsidy era ideas include fee averaging across block intervals to smooth fee revenue."—Adam Back

Modeling Security Post Subsidy

What do transaction fees in a post block subsidy world look like? I built a model that would help us think through what they might be in the year 2140 (in today's dollars), with a few necessary assumptions that you can view for yourself below. In its most congested state in the year 2140, a transaction on layer 1 may only cost between $8—$82 depending on Bitcoin's market capitalization. Transacting on layer 1 will be an infrequent occurrence for most consumers, just like wiring money.

$10T Market Cap

Fee Calculator (Post Block Reward)	
Year	2140
Hyperbitcoinization Market Cap	$10,000,000,000,000
Layer 1 Block Size Increase	500%
Layer 1 Efficiency Increase	40%
Annual Mining Rev as % of Market Cap	0.3650%
Annual Miner Revenue	$36,500,000,000
Layer 1 TPS	140
Layer 1 Median Transaction Fee	$8.27

You can play around with the model here if you'd like to plug in your own assumptions.

$100T Market Cap

Fee Calculator (Post Block Reward)	
Year	2140
Hyperbitcoinization Market Cap	$100,000,000,000,000
Layer 1 Block Size Increase	500%
Layer 1 Efficiency Increase	40%
Annual Mining Rev as % of Market Cap	0.3650%
Annual Miner Revenue	$365,000,000,000
Layer 1 TPS	140
Layer 1 Median Transaction Fee	$82.67

You can play around with the model here if you'd like to plug in your own assumptions.

Assumptions

Hyperbitcoinization

Bitcoin survives, thrives, and continues to grow in market share exponentially, as it has done the last 10 years. I've chosen Bitcoin's max market cap in hyperbitcoinization value to be between $10T (value a bit higher than gold) and $100T, which has been a popular estimate for bulls. To put this value in perspective:

Total wealth in the world: $750T

Real Estate: $225T

Fiat: $50T-100T

Gold: $7.5T

Block size

Block size is constrained by latency, bandwidth, and storage. Without fundamentally changing how packet routing works, or advancing speed of transfers improvement in latency, picking a growth rate just based on bandwidth or storage increases isn't the correct way to look at it (Another consideration with latency is usability with Tor). We have to look at the issues with larger blocks size holistically.

Certainly, a larger block size would alleviate some of the explicit fee pressure felt by transactors (thereby decreasing public scrutiny by ill-informed critics,

and perceived "cost" for transactors). However, that offsets the cost onto node operators, simultaneously decreasing decentralization in some manner, which is what makes Bitcoin valuable in the first place. Also, this increases mining pool centralization. What level of centralization is allowable is a continuing debate in the Bitcoin community.

There is a case to be made for a market mechanism that would compensate node operators. For example: prompt relays, transaction data, SLAs, etc. However, it is mostly theoretical at the moment.

If a rate of block size increase is decided on, it should have a decreasing growth rate (similar to Bitcoin's inflation rate). Otherwise, we are going to have to agree to softfork a smaller limit in later, which is the exact opposite of the position we want to be in. Some research has shown that 8MB might be the largest block size possible without material detrimental effects.

And finally, there have been some discussions around decreasing block time, which would provide the ability to further increase block size.

Layer 1 Efficiency

With Schnorr signatures (soon to be implemented), it is estimated that this upgrade would reduce the use of storage and bandwidth by at least 25%. We can assume some additional efficiency gains will occur over the next 120 years (Taprooft/Graftroof on the immediate horizon).

In the chart below, we can see that transaction fees as % of market cap trend towards a little above 0.001% daily over the next decade. Even with the continual decline of the block subsidy, total mining revenue (ie security) has increased exponentially as Bitcoin gains further adoption.

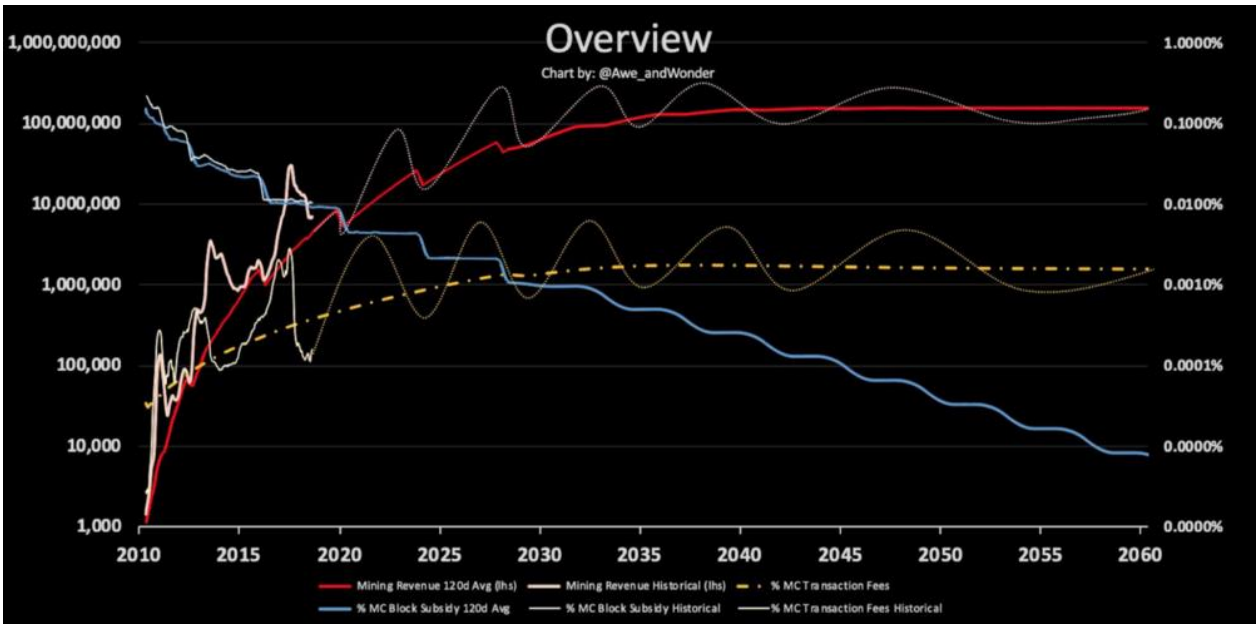


Chart and projections by Awe and Wonder

TPS

Assuming that current Layer 1 is 20 TPS max w/ Segwit. TPS depends on the byte size of the transaction but I had to choose a value to build the model.

Flawed Potential Solutions

Proposals for increasing the 21M hard cap, or "unlocking" dormant coins, aren't appropriate to bring up at this stage for three reasons:

- Lack of evidence that the decreasing block subsidy will be an issue
- The divisiveness of the ask due to its ethical tradeoffs
- More palatable fixes if there is an issue at least a decade from now

Conclusion

I've addressed what an adequate level of security could be, Bitcoin's prime (and unreplicable) block space, transactional demand, what happens when the subsidy runs out, and security stability. We have empirical evidence that there will be proper security budget financing will equilibrate through fees. The tradeoff is always between inflation (block subsidy) and fees and Bitcoin is the best positioned to charge fees reliably. If there is no economic (transaction) volume in 10 years bitcoin will have failed anyway.

Most well-pedigreed critics predicting doom and gloom used absurd assumptions in their models. Conversely, Cypherpunks write code.

Satoshi was essentially an academic that wrote production code, and published working models in the environment first focusing on practical implications.

His experiment, Bitcoin, has worked for 10 years despite an intensely hostile environment—all data indicates we have reason to believe it will continue to thrive.

Lightning at the End of the Tunnel

Overcoming Bitcoin's UX Challenges

By Roy Sheinfeld

Posted May 14, 2019

(Sources: pixabay & publicdomainpictures.net)

The Lightning Network is laying the ground for bitcoin to take the next giant leap in its evolution. Instead of just being an asset for HODLers', bitcoin now has the speed and economy to become a universal currency. We stand before the threshold of mass adoption.

The only thing holding bitcoin back is the UX. Raw technical possibility is not the same thing as an attractive, engaging, useful experience for all users.

But UX is a small term that hides great complexity. It implies many issues for which there are many solutions, each with advantages and disadvantages that different users will value in different ways.

For all their differences, we can assume that all users want at least one thing: simple functionality. Any viable solution must do its job simply and efficiently, so the complex technology has to operate seamlessly in the background. Perhaps the best measure of a UX is the gap between the utility it delivers and the complexity it manages to hide.

Here we take a look at the various challenges that remain in implementing the Lightning Network as a global payment solution for bitcoin and the different ways existing and impending technologies can overcome them.

Challenge #1: Zero Configuration

If the primary UX goal is to spare users complexity, the right amount of effort they should have to devote to configuration is zero, none, nada.

Autopilot

Lightning Labs has developed the autopilot feature to reduce the difficulty of configuring a Lightning Network wallet. Autopilot scans the network to determine which routing nodes are actively managing their channels' liquidity and recommends them to users.

The idea is to connect new users with the most active routing nodes on the assumption that they will provide the best service. Just like a 24-hour ATM usually provides a better UX than a 6-hour bank teller, active routing nodes should provide users more connectivity and payment flexibility—other things being equal.

That's a good start, but plenty of complexity remains. For one thing, users need to fund their own channels. Second, if a user funds a channel herself, she can send those funds down the channel, but she won't be able to receive funds until she has made some transfers. Third, users will have to fund a number of channels for adequate connectivity.

Lightning Service Providers (LSPs)

LSPs are basically network hubs. Just like ISPs, they make it easier for users to connect to the network.

In the language of autopilot, an LSP is just a routing node that recommends itself. As an active partner in its users' payment channels, the hub can spare users some further configuration hassles. For example, Breez funds users' channels with inbound liquidity, letting them receive bitcoin over the network immediately. Bitrefill's Thor service works similarly. LSPs are one big step closer to zero-configuration.

Centralization is not a concern with LSPs because a number of them exist already (with many more to come), so users can connect to several. In fact, Breez will soon allow users to select an LSP of their choice, minimizing configuration while preserving decentralization and user autonomy.

A good LSP is like a concierge service for your Lightning Network transactions. (Source: Wikimedia)

Challenge #2: A Single Balance

The Lightning Network is a second layer on top of the bitcoin mainnet, and users have to dedicate bitcoin to their payment channels exclusively if they want to use the network. A satoshi cannot be on the mainnet and the Lightning Network simultaneously.

The separation of funds between on-chain and off-chain balances complicates the user experience in two ways:

1. Managing two balances for one currency is just unnecessary complexity.
2. The off-chain balance is typically spread across multiple payment channels, which limits how much users can spend in any single transaction (at least without AMP—see below).

Therefore, in terms of UX, the technical separation between users' on-chain coins and off-chain funds on the Lightning Network is part of the complexity that must disappear into the background. The technology to perform this illusion already exists, and improvements are on the way.

Submarine Swaps

Submarine Swaps transfer funds between the base-layer chain and the second-layer Lightning Network through (paid) intermediaries—importantly—without trust. In effect, Submarine Swaps can bridge users' on-chain and off-chain balances.

Breez uses Submarine Swaps to move on-chain bitcoin directly to the user's Lightning node without the need to send the funds to a local bitcoin wallet first. As a result, users only see and manage their Lightning balance without a need to manage a separate on-chain balance.

Automatic Rebalancing

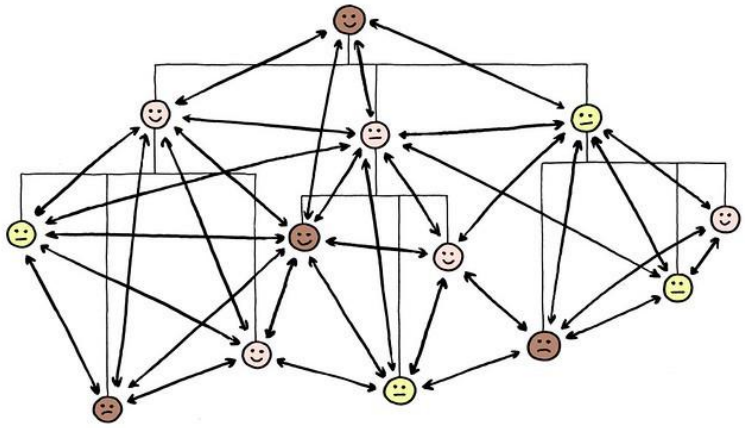
Another characteristic of the Lightning Network that could force users to deal with multiple balances is the dispersal of their funds across multiple channels. If a user's funds are split equally across five payment channels, making a payment above 20% of her total balance presents a challenge. She needs to find a way to reallocate those funds to the desired payment channel.

Currently, automatic rebalancing is probably the best way to work around this obstacle. In effect, a user reallocates her bitcoin by paying herself funds from the channels with excess capacity into the one that needs topping up. Ideally, rebalancing occurs in the background to hide the seams between the channels from the user. Automatic rebalancing can give users access to all their funds for any transaction.

Atomic Multipath Payments (AMPs)

As a means to achieve a single balance, AMPs will—once released—produce the same result as automatic rebalancing, but they do so more efficiently. AMPs split a payment into several smaller pieces that take different routes before being reconstituted in the recipient's wallet. The protocol ensures that the transfer can only be registered as successful if all the pieces do indeed arrive at their common destination, which prevents confusion and fraud.

AMPs overcome the dispersal of funds across channels by routing bitcoin from multiple channels to the single desired recipient, without prior local rebalancing. It's like having your friends meet at the restaurant instead of having all of them meet at your house before going to the restaurant. Again, this function can be automated, letting the user forget about how many coins are on which channel.



AMPs: Many paths from peer to peer. (Source: Jurgen Appello)

Challenge #3: Inbound Capacity

The funds in a payment channel are split between the two nodes at either end: some are local, and some are remote. If the remote balance depletes to zero, the local user will no longer be able to receive payments. If, say, a retailer receives far more payments than he makes, his customers will eventually lose the ability to pay because all the funds on the channel will *already* be on the retailer's side. A few solutions exist to preserve the two-way functionality of payment channels.

Connecting to LSPs

Since "the inbound-capacity problem" depends on how funds are split between a user's local balance and the remote balance at the other end, LSPs can help by actively managing the balance at their own end. For example, Breez funds users' channels as soon as they open, giving them the ability to receive funds immediately, and it manages their inbound capacity automatically. Other examples of LSPs that provide inbound liquidity include LNBig.com and Bitrefill's Thor.

Dual-Funded Channels

As it stands, one party opens a channel, and the user on the other end cannot use the channel until the first initiates a transaction. However, there is a promising proposal to introduce dual-funded channels. Two users would open a dual-funded channel together with starting balances at each end, giving both sides inbound and outbound capacity right away.

Loop Out

Using Lightning Labs' Loop feature, users can also remove funds from their local balance and move the coins to another wallet, onto the chain, or into

cold storage. Removing these funds locally gives the user on the other end the chance to top up and transfer more.

Looping out solves the inbound-capacity problem, but it's far from a UX panacea. Before they can loop funds out, users need a functional bitcoin wallet (so long, single balance). Looping also requires channels to be pre-funded. The less experience a user has, the greater these obstacles will appear.

Challenge #4: Effortless Payments

Transferring fiat can be so smooth that the sender doesn't even notice. That's the whole idea behind direct debit … and pickpockets.

To send digital funds from one device to another, data needs to flow between them. Scanning QR codes is one way many wallets use to transfer data between devices. It works, and most people with a smartphone have had to do this at least a few times, so the inconvenience is perhaps bearable.

"Bearable inconvenience," though, is a hallmark of a UX in need of improvement. Even under optimal conditions, with good lighting and no jostling, QR codes are annoying. In low light or a rocking bus, though, trying to scan a QR code is as much fun as reading braille printed on sandpaper. There has to be a better way than QR. (And no, copy/paste is not a better way.)

"I know you're hungry, but there'll be no pizza until I can get the QR to work!" (Source: wikimedia)

Links

Links are nothing more than addresses for data. They are easy to use, and they can be transmitted in any text-based medium, like email or text message. As a means to transfer payment information between devices, links are the wheel that QR codes never needed to reinvent. With links, payment

execution is a smooth, effortless process. Breez's Connect-to-Pay is a great way to see this solution at work.

Sending a Lightning payment can be as easy as sending a text message, and receiving a payment is as easy as reading one. It's like Venmo, but with bitcoin, and like DropBit, but off-chain.

Near-Field Communication (NFC)

NFC is very convenient for payments at short range. It also facilitates different hardware, giving users the option of using cards or their mobile devices. For face-to-face payments—and >90% of retail purchases are still in bricks-and-mortar stores—the UX of a well conceived NFC transfer is hard to beat.

Challenge #5: Instantaneous Payments

A fiat wire transfer can take a couple of days, a domestic transfer or card payment takes seconds, and passing cash from one hand to another is instantaneous. Lightning has to beat fiat at its best, but two processes in the Lightning Network can present users with delays:

1. initially opening a user's channel, which has to be recorded on the chain;
2. keeping that channel's state current with the bitcoin chain and updating the Lightning Network graph.

The good news is that the first delay can be reduced to minutes and the second can be eliminated entirely.

LSPs

A new payment channel has to be posted to the chain. That means a delay of at least 10 minutes before a user can start sending and receiving payments over the Lightning Network. Compared to acquiring a new credit card—or even signing up for a fiat payment service like PayPal—10 minutes is not bad at all.

Easing the on-boarding process and reducing the amount of time new users have to wait before being able to make their first payment is another area where LSPs shine. For example, by paying higher fees they can accelerate the process of posting users' payment channels to the bitcoin blockchain and minimize the initial on-boarding delay.

Bitrefill's Thor Turbo channels even give users 500K-5,000K Satoshis of outbound liquidity immediately—for a price. But since Thor Turbo channels open even before on-chain confirmation, they can only *send* payments initially, and they do so without bitcoin's underlying benefits.

Background Sync

Any bitcoin wallet worthy of the name needs to stay in sync with the mainnet. Otherwise, anything could happen with the users' funds. And syncing needs to happen in the background, or the lag when opening the app will be a frustrating experience.

Different syncing solutions demand different amounts of trust from the users, depending on how much control over their money and their data they have to sacrifice. Low-trust solutions let users maintain control over their money and their data.

Neutrino (BIP 157) provides the raw, low-trust technology, but if Neutrino has to re-sync every time users open the app, they'll have to wait. So a UX-sensitive implementation has to hide Neutrino's constant updates in the background. To give users even more control, Breez syncs Neutrino over a node of the users' own choosing. No other Lightning Network app gives users more privacy or control.

Trampoline Payments

At the moment, a user's light client has to download the network graph and calculate the best route from among all possible routes. As the network grows, we'll need a more efficient way to route payments than downloading the complete graph.

Trampoline payments would drastically reduce the amount of data and computation required by routing a payment first to a known trampoline node, which would then either pass it on to the recipient or to the next trampoline node, and so on until the payment reaches its recipient. Instead of having to survey the whole graph, a light client only needs to know a few trampoline nodes, and the rest takes care of itself.

Challenge #6: Topping Up Naturally

Wallets empty. All wallets, whether physical or virtual, leather and digital alike. It's one of life's tragedies. To remain useful, they need occasional

topping up. While there's no way around the need for topping up, there are different ways to realize it.

Fiat ↔ Lightning Interoperability

As long as fiat dominates the currency markets, everyone will need a way to convert the value of their fiat into bitcoin on the Lightning Network. For the time being, exchanges are the inevitable solution.

Exchanges, however, are not all equal. They can do users a great service by offering conversion directly from fiat into Lightning, bypassing the intervening step of a bitcoin wallet. Breez cooperates with FastBitcoins to give users a safe, easy, in-app means to acquire the bitcoin they need with the fiat they have.

Submarine Swaps

Since Submarine Swaps allow users to move funds back and forth between the bitcoin mainnet the Lightning Network, they're a convenient way to let users keep their wallets full of bitcoin. And with some canny design, the users won't even know they're doing it.

Challenge #7: Enabling Large Transactions

In order to transfer over a payment channel, a user has to commit funds to it. Since there is no overdraft, no transfer can exceed the amount of funds on the respective payment channel—in theory. Practically speaking, transaction size and channel capacity are two different measures, but the general rule applies that a user cannot shift more beads on a given abacus wire than the wire holds.

In practice, users will likely have their funds distributed across a number of payment channels. But a user might want to combine those amounts to transfer a large sum over a single channel. Users need to be able to shift their beads from one wire to another at will. Ideally, they would be able to ignore the underlying channel architecture entirely and just pay—pay whomever, whenever, and as much as they like.

AMPs

A corollary of AMPs providing users with a single balance (see above) is that they could tap funds from all of a user's various channels to enable whatever transfer the user wants.

Wrong AMP, right idea. (Source: maxpixel)

Wumbo Channels

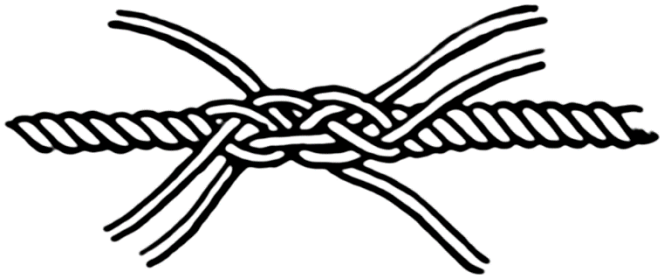
Appropriately enough for a new technology, payment channels are limited to a maximum of 0.167 BTC as a security feature. Wumbo channels are one method proposed to relax that limit.

What's wumbo? Patrick explains it best. It's the opposite of "mini." If the two nodes at either end of the channel agree to remove the limit, they create a wumbo channel. And thus begins the science and art of wumbology.

Splicing

Splicing—especially combined with AMPs—could remove limits on channel capacity from users' consciousness entirely. With splicing, a channel can be closed and a new channel can be opened, with funds being added or removed in the process, and *all in a single transaction*.

Channel capacity would remain a feature of the network, but it could be tailored to fit the current transaction. This feature would also effectively obscure any difference between the Lightning Network and the bitcoin main chain from a non-expert user's perspective.



See where the one ends and the other begins? Exactly. That's splicing. (Source: Wikimedia)

Mass Adoption Wasn't Built in a Day (but maybe in a couple of decades??)

While fiat sets the UX standard bitcoin has to beat, it also has the benefit of centuries of practice. Bitcoin has come a long way in a short decade, and its inherent benefits mean that fiat's days are numbered. Mass adoption has been three quarters away for years, but there is finally Lightning at the end of the tunnel.

The biggest and last remaining obstacle impeding bitcoin's mass adoption is the UX. The Lightning Network is the second layer bitcoin has long needed, and the technologies we've outlined here give it the speed, economy, and intuitiveness that users need now. If habit is the only thing left that speaks in fiat's favor, bitcoin wins by default.

Bitcoin is the worst enemy of communism and dictatorship

By Merwane Draï

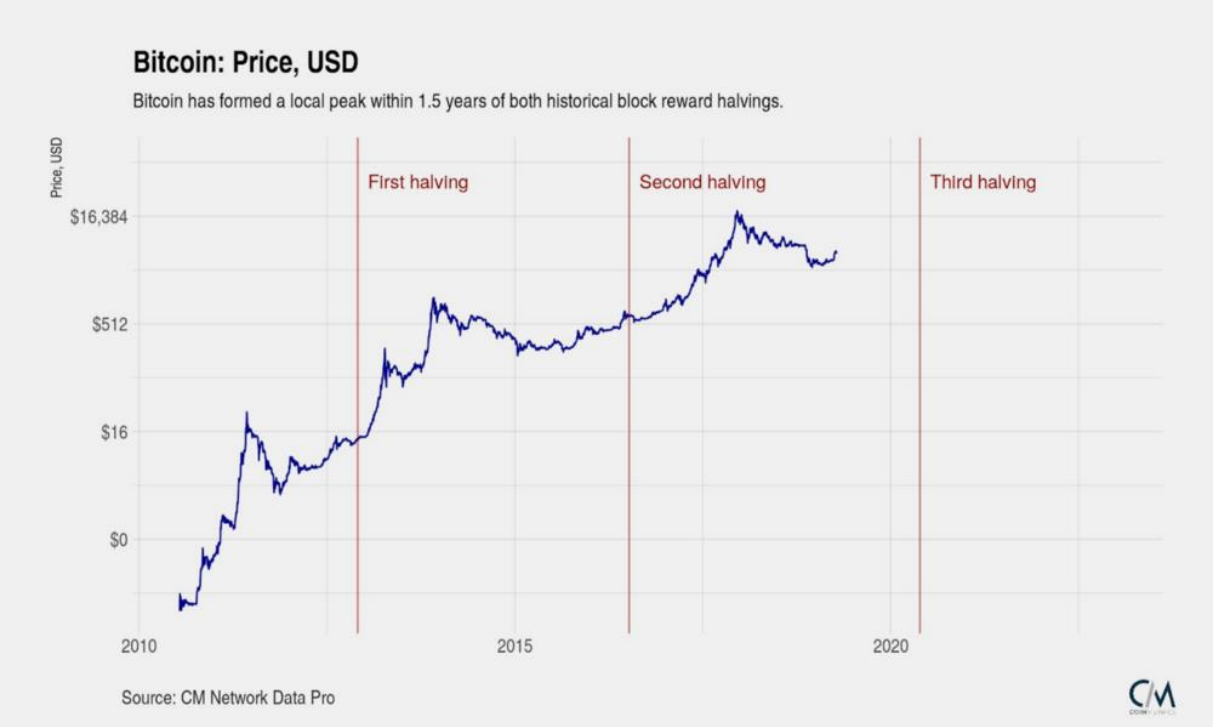
Posted May 18, 2019

Bitcoin and cryptocurrencies in general are seen as technologies favorable to anarchism because of their decentralized nature that rejects all authorities and because of the way we can not control transactions occurring on them. But what is the relationship between Bitcoin and communism? And why do cryptocurrencies make launching a revolution easier than ever? Communist states abolished private property and made sure not to let people prosper from their own business by imposing a totalitarian dictatorship. In the USSR during the communist era, no one was allowed to own real estate or invest in safe stocks like gold, which is the case of the current North Korea. People did not have the chance to put their money in safe values to secure their future or their children's, and even if they wanted to, the law did not allow them. But imagine if all these people had the opportunity to put their money in a safe value that doesn't depend on any authority and is totally anonymous. That would probably have changed the history of the world, there would have been no cold war because the communist bloc would have collapsed much earlier.

Natural prey of Bitcoin: a dictatorship. Photo by Soviet Artefacts on Unsplash

Hundreds of thousands of North Koreans would surely place their saves in Bitcoin to ensure a secure future if the DPRK government hadn't restricted the access to the Internet and information. However, as far as we are concerned, we have access to information and we know how to circumvent government restrictions in the event of a

crackdown. And thanks to technologies like Bitcoin we will never sink into dictatorship or into a new restrictive economic dogma. Cryptocurrencies give us total control over a new decentralized economy. Let's be pragmatic, launching a revolution has never been so simple, we saw it in 2011 with the events of the Arab Spring in Egypt, people organized strikes via social networks, we see it now in Algeria where people have urged the resignation of the dictator Abdelaziz Bouteflika by organizing peaceful protests across the country via Facebook. Imagine if we pushed the game further by launching a fundraising campaign for a revolution thanks to cryptocurrencies, a decentralized and totally anonymous funding where people would not be afraid to see their names. Yes it can be dangerous because terrorist organizations or extremist groups could do the same thing, but it is the price to pay for total freedom.



The Algerian peaceful revolution. Photo by Amine Rock Hoovr on Unsplash

The technology behind Bitcoin (Blockchain) can take us even further by giving us the opportunity to create decentralized communication networks that can not be clamped down by governments. For example, the Chinese government blocks the access to Facebook to 1.6 billion people, but if a decentralized and "peer to peer" version of Facebook existed, they will not be able to restrict its access. Corruption could disappear because the Blockchain

acts as a register impossible to falsify, and at some point, dictatorship will no longer be possible thanks to technology.

Five Fundamental Effects in Bitcoin

Cobweb Supply, Reservation Demand & the Foundations for Understanding Bitcoin's Price

By Prateek Goorha

Posted May 19, 2019

Bitcoin. An actual diagram.

Bitcoin's value has little to do with its quotidian price histrionics. Yes, exuberant speculation routinely outplays rationality. And, of course, there are complex interactions from extant and expected financial market innovations, growing or abating regulatory risks, and the insidious exertions of misinformation.

But price *is* important. To say you are interested in Bitcoin, but far too cerebral to care about its price is as daft as saying that you are interested in gold, but only as an element on the periodic table.

That said, I fear that you learn nothing of value about Bitcoin from looking at charts and following the mood swings of 'traders' on Twitter (especially about its price!). What you need to understand price is a deeper understanding of the effects that are unique to Bitcoin and how they come together in a market in interesting ways.

Therefore, in this piece I wish to give you a simple demand and supply model that has helped my thinking about Bitcoin, and it continually helps me absorb the insights of others. And, to make the model real for Bitcoin, I will also enumerate five of the most basic effects that are important to Bitcoin's price.

Together, the model and the Five Effects, will, I sincerely hope, help you appreciate the splendor of the forest rather than be distracted by its weirdest trees.

Supply and Demand Redux

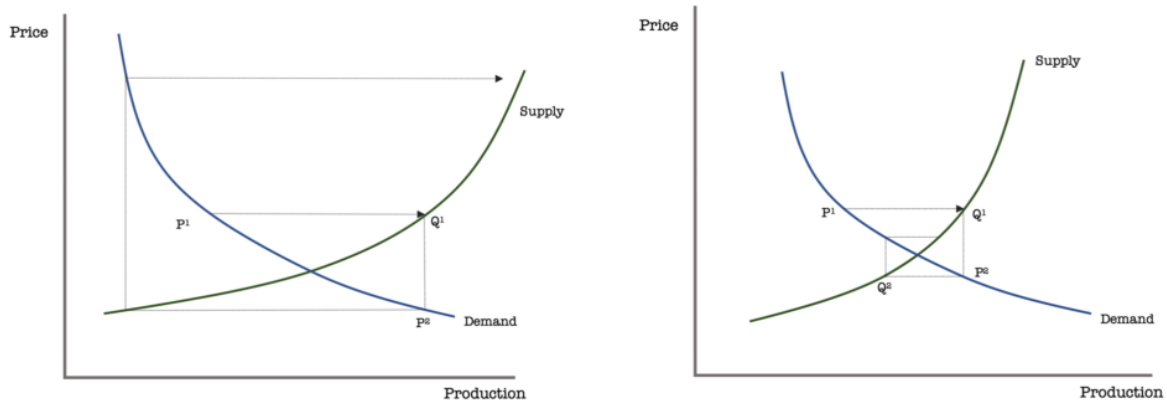
Let's start with the demand and supply model. The Five Effects we will examine below are each part and parcel of an overarching market dynamic that the model helps bring together.

Simply put, the model shows how Bitcoin's market price emerges from the ideas of a **cobweb supply** and a **reservation demand**.

The cobweb model, developed in the 1930s, favors the supply-side in its construction. Essentially, it relies on decisions made by firms on production volumes reacting to extant market prices with a lag between *current* market supply and *future* market supply. Suppliers produce based on extant resource costs and permit the ramifications of these ex ante provisioning decisions to play out in the market with a delay, ex post.

At a given price, say P1, suppliers plan production at a level of Q1 in advance. Later, when the produce is sold, the price may be pushed down to P2 by virtue of a market glut. This lower price then inspires a lower level of planned production among suppliers. This time the market pushes the price upwards by virtue of a shortage.

This feedback loop of lagged responses creates a 'cobweb effect' on the demand and supply diagram, as shown in the figure below. Two cobweb patterns are possible: Depending on the relative elasticities of supply and demand the spiral can lead to an explosive price dynamic further and further away from an equilibrium price, or it may cause the market to converge toward the equilibrium price.



Cobweb Supply. The left panel shows a divergent price dynamic: When supply is more elastic than demand, market price is pulled farther away from an equilibrium (a divergent cobweb). The right panel shows a convergent price dynamic: When supply is less elastic than demand, market equilibrium becomes more attractive (a convergent cobweb).

There are several important aspects of the cobweb model that can be challenged, and the most critical among these is that of learning by producers. Indeed, it seems reasonable to argue that, when producers adapt their expectations of future market prices, the oscillations in the cobweb supply ought to be more muted. While this may have been the reason for the model falling out of favor in economics, the cobweb model *is* full of insight for the case of Bitcoin for very sound reasons.

When a particular market price is expected, miners in Bitcoin have the option to increase their stocks in order to dampen the effect of a divergent cobweb. For miners this ability directly depends on the block rewards progressively contracting at each halving event and the average costs of production progressively rising. The effect of both these aspects is that supply elasticity progressively diminishes, albeit conditioned by the stock that miners, large retailers and 'HODLers' with a long-term commitment to Bitcoin can maintain. As Bitcoin matures, the fluctuations become less pronounced between a divergent and a convergent cobweb.

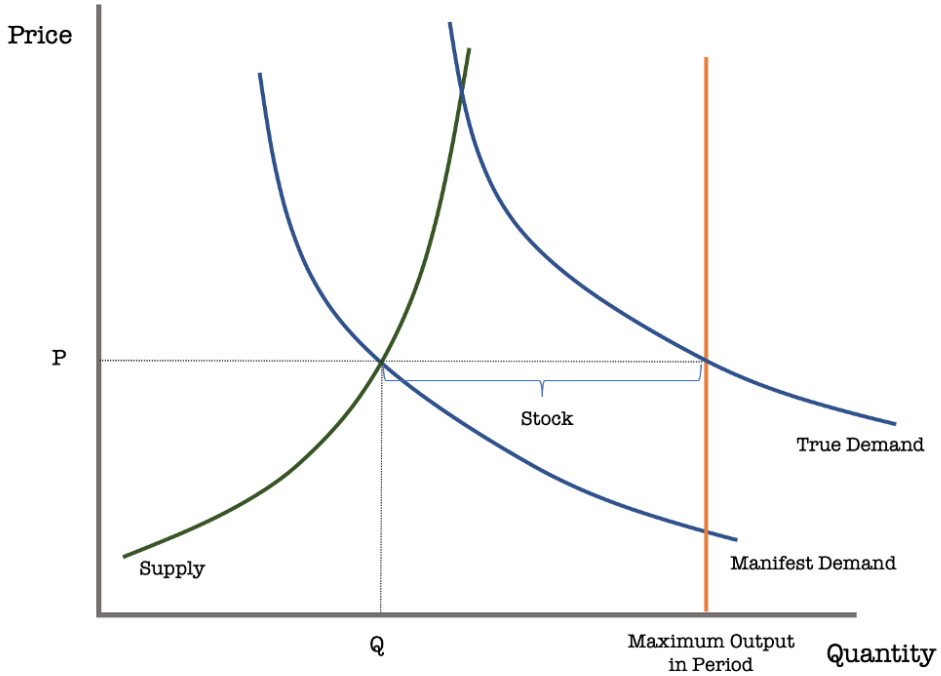
Key to the above is understanding the role of demand. More than just the relative elasticity of demand, what also matters are the *shifts* in demand. Adverse impacts to demand (that cause it to shift leftwards) exacerbate the divergent cobweb's explosive nature, and place an even greater burden on the ability of suppliers to hold stock as inventory.

The demand-supply diagram we have drawn above depicts the usual 'Marshallian' market that is familiar to any student who has studied elementary economics. However, demand curves like these tend to gloss over the assumption that they are aggregating over different *kinds* of consumers; specifically, firms who have a *reservation demand* for their own good so that they may add to their stock.

The rationale for why firms can have a reservation demand for their own produce is partially already clear from the cobweb supply model. Suppliers often face contextually strong production conditions that can force them to plan production levels well in advance of sales and then require them to maintain a stock of their output.

Expected increases in resource costs or uncertain regulatory changes; the threat of technological breakthroughs; periodicity in market interest, and a host of other factors can motivate a distinct reservation demand for producers that is different to the demand for the good that its consumers may have.

To such contextual conditions, Bitcoin also adds structural parameters in the form of a difficulty that adjusts to coordinate the competitive efforts and resource commitments that miners must undertake. And, of course, the prospect of halving events that force the supply curve to become increasingly inelastic.



Reservation Demand. True demand represents the manifest consumer demand plus the reservation demand from suppliers for the stock that is produced for the period, which is capped in advance.

So, the above is a quick sketch of the demand-supply model that I think is useful to have in mind when understanding how the latest news story or development will impact the demand and supply. Now, to fill in the details for this model with some hard data from Bitcoin let us examine the five key factors.

The Five Effects

The five foundational aspects for Bitcoin are:

1. *The Limited Supply Effect*
2. *The Market Vibrancy Effect*
3. *The Competitive Effort Effect*
4. *The Resource Constraint Effect*
5. *The Structure Parameterizing Effect*

We shall now consider each effect, in turn, by considering a proxy variable that we can use to develop an overall statistical model. The results of this regression analysis are presented in the final section.

It is important to understand that the effects *all* matter to Bitcoin, and so any bivariate model that only picks any one of the effects and examined its effect on Bitcoin's is likely incomplete. With this in mind, I have stated the partial influence that each of the five effects exert on Bitcoin's price in the sections that follow.

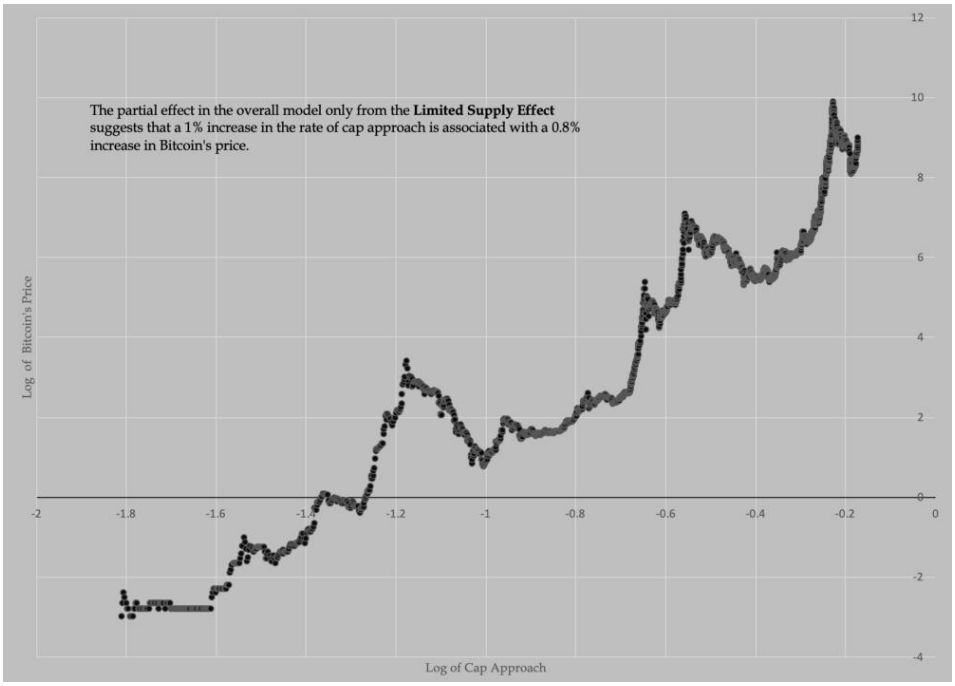
The data are drawn daily, covering the period July 17, 2010 to May 14, 2019, constituting 3224 observations for the overall regression model.

1. The Limited Supply Effect

Limited supply is the bedrock of Bitcoin. It is also crucial to seeing why cobweb supply and reservation demand are the right tools to understanding Bitcoin as an economic market.

Here, I have proxied the limited supply effect with a variable I have called *cap approach*. The idea is that an approaching cap on the amount of production exerts itself on the production plans for miners. A strongly convex supply curve is common knowledge among miners and the cap approach rate makes it increasingly vivid to market participants over time.

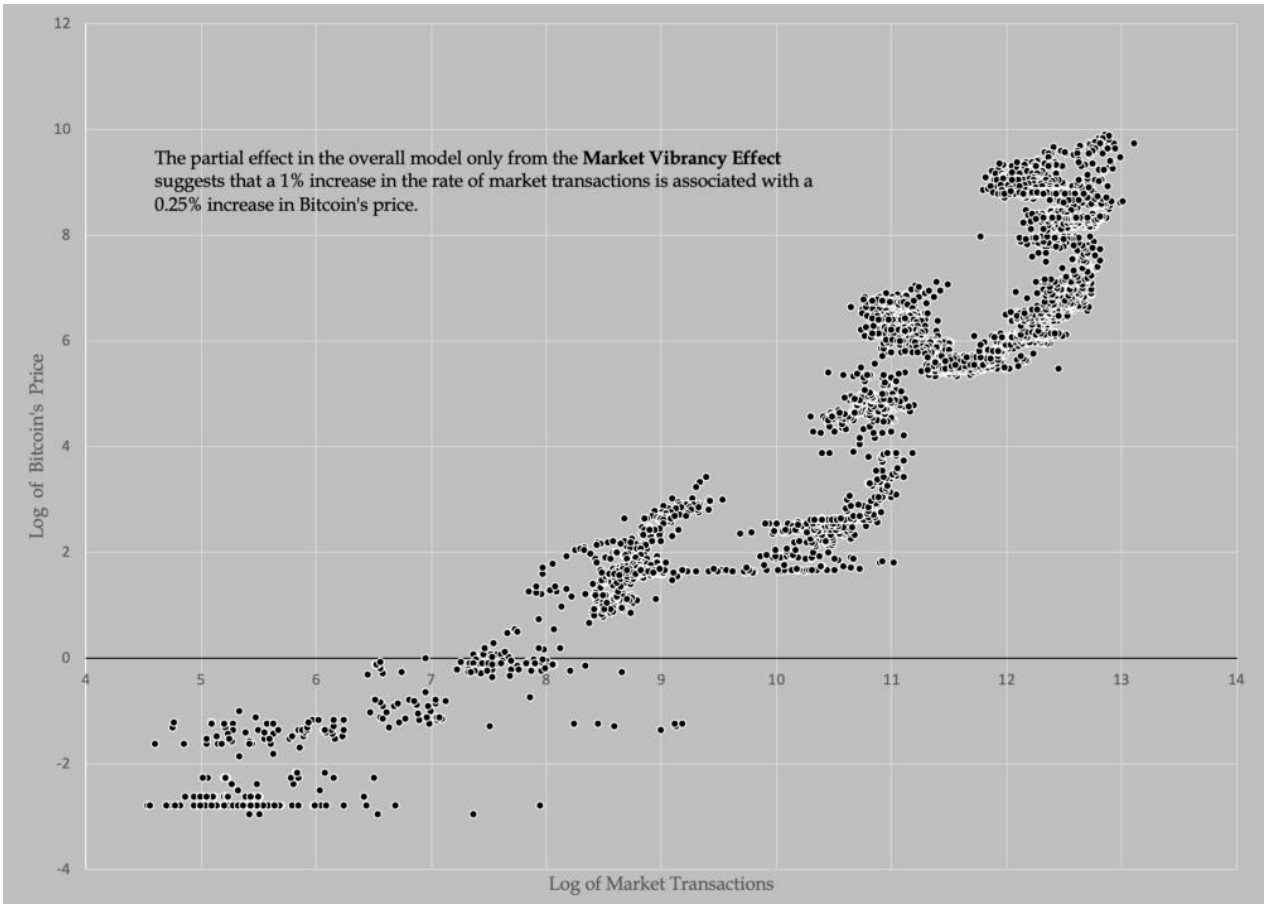
The figure below plots price against the cap approach to give a sense of how they relate. The inset text shows the size of the effect from Limited Supply Effect in the context of the broader model conditioned by all five effects simultaneously.



2. The Market Vibrancy Effect

Any market model's usefulness is mediated by the vibrancy of the market. The cobweb supply and reservation demand model is no different; without a robust level of transactions in the market the relative position of manifest demand compared to true demand becomes much harder to establish. This, in turn, makes gyrations in the cobweb model between convergence and divergence more unpredictable.

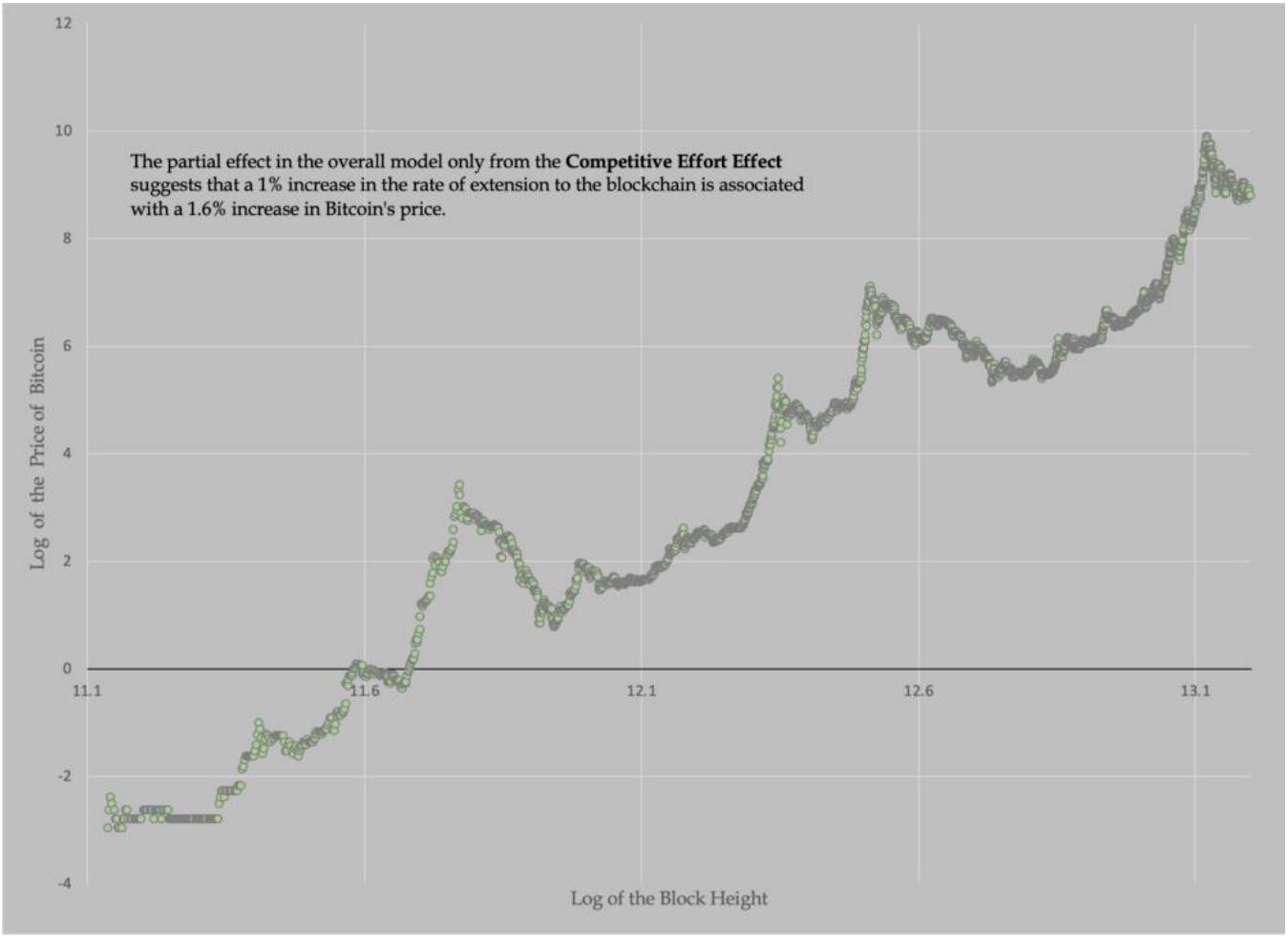
The figure below uses the *number of market transactions* as a proxy variable for the Market Vibrancy Effect.



3. The Competitive Effort Effect

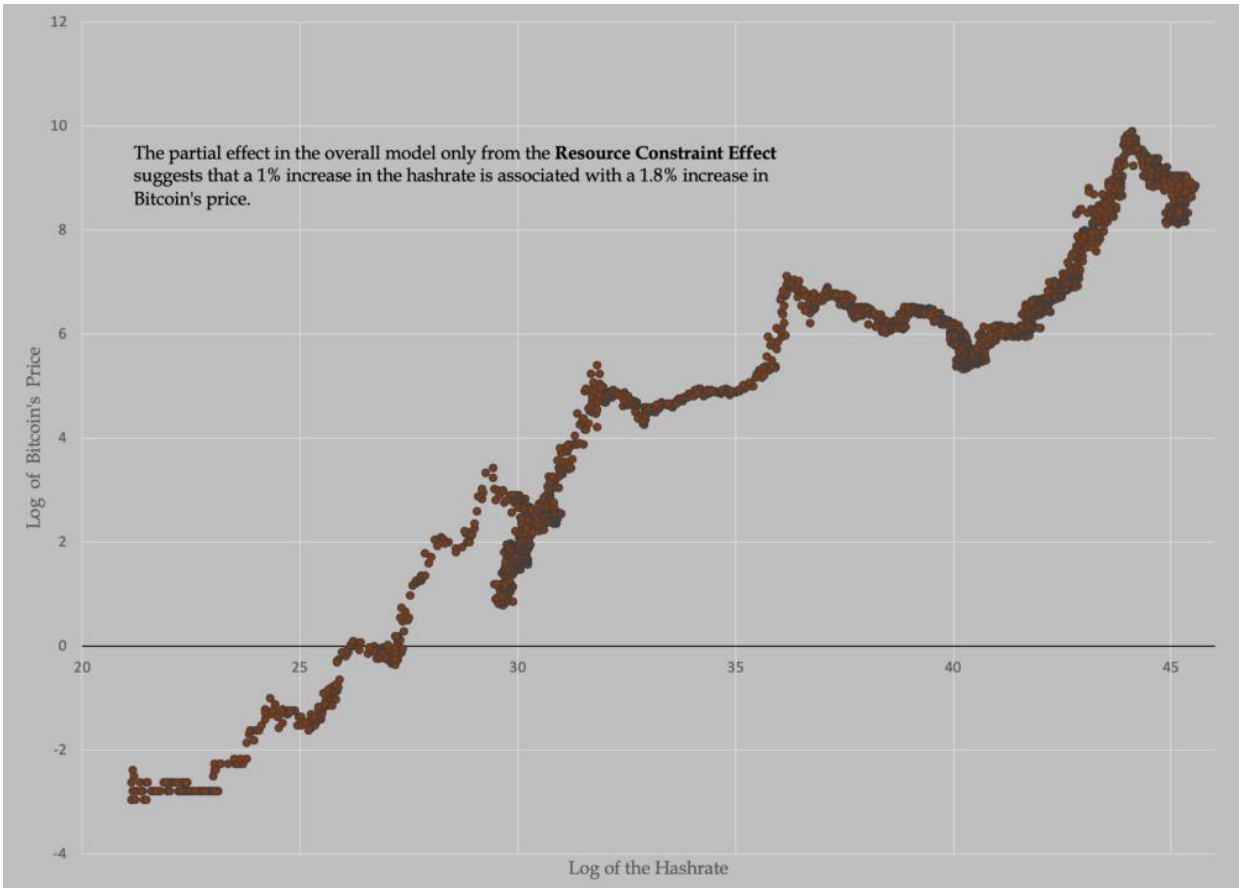
The incentive to increase reservation demand depends on the manifest market demand, but it also has a direct relation to the competitive efforts of rival producers. In Bitcoin, miners can gauge the level of such competitive efforts through multiple publicly visible variables. *Block height* is perhaps not the only proxy variable that one might use for this purpose, but it does make a great deal of sense to do so. Block height is sufficiently separated from price and the rate at which it alters is far more closely linked with the competitive efforts expended across all miners.

The figure below presents the results and states the partial effect of the competitive effort effect on Bitcoin's price.



4. The Resource Constraint Effect

Resource constraints are essential to the idea of what inspires producers to provision supply ahead of realized demand. The stronger the influence of the opportunity costs of resources deployed for production, the more likely it becomes for producers to plan production, hold stocks and impact market price through the rate at which they sell their stocks. The hashrate stands as a strong candidate for a proxy variable for this effect. The figure below presents the result and states the partial effect of hashrates on Bitcoin's price within the overall model.



5. The Structure Parameterizing Effect

The final effect is my firm favorite for the simple reason that it forces us to contend with a rude fact: The rules of the game for Bitcoin are fundamentally different from the other economic markets we have learned to caricaturize with the aid of demand and supply diagrams taught at school.

The structure for the overall Bitcoin market is represented with an algorithmic mechanism that governs its functioning. The word 'govern' is anathema to why I admire Bitcoin, but it is also the right word in this context. If market participants can adjust their strategies in such a manner that the market can be subverted into operating differently from its idealized conception, it isn't parameterized in any meaningful way. Bitcoin is parameterized, and there is arguably no better proxy variable for this than the *difficulty* adjustment variable. It is because of the difficulty adjustments that miners alter their production plans; because of it that the feedback loop of a cobweb model does not spiral out of bounds with invidiously explosive overproduction or throttling underproduction.

The overall regression model, *with all Five Effects*, is presented below. That the coefficients are all highly significant and that the overall model specification is also highly significant with an R-Squared that exceeds 97% is less relevant. There are a host of statistical issues that need resolving, but which are beyond the scope of this informal piece. However, it does make the message clear:

Bitcoin's value comes from an understanding of demand and supply that is uncomfortably new to most (especially to most economists!). And, much of this intrinsic value rests on the firm foundations provided by just five effects.

Effects		Coefficients	Standard Error	t Stat	P-value
	Intercept	-50.3761	3.7710	-13.3590	1.1733E-39
Limited Supply Effect	ln (Approaching Cap)	0.8225	0.3111	2.6436	0.00824363
Market Vibrancy Effect	ln (Total Tx per Day)	0.2422	0.0350	6.9257	5.2169E-12
Competitive Effort Effect	ln (Height)	1.6008	0.2930	5.4638	5.0151E-08
Resource Constraint Effect	ln (HashRate)	1.7974	0.0919	19.5582	1.404E-80
Strcuture Parameterizing Effect	ln (Difficulty)	-1.5811	0.0920	-17.1836	2.1854E-63

Further reading

1. Holland, Thomas E. "Marshall, Walras and the Cobweb Theorem." *The American Economist* 21, no. 2 (1977): 23–29.
2. Ezekiel, Mordecai. "The Cobweb Theorem." *The Quarterly Journal of Economics* 52, no. 2 (1938): 255–80.
3. Coase, R. H., and R. F. Fowler. "The Pig-Cycle: A Rejoinder." *Economica*, New Series, 2, no. 8 (1935): 423–2

Bitcoin: An Accounting Revolution

By Permabull Nino

Posted May 21, 2019

Decentralized Credit (DR/CR)May 21

Building Accounting Systems, Triple-Entry, & Absolute Assurance

Bitcoin is an accounting revolution. This accounting revolution enables a monetary revolution. Another way to look at this is:

Accounting Revolution = Technological

Monetary Revolution = Social

Disruptive technologies spark social movements. If they didn't spark social movements, then they would (by definition) not be disruptive. Facebook, YouTube, and Airbnb are all technologies that changed the way we understood and interact with friends, content creation, and travel, respectively. Bitcoin is no different in this regard, as it is an accounting technology that is in the process of transforming our understanding +usage of money.

This piece will provide a detailed discussion on Bitcoin and how it provides a simple, yet revolutionary step forward in the field of accounting. With this in mind—wrapping our heads around Bitcoin as an accounting phenomenon requires some build up. Our game plan goes as follows:

1. Brief History of Accounting + Audit
2. Historical Trends of Accounting + Audit
3. Introducing Bitcoin + Triple Entry Accounting in Depth
4. Bitcoin Accounting vs Double Entry Accounting
5. Bitcoin + Lightning vs Double Entry Accounting
6. Implications + Conclusions

1: Brief History of Accounting + Audit

Accounting and audit both have rich histories that are worthwhile exploring for purposes of our discussion. It's important that we understand how these fields advanced over the long arc of time because this understanding will allow us to appropriately frame Bitcoin and its design. It is common to cite the cypherpunks and their compelling works as the beginning of Bitcoin's

story. However, what we will see through our historical lens is that Satoshi's invention was thousands of years in the making. Below we will walk through each historical point / accounting advancement and attempt to concisely elaborate on its relative significance:

Counting

Before concerning ourselves over value-recording capabilities we needed the ability to communicate numbers at the most basic level. These communication building blocks included (1) signaling numbers non-verbally, (2) verbal communication of numbers, and (3) written communication of numbers. All three historically occurred in the order as presented and originate from a single descendant: the human body. Quite naturally—humans used parts of their body to communicate early on, and this habit even continues until this day. Popular body parts leveraged for counting included fingers, toes, knuckles, and even ears. Different groups of people built numerical systems + created numerical language using certain body parts, and the body part of choice determined the numerical layout. For this reason, it seems more than appropriate that 2 & 5 are such important numbers within our contemporary counting system. Just look at your own body and you'll find the answer to be self-evident.

Private Record Keeping

As human exchange evolved, a need to track such dealings emerged. Until the 14th century this generally involved jotting down rough "notes" which described in a sentence / paragraph format the nature of an exchange, including counterparties, goods, and amounts. During this time period "accounts", which are merely a batching of transactions based on type to arrive at an easily digestible balance, did not exist (categorization of receipts & disbursements, however, did exist). Organizing the numbers for the transactions in a column to the right of the description hadn't been popularized either, with amounts just included within the written transaction description.

In this era single entry accounting reigned supreme, and with this accounting scheme the complexity of exchange sat stationed in a form of financial purgatory. How so? Well—simply put, only 1 half of each transaction found its way into the accounting books of each party under single entry. This weakness heavily impacted the auditability of transactional records, and this deficiency naturally made it substantially more difficult to settle disputes.

Lack of recourse and an absent “safety net of truth” in the form of reliable accounting records made stakeholders much less inclined to expand their transactional reach, and rightfully so. Fortunately, a solution emerged to fix these problems...

Double-Entry Accounting

The accounting quality standards through the private record keeping era left a lot to be desired. This was the case for good reason, as the records being kept were only for the eyes of the party doing the transacting. However—a great leap finally occurred that led to the need for systematic bookkeeping: accountability to external parties. Recording a transactional history with an external user in mind requires an effective, easy to follow approach, that ultimately provides an auditable trail of evidence to identify errors / fraud in the case of dispute. Double-entry accounting fulfilled this need in a simple, yet elegant fashion. The genesis of double entry as we know it emerged in Genoa, Italy during the 14th century before spreading to the rest of Italy and neighboring European countries. Luca Pacioli, a Florentine friar-mathematician, is known for popularizing double-entry via his treatise *Summa de Arithmetica*, which included a chapter on the newly discovered double-entry scheme.

Following the publication of Luca’s treatise the world witnessed a viral spread of double-entry bookkeeping, but not without opposition. On multiple occasions accountants dispersed throughout various parts of Europe attempted to debunk double-entry or invent a “new and improved” bookkeeping system, to little avail. Double-entry survived peer-review and was here to stay. The fact of the matter is that it withstood the test of time because double-entry captured the true essence of transacting, by recording the “give” and the “take”, so to speak. Early success and basic accounting framework aside, double-entry did require iterations over the years. A couple instances that exemplify this need to iterate include:

(1) Checking that debits and credits balanced (i.e. netted to zero) wasn’t initially understood. This needed to be discovered later.

(2) Transferring residual income into a capital account at the end of a reporting period (Net Income →Retained Earnings) wasn’t always obvious and required time for discovery.

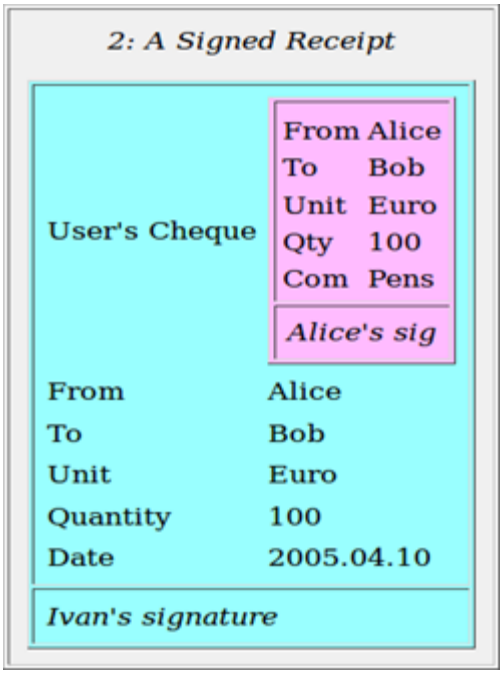
Those that are accountants by training understand these 2 iterations as a given nowadays, which is a testament to the advancements in double-entry in the past ~ 600 years. Despite these large strides, double-entry and the

reporting systems such as GAAP & IFRS built on top of it are still works in progress.

Note: Double-entry adoption also introduced formal audits of accounting records to the mainstream.

Triple-Entry Accounting

The turn of the millennium welcomed a once in 1,000 years evolution of accounting: triple-entry. Particularly of interest for purposes of our discussion is Ian Grigg's suggested implementation of triple-entry, which he describes as a "...system [that] creates bullet proof accounting systems for aggressive uses and users". This bullet proof accounting system supposedly was to bring together "financial cryptography innovations such as the Signed Receipt with the standard accountancy techniques of double entry bookkeeping". Further, the system was to create 3 sets of entries: two of which that are included as a part of the standard set of double entries, and additional entry to be provided by the issuer. This entry was provided by the issuer in the form of a digital receipt of the transaction, signed by the issuer, to create a "dominating record of the event" to be stored by all 3 parties.



(A Signed Receipt, i.e. the "dominating record of the event")

Note: Alice + Bob = transacting, Ivan = "issuer"

Grigg makes several noteworthy observations such as the importance of transparency within the system to track the "clear relationship of participants", which would in turn require pseudonymity. He also touches on the digital receipt's dominance in information terms, but its relative weakness in processing. Overall, his handle on the triple entry scheme is mind-bendingly strong for someone who wrote this Christmas Day 2005. If I'd have to guess—this paper written by Mr. Grigg went unnoticed by most of the world at the time of its publication. However, speculatively speaking, it seems likely this paper served as the final spark to create the ultimate accounting scheme which would support decentralized, digital cash 3 years later. This gap in time between Grigg's

piece and a very famous whitepaper published on Halloween 2008 seems hardly coincidental.

2: Historical Trends of Accounting + Audit

Our short run through the history of accounting + audit helps track our progress as a species in synthesizing and documenting value. In this section we will list trends that have persisted throughout the history of accounting + audit to provide additional context to such history. By doing this we will much better understand the core pieces to building accounting systems and thus be capable of comparing various accounting schemes along with their respective pros / cons. Without further delay, standout trends through history include:

§ Tamper Resistance: Accounting cannot serve its purpose for tracking value through time if records are easily reversed / changed.

o Example: Dating all the way back to 2600 B.C., Babylonian scribes used to record business dealings on clay slabs. These clay slabs were subsequently baked or sundried to preserve permanence of the documentation.

§ Redundancy: This feature of accounting systems serves as the backbone of error + fraud prevention. Redundancies such as financial controls aid in maintaining internal accounting quality and audits from independent third parties provide an extra layer for identifying issues.

o Example: Ancient Egyptians implemented redundancy into their financial dealings by assigning two separate officials the task of recording independent accounts of each transaction.

§ Transparency: Accountability cannot be ensured without transparency in some sort of capacity.

o Example(s): In Ancient Greece elected officers of finance had their accounts engraved on stones, which were available for scrutiny to the public. A more contemporary case of transparency / accountability can be found in publicly traded stocks, and their public release of quarterly / annually reviewed and audited financial statements.

§ Adaptability: Accounting as a technology has had a great track record of adapting to satisfy the needs of its contemporary period. A lack in adaptability would stunt future growth in any economy as entrepreneurs would trip over themselves attempting to scale their value-recording capabilities with their business operations.

o Example(s): Pacioli used a book for recording entries called the “Memorial”, which preceded entries in the Journal. This book was treated as a “conversion journal” of sorts, as there was very little uniformity of monetary systems during the Medieval period. Amounts in the Memorial were converted to a single unit of account, and subsequently recorded in the Journal. For something more contemporary—today GAAP & IFRS are constantly changing to account for complex, newly identified issues.

§ Enabling: There’s a degree of reflexivity in accounting systems and the economies they’re created to support. Accounting systems need to adapt to support entrepreneurs, but once they do, they enable further economic expansion and prosperity.

o Example: Double-entry bookkeeping’s birth occurred right as the Renaissance was beginning, an era which marked the transition to modernity as we know it. Albeit not a popular opinion, there’s an argument to be made that the creation of such a bookkeeping system provided a strong undercurrent for pushing the world ahead during this period.

§ Exclusive: Accounting has historically been a field dominated by the educated, with high barriers to entry.

o Example(s): In the early days of double-entry, the number of accountants within a country could be counted on two hands. Later, accountants were prohibited from practicing for not possessing enough apprenticeship / educational hours. These standards in some respects persist today.

§ Simplicity: An unspoken rule in accounting / audit is that the procedures used to account for a transaction should only be as complicated as the situation demands. Simplicity is key in error prevention (before the fact) and detection (after the fact).

Additionally, simplicity greases the wheels for adoption of an accounting scheme.

o Example: Edward Thomas Jones, an English accountant, created a bookkeeping system in the late 18th century that he claimed would upend double-entry. His so-called groundbreaking system used 10 columns, instead of 2, and supposedly provided stronger assurances surrounding error / fraud prevention of ledger data. Needless to say, the system was overly complex for the little, if any, improvements in ledger integrity the system offered.

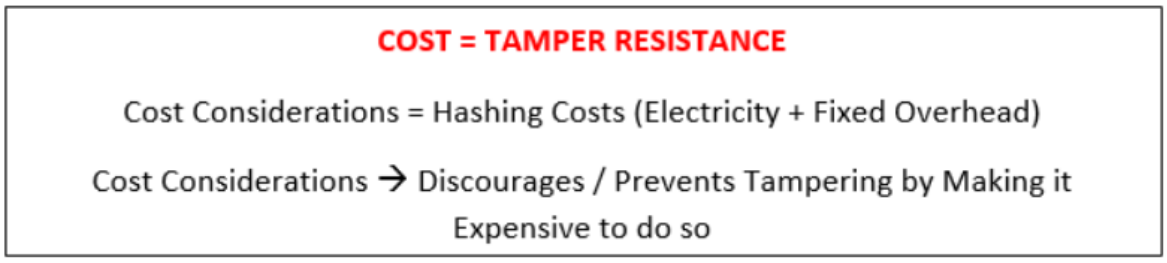
3: Introducing Bitcoin + Triple Entry Accounting in Depth

Of the characteristics used to describe accounting systems in the previous section, the 3 most important are arguably (1) Tamper Resistance, (2) Redundancy, and (3) Transparency. With Grigg's instantiation of triple-entry, real-time transparency emerged as an obvious improvement from the well-established double-entry scheme. A degree of additional redundancy showed itself as another innovation within his proposed system by creating the receipt ("dominant record of events"), which was to be stored by the 2 transacting parties + the "issuer" (third party verifier). However—with only 3 parties storing the receipt, the possibility of losing it remained. In addition, purposely disposing of the receipt loomed as a "what could go wrong" as well. At risk of sounding repetitive, some work remained to make Grigg's system truly "bullet proof", as the tamper resistance and redundancy pillars were not fully resolved as of his 2005 paper.

This is where Satoshi comes in. Using a small tweak to Grigg's system, Satoshi fully solved the remaining tamper resistance and redundancy issues within the triple entry scheme. How did he/she pull this off? By gamifying the process for providing the signature on the issuer receipt. Via gamification, competing for verification + signature rights became explicitly profit-incentivized. The opportunity to profit gave outside parties a selfish want / need to provide third party verification services, and with this desire came a gigantic redundancy upgrade. In astounding fashion, the redundancy enabler within Satoshi triple entry also provided the engine for mitigating the remaining tamper resistance problems. The mechanism leveraged for accomplishing this is called "Proof of Work" (PoW).

Simply (and generally) stated, PoW requires an unforgeable, costly amount of effort to prove work was performed in order to reach a certain conclusion. Within the Satoshi scheme, Bitcoin, work is carried out via *repeatedly* hashing a subset of relevant block data + a random number (nonce), to find a

hash below the required network difficulty target. This hash itself can be verified by other third-party verifiers within the Bitcoin network and ultimately serves as the "receipt signature" for each published receipt i.e. blocks. The cost to hash comes in the form of electricity used to fuel hashing machines (ASICs), and this cost makes it expensive to tamper with the dominant record of events (i.e. the blockchain). The coinbase rewards (newly minted coins) of each block that is published / accepted by the network + transaction fees serve as the profit motive. To cleanly summarize the solving of the tamper resistance and redundancy issues:



4: Bitcoin Accounting vs Double Entry Accounting

The differences in Bitcoin's triple entry scheme and Pacioli's double entry go beyond the 3 characteristics mentioned in the previous discussion. Within this section we will explore in detail the differences between the two systems, the implications of Bitcoin's existence as it relates to accounting, and whether the two systems represent substitutes or complements to each other. Below is a table listing out the primary differences between Bitcoin and double entry:

Category	*Double-Entry*	*Bitcoin (POW Accounting)*
Greed Effect	Fraud, other aggressive accounting practices	Under the correct conditions, deters motivation for fraudsters and encourages bad actors to play by the rules
Audit	Audited historically	Audited in real time
Audit Quality	Reasonable Assurance	Absolute Assurance
Accounting + Audit Dependence	Human professional judgement + software	Largely software driven
Unit of Account	Fiat / Crypto denomination of choice	bitcoin
Accuracy	Pre-audit, accuracy depends on quality of financial statement control design and execution	Accuracy depends on users running compatible client versions, non-buggy code, and a majority of hashrate being honest
Fraud Cost	Cheap	Expensive
Determining Intent (Fraud or Honest Mistake)	Difficult	Easy, and obvious
Fraud Detection	After the fact	Immediate
Network Effect Upside	Average - can run double entry accounting with your own local currency (including Bitcoin)	Very Strong - need to use the network incentive token (i.e. bitcoin) to access available assurances
Accounting Dependence	Run independently - fraud in Company A largely does not affect Company B	Run independently - but fraud within the accounting system causes large disruption for all stakeholders
Ledger	Private	Public
Redundancy	Low - ledger stored by a few parties at most	High - ledger stored by a large amount of parties
Ledger Entry Rights	Closed - only company employees allowed to make entries	Open - anyone can create entries
Entries	Subject to change	Immutable
Entry Finality (Timing)	Delayed - post annual audit	After x amount of blocks that makes it infeasible to rewrite ledger history
Scalability	High	Low

Double-Entry vs Bitcoin

At a high level, the differences between these systems can be summarized into 3 categories: (1) Flexibility, (2) Scalability, and (3) Intensity of Assurances Offered. However—these categories are not all created equally. Flexibility + scalability characteristics of each respective system are what ultimately yield a difference in intensity of assurances offered. The prior reflects specific means of differentiating Bitcoin from the traditional accounting system, and the latter more so illustrates the “grand innovation” when you put all the pieces together. This grand innovation will be our focus for the rest of this section...

With this in mind—the whole world runs on double entry accounting. This double entry dominance is to be expected, as it is a highly flexible, scalable, and simple system for recording / communicating value. Furthermore, in the event of errors / fraud there also exists an audit trail for identifying what went

wrong. Financial controls in some capacity provide a means to prevent these problems (before) and external auditors perform their role in detecting (after). All things considered, double entry has been a raging success and continues to serve us very well. However—there is one glaring flaw with it: the assurances that it offers its users over data integrity. In the accounting profession, the intensity of the assurance that double entry offers is known as "reasonable assurance". Although reasonable assurance does suggest a high degree of reliability post-audit, it by no means is a guarantee that the ledger is completely accurate, only accurate "enough". Take the accounting / auditing of cash balances as an example, a relatively low-risk area of any audit engagement (and the most comparable asset to bitcoins on any balance sheet). External audit gains confidence over the cash balances by requesting bank confirmations, which are paper / digital reports that take anywhere from 24 hours to a few weeks to get from the bank holding the client's funds. Reports from external third parties such as these are considered highly reliable pieces of audit evidence, as collusion would be the only manner of which fake balances could be hypothetically supported. Collusion is very difficult to detect because the auditors have no reason to suspect foul play, they do not have access to the bank's accounting system, and there might not be any signs of fraud in the report(s) provided. The purpose of this example is to show that even in the simplest cases, it is impossible to attain *full guarantees* over the integrity of accounting data under the double entry scheme. Herein lies the pinch, and where Bitcoin makes one of the greatest leaps in the history of accounting...

Bitcoin is the first accounting system to ever provide *absolute assurance_over ledger data. Unlike double entry, Bitcoin accomplishes this by providing _expedient third-party verification* via its inflexible, highly redundant protocol + network. From an accounting perspective, the speed at which this verification from independent parties occurs is incredibly significant, as it reflects a paradigm shift from an overhead intensive and slow verification regime to one that is lightweight for users and only "a click away" at all times. To put more simply, it disintermediates the old and separate internal accounting + external audit functions by combining them into a single, inseparable product.

It is worthwhile noting that absolute assurance is not an "out of the box" feature with all public blockchains and can only be earned with enough resources committed to the network. These resources strengthen the tamper resistance and redundancy pillars we discussed earlier, and very few (if not only Bitcoin) public blockchains meet this criterion. This ability to provide absolute assurance is mission critical for the longevity of any crypto network,

as entrepreneurs will only rally around accounting schemes that prove to be highly reliable.

It's likewise important to note that double entry and Bitcoin triple entry are complementary in nature. A quick glance at the table provided within the section should show that Bitcoin fills some gaps in the double entry scheme that are welcomed additions to the accounting offerings available on the market today. It is of equal importance to note that bitcoins (the unit of account) are compatible with both the Bitcoin network and a locally run double entry software. The same cannot be said of competing fiat monies such as the US Dollar, the Euro, or British Pounds, which only have access to one part of the full accounting suite (double entry). In a later section we will further explore the implications of such a distinction.

5: Bitcoin + Lightning vs Double Entry Accounting

Detractors have long argued that Bitcoin would never be anything more than a fledgling network due to its inability to scale. These same naysayers have further posited that layer 2 solutions were a pipe dream and would never come to fruition. Fortunately, this has proven not to be the case as of early 2019, with the rapid expansion of Lightning Network in terms of users, nodes, channels, and BTC capacity. On the surface Lightning looks like an additional payment rail that will help expand Bitcoin's transactional reach. This description is accurate, but the real question is "why does it enable higher transactional throughput?". From an accounting standpoint, the answer is that Lightning represents an iteration on old school double entry, and more specifically, a Bitcoin-native double entry scheme. Before discussing Lightning any further, let's present the table from the previous section with a new column attached:

Category	Double-Entry	Bitcoin (POW Accounting)	Lightning
Greed Effect	Fraud, other aggressive accounting practices	Under the correct conditions, deters motivation for fraudsters and encourages bad actors to play by the rules	Fraud, but with explicit rules for getting caught
Audit	Audited historically	Audited in real time	Audit timing dependent on when channel closes
Audit Quality	Reasonable Assurance	Absolute Assurance	While channel is open Reasonable Assurance < Lightning Assurance < Absolute Assurance Upon closing channel = Absolute Assurance
Accounting + Audit Dependence	Human professional judgement + software	Largely software driven	Largely software driven
Unit of Account	Fiat / Crypto denomination of choice	bitcoin	Crypto denomination of choice
Accuracy	Pre-audit, accuracy depends on quality of financial statement control design and execution	Accuracy depends on users running compatible client versions, non-buggy code, and a majority of hashrate being honest	Pre-settlement on the blockchain, accuracy depends on non-buggy code and channel monitoring
Fraud Cost	Cheap	Expensive	Cheap < Lightning Fraud Cost < Expensive
Determining Intent (Fraud or Honest Mistake)	Difficult	Easy, and obvious	Easy, and obvious
Fraud Detection	After the fact	Immediate	After the Fact < Lightning Fraud Detection < Immediate
Network Effect Upside	Average - can run double entry accounting with your own local currency (including Bitcoin)	Very Strong - need to use the network incentive token (i.e. bitcoin) to access available assurances	Average - can run lightning on top of any compatible crypto network
Accounting Dependence	Run independently - fraud in Company A largely does not affect Company B	Run independently - but fraud within the accounting system causes large disruption for all stakeholders	Run independently - fraud in Channel A largely does not affect Channel B
Ledger	Private	Public	Private
Redundancy	Low - ledger stored by a few parties at most	High - ledger stored by a large amount of parties	Low - ledger stored by a few parties at most
Ledger Entry Rights	Closed - only company employees allowed to make entries	Open - anyone can create entries	Closed - only channel participants can make entries
Entries	Subject to change	Immutable	Subject to change
Entry Finality (Timing)	Delayed - post annual audit	After x amount of blocks that makes it infeasible to rewrite ledger history	Delayed - upon broadcasting to the settlement network
Scalability	High	Low	High

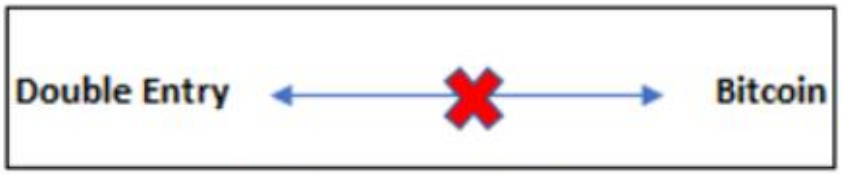
Double-Entry vs Bitcoin vs Lightning

What we start to see from the table above is that Lightning represents a middle ground between double entry and Bitcoin triple entry from an assurance perspective. This trade off for establishing a middle ground is accomplished at the expense of simplicity and flexibility that old school double entry offers. As such, double entry remains relevant and useful in an accounting universe where Bitcoin + Lightning exist. Dually important is what the layered approach to scaling represents: an adherence to accounting + audit principles. During any financial statement audit, amounts that are below a certain materiality threshold individually + summated are ignored, as assurance over the small balances would generally provide trivial amounts of additional confidence in the state of the financials in question. Bitcoin and Lightning leverage this rationale for scaling Bitcoin, by moving smaller transactions to a less redundant accounting + audit layer, with the option of always using Bitcoin's on-chain absolute assurance at the click of a button when closing out a Lightning channel.

6: Implications + Conclusions

Bitcoin as the Ultimate Accounting Tool

Bitcoin has the potential to become the center of the accounting universe. Why? Because bitcoins (the unit of account) are fully compatible across all 3 parts of the accounting suite, whereas fiat monies only have access to a single part. Visually speaking, we can illustrate this difference as follows:



The Fiat Accounting Suite

The Full Bitcoin Accounting Suite

Since fiat monies are not natively crypto based, they are incapable of accessing the full depths of the accounting + utility assurances offered by cryptocurrencies. Stablecoins do not qualify as they have huge centralized dependency issues and, the stablecoin merely represents dollars that only exist off-chain (or in some cases, "supposedly" exist off-chain). What this difference implies is that when Bitcoin comes of age it will be more useful than fiat, as there will be more ways to reliably account for value for prospective entrepreneurs. More ways to account for value with different accounting models that are strong in different arenas suggests that there will be new types of businesses created with a Bitcoin-centric viewpoint, while fiat sits watching on the sidelines.

Lastly, "The Full Bitcoin Accounting Suite" graphic might provide some clues to lingering concerns over a low block subsidy future. If Bitcoin becomes the center of the accounting universe and the ultimate source of value-based truth, there's a high chance that demand will capably support security of the network. Those who argue "high fees will kill adoption" fail to understand the intensity of assurances Bitcoin offers, and the ease at which it does this. Put

lightly—Bitcoin is insanely cheap compared to alternative options for obtaining high degrees of assurance. Bitcoin is a vehicle built for moon missions, but we are giving it similar treatment to a scooter.

Extra thought: Bitcoin might not be considered a “Unit of Account” from a monetary perspective, but it is already the ultimate Unit of Account in the most important sense of the phrase—from the accounting viewpoint.

Blockchain Model is Here to Stay

This point isn’t something many people spend much time thinking about. However, there are still some out there that are looking to speculate on alternative forms of Distributed Ledger Technology (DLT). If these other distributed accounting models aim to upend the blockchain model, they need to equally / stronger provide (1) simplicity in accounting for value or (2) intensity of assurances that the blockchain model already offers. I for one consider this unlikely, as the blockchain model is quite simple (Satoshi explained it in 6 sentences in the Bitcoin whitepaper) and the assurances blockchains provide are almost absolute in their guarantees under the correct implementation + resource commitment to the network.

Bitcoin’s Most Fundamental Value Proposition

We hear a variety of reasons for why bitcoins might be valuable. Some of these reasons include sound money, a hedge against central banking, etc. These are all true but provide reasons that are external to the network itself. To date I have not seen the true value proposition for Bitcoin and its unit of account, bitcoins, described anywhere at the most fundamental level. By establishing the fundamental value proposition, we can work our way into the more social realms that are popularly discussed. So, before concluding, we will attempt to concisely explain it below:

Bitcoins are valuable because they are the irreplaceable, scarce incentive token that serve as the glue to a distributed, novel, triple-entry accounting scheme that disintermediates money + accounting + third party verification by combining them into a single, software-based product. Demand exists to use this software because it offers absolute assurance in accounting for value transfer / storage, which is a proposition that no other accounting system on the planet is capable of offering. Bitcoin’s accounting scheme is also unique in that it possesses the properties that enable intense utility-based assurances for users such as censorship resistance and asset seizure resistance. These very features make bitcoins a popular value storage

vehicle for "aggressive uses and users", who also have the benefit of easier access to it as a result of its digital + open build. The combination of accounting + utility based assurances + digital / open build makes bitcoins an ideal tool for protection against the current monetary regime, and ultimately a quality candidate for a market-selected "sound money".

Final Thought

Double entry accounting has survived 600–700 years and has more than capably supported a wide variety of enterprises, ranging from textile firms of the industrial revolution to space travel companies of today. This accounting scheme has outlived 99% of the businesses built on top of it and has provided such a large amount of value that it would be futile to attempt to make the calculation. With this in mind—it's still worth wondering what an investment in double entry within its first 10 years would have amounted to today.

Why? Because the opportunity to invest in Proof of Work + Triple Entry accounting is available via Bitcoin. The ability to provide absolute assurance from an accounting perspective is unique historically and completely underappreciated by the market at large. Nonsense from the "Blockchain, not Bitcoin" era of 2015–2016 scared people off from the accounting side of the coin, but it's time we come full circle to fully appreciate Bitcoin for the accounting beast that it is. This robust accounting layer enables everything that we appreciate about Bitcoin and will likely propel it forward in the global money battle that is already well underway. For this reason it is imperative that all involved understand Bitcoin as a money AND accounting revolution.

Big thank you to Oke Pearson (@OkePearson on Twitter) for his help in reviewing this piece + all accounting related material included within.

Sources:

1. **Triple Entry Accounting** *The digitally signed receipt, an innovation from financial cryptography, presents a challenge to classical double entry...* nakamotoinstitute.org
2. **Formalizing and Securing Relationships on Public Networks - Satoshi Nakamoto Institute** *Computers make possible the running of algorithms heretofore prohibitively costly, and networks the quicker...* nakamotoinstitute.org
3. **The Ricardian Contract** *Describing digital value for payment systems is not a trivial task. Simplistic methods of using numbers or country...* nakamotoinstitute.org 4, **Money, Blockchains, and Social Scalability**

Blockchains are all the rage. The oldest and biggest blockchain of them all is Bitcoin, which over its eight-year… nakamotoinstitute.org
4. **A History of Accounting and Accountants** *Edit description* books.google.com
5. **Unpacking Bitcoin's Assurances** *Dis-aggregating the system's guarantees* medium.com
6. **#1: Assurances in Crypto** *A Breakdown of BTC, DCR, & Everything Else* blog.goodaudience.com
7. **Double Entry: How the Merchants of Venice Created Modern Finance** *"Lively history. . . . Show[s] double entry's role in the creation of the accounting profession, and even of capitalism…* www.amazon.com

Crypto Voices 2019 Q1 Global Monetary Base

By Crypto Voices

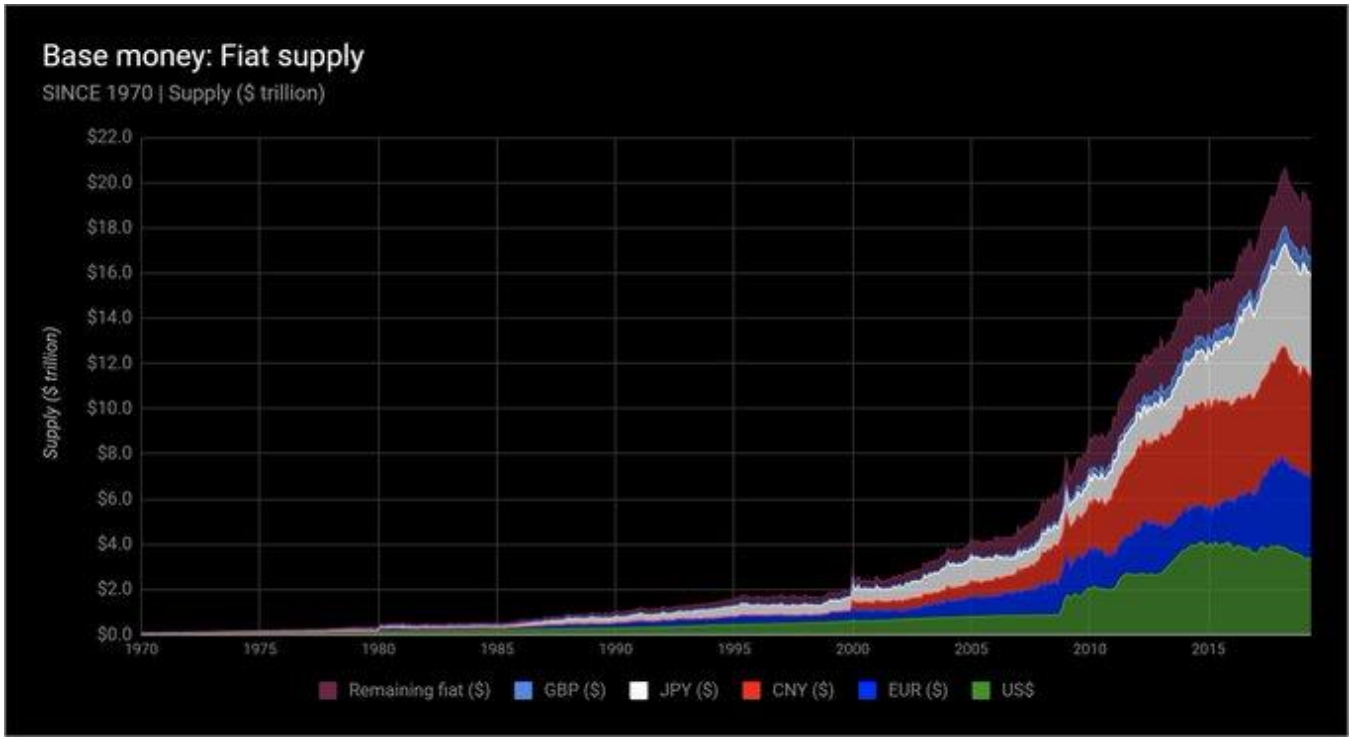
Posted May 22, 2019

1. Here is the @crypto_voices 2019 Q1 release on the global monetary base. This is the only comparable money supply with Bitcoin's 21 million. #Bitcoin is currently the 12th largest money in the world. To dig

deeper on what it all means, follow on below. 👇This is installment #4.
2. Gold & silver is base money of the past. Government fiat is base money today. It comprises both physical cash… and a digital cash component! Bitcoin may be base money of the future. Before we get to the charts, it's important to clarify a few common misconceptions in money.
3. The first is everyone looking to value Bitcoin always jumps to the "narrow" or "broad" money supplies (M1/M2/M3). This is incorrect. The reason is those money supplies represent "claims" on something else. What is that something else? Answer: the base money supply!!
4. Fiat base money today includes both physical (notes & coins) and digital (bank reserves at the central bank) components. Think of the digital part as the "account" each bank holds with its central bank. This & only this money supply compares economically with 21 million BTC.
5. Another mistake that's often made when comparing bitcoins to the analog monetary world is looking at a simple chart like US M1, or

Eurozone M2. Besides again being incorrect on the M1/M2/M3 comparison, this method is inadequate because Bitcoin is global, and those… are not.

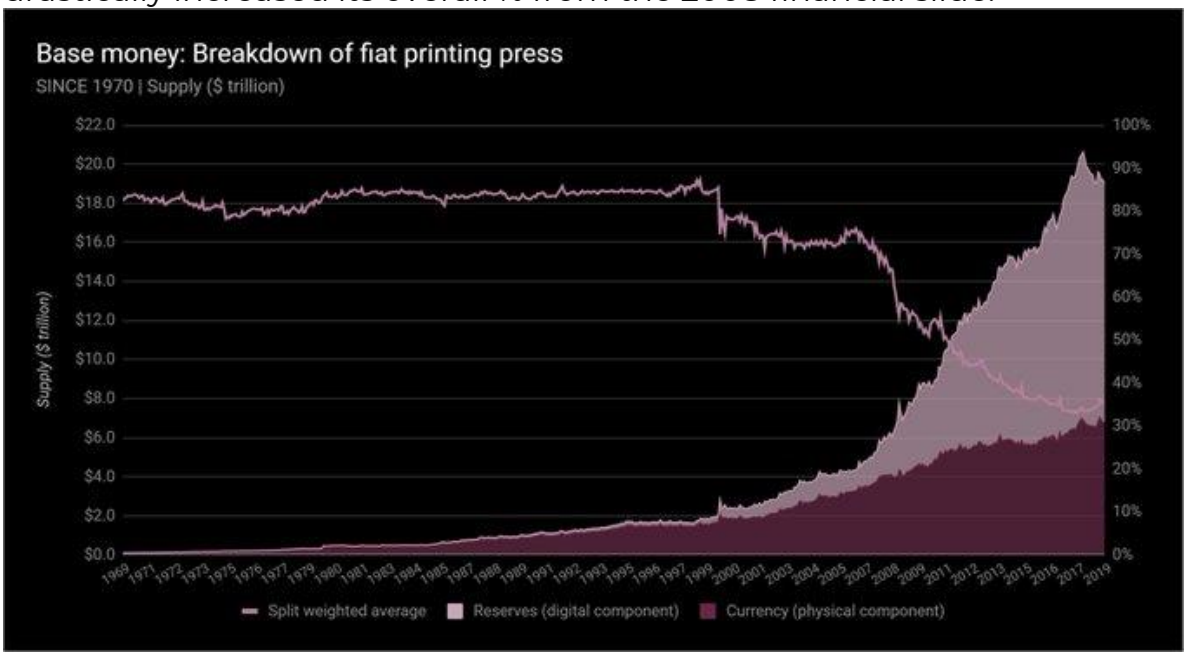
6. We can't simply look at one or two nation states' base money supplies to gauge any kind of market depth. The sample must be global. We've done that here, tracking the top 30 floating currencies in the world. This



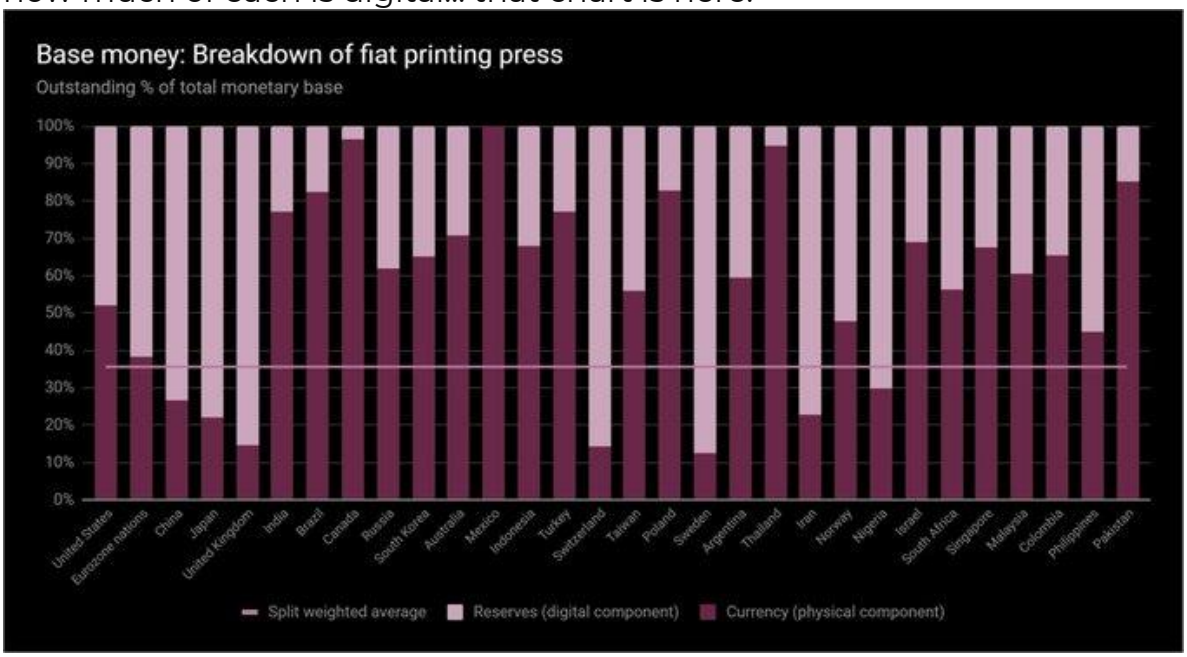
is how the real, global fiat base money supply looks since 1970.

7. This top 30 base money sample in fact covers 95% of global GDP, 114 countries, and 83 currencies. Why? The euro is one reason. The other is all the remaining countries/currencies either use one of these top 30 directly, or are legally pegged or fixed to one via currency board.
8. Let's look again at the global base money supply curve since 1970, but this time see how the split shakes out between physical versus digital base money. Note how bank reserves (the digital printing press)

drastically increased its overall % from the 2008 financial slide.

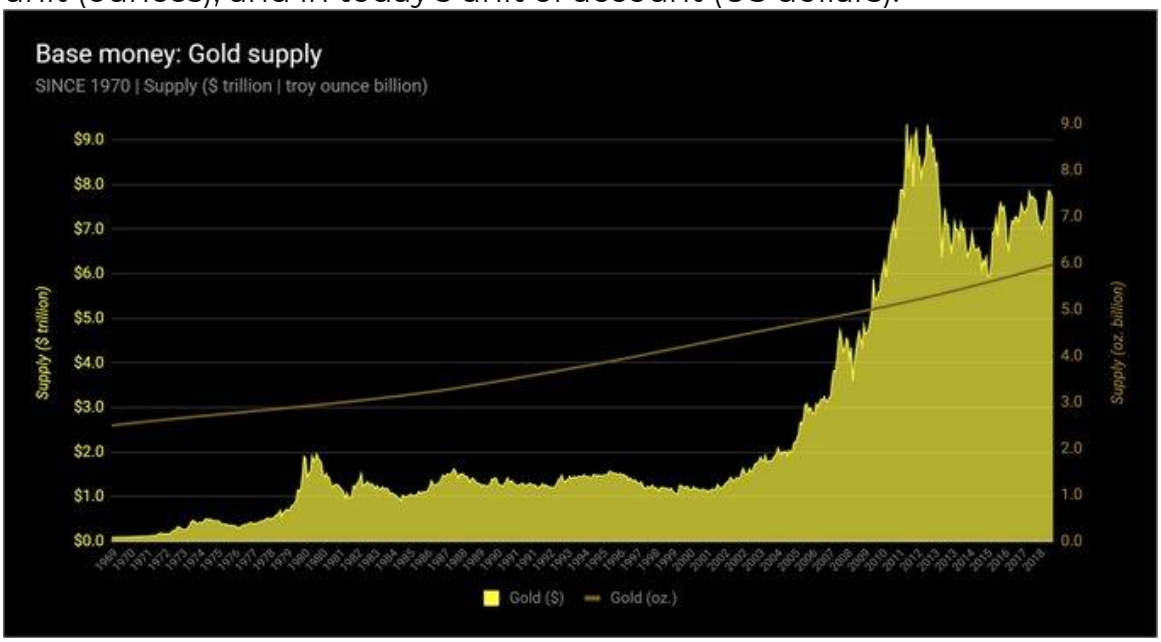


9. And for the current breakdown of each country's printing press - of the top 30 monetary bases - how much of each currency is physical, and how much of each is digital... that chart is here.

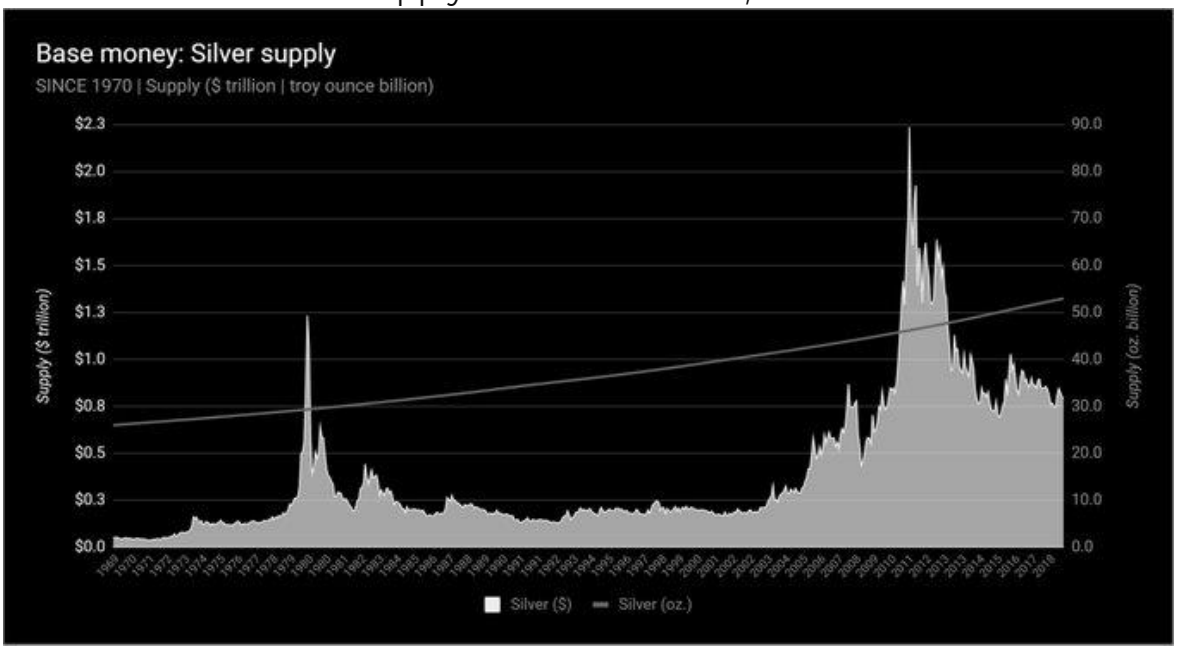


10. Final point on fiat money. The monetary base is in fact a graph of the money monopoly today; meaning, it is the source of the printing press, and only central banks control this. If you're curious where to find it, the answer is simple: the balance sheet of each central bank!
11. Now let's look at gold. Though central banks hold gold, it no longer acts as base money. This is another topic for another time, but everyone

should still understand the global gold supply in both its native market unit (ounces), and in today's unit of account (US dollars).

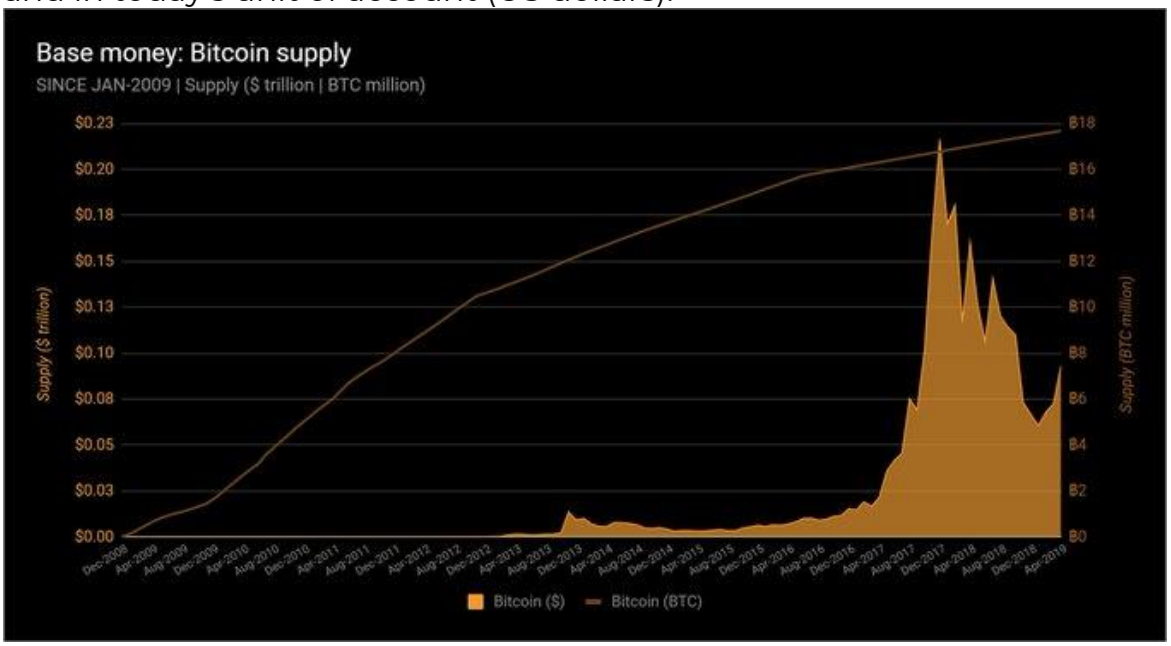


12. Now silver. It's true, 50%+ of silver demand today is industrial, not remotely monetary. But silver was base money well before gold. 50 billion ounces of the stuff has been mined throughout humanity, and it's worth it to scan its supply curve. Since 1970, this is silver.

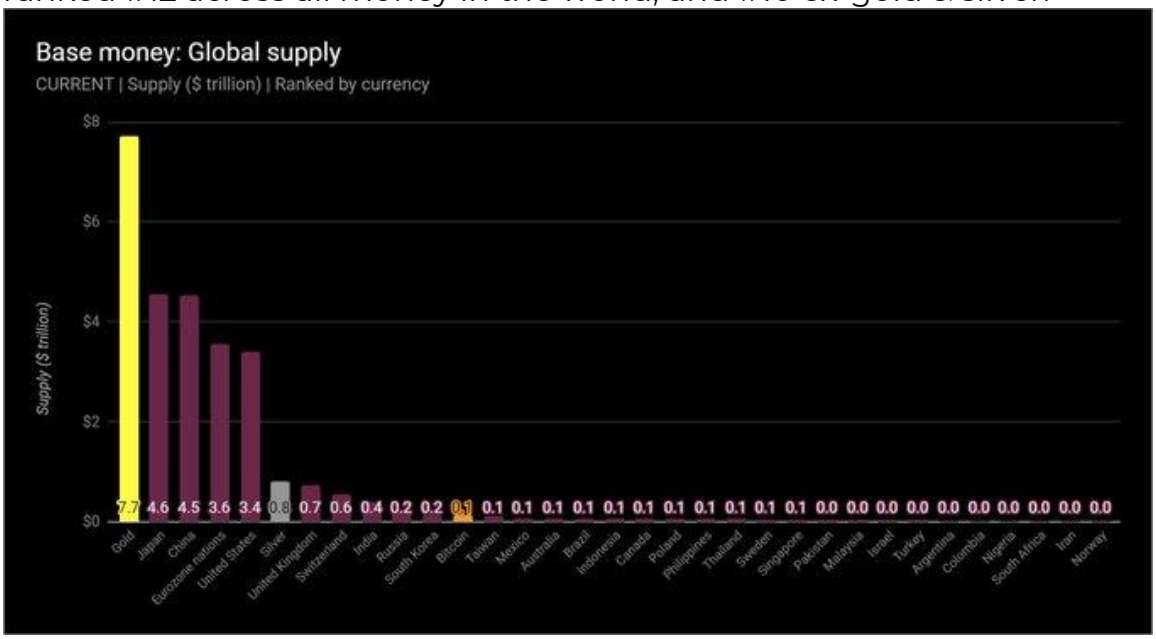


13. And finally Bitcoin. Bitcoins are limited by the protocol to an eventual 21 million in supply by the year 2140. Bitcoins may circulate as base money of the future. Here is its global supply, both in native units (bitcoins),

and in today's unit of account (US dollars).



14. And now we'll put them altogether - global fiat, gold, silver, and bitcoin - today. Without further commentary, note that Bitcoin the system is ranked #12 across all money in the world, and #10 ex-gold & silver.



15. And for a broad, historical ranking in table format, for the entirety of Bitcoin's history since 2009, that information is here.

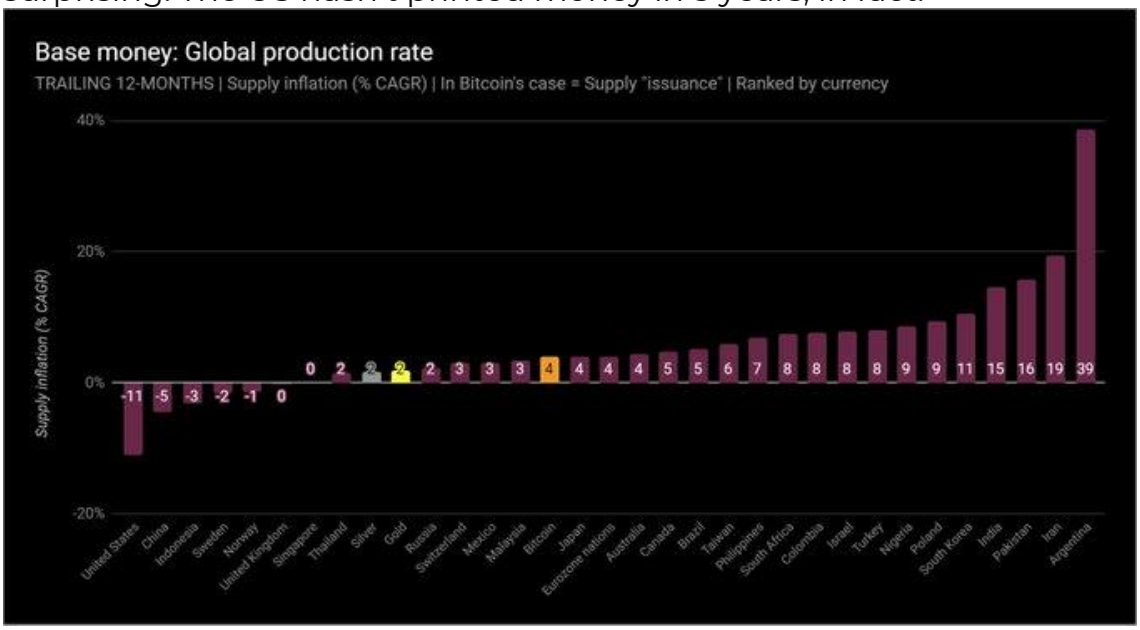
PROGRESSION OF THE WORLD'S MONETARY BASE
~ Gold & Silver | Base money of the past ~
~ Top 5 fiat currencies | Base money of the present ~
~ Bitcoin | *Possible* Base money of the future ~

Year End	Gold	JPY yen	CNY yuan	EUR euro	USD dollar	Silver	GBP sterling	Bitcoin
Dec-2009	#1 $5.45	#5 $1.14	#2 $2.11	#4 $1.72	#3 $2.05	#6 $0.76	#7 $0.33	n/a $0.00
Dec-2010	#1 $7.17	#6 $1.34	#2 $2.81	#4 $1.54	#3 $2.04	#5 $1.42	#7 $0.31	n/a $0.00
Dec-2011	#1 $7.95	#5 $1.62	#2 $3.57	#4 $1.98	#3 $2.64	#6 $1.30	#7 $0.35	n/a $0.00
Dec-2012	#1 $8.76	#5 $1.60	#2 $4.05	#4 $2.16	#3 $2.69	#6 $1.44	#7 $0.56	n/a $0.00
Dec-2013	#1 $6.49	#4 $1.92	#2 $4.48	#5 $1.82	#3 $3.74	#6 $0.94	#7 $0.61	n/a $0.01
Dec-2014	#1 $6.62	#4 $2.30	#2 $4.74	#5 $1.67	#3 $3.95	#6 $0.77	#7 $0.58	n/a $0.00
Dec-2015	#1 $5.93	#4 $2.96	#2 $4.27	#5 $2.01	#3 $3.87	#6 $0.69	#7 $0.56	n/a $0.01
Dec-2016	#1 $6.54	#3 $3.75	#2 $4.45	#5 $2.57	#4 $3.56	#6 $0.81	#7 $0.56	#31 $0.02
Dec-2017	#1 $7.51	#3 $4.26	#2 $4.95	#5 $3.67	#4 $3.88	#6 $0.89	#7 $0.74	#11 $0.22
Dec-2018	#1 $7.58	#3 $4.60	#2 $4.81	#4 $3.60	#5 $3.42	#6 $0.81	#7 $0.73	#19 $0.07
Mar-2019	#1 $7.71	#2 $4.57	#3 $4.53	#4 $3.55	#5 $3.40	#6 $0.80	#7 $0.73	#12 $0.14

All figures in $US trillion; ranked at displayed period end, according to market exchange rates with US$.
Note on last row: Unlike all other currencies in this table whose value reflects the latest period, Bitcoin's latest value is ranked as of 22-May-2019.
Bitcoin ranked once broken into top-30 fiat currencies' monetary base value.

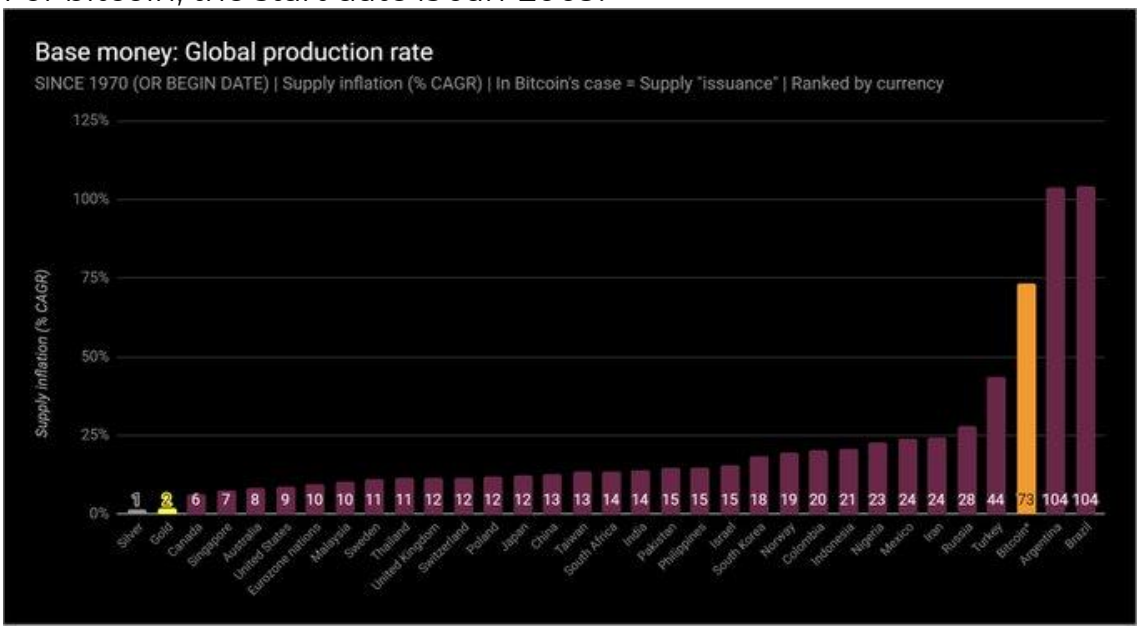
16. Now for the main event of this analysis: Inflation. Inflation today means "price increases." It's usually measured by the central bank and usually wrong. There is no way all prices can ever be measured in a simple index. The input variables are changed all the time to boot.
17. When we analyze inflation, we are using the classical definition, which is "monetary inflation." In other words, "money growth," or "money production." Understanding this rate of increase can be very, very helpful when trying to understand money.
18. Inflation is one of the most important things to understand about money, in fact. Money growth inflation reflects scarcity. But to be clear… The charts * that follow * have nothing * to do * with price growth * or prices * at all.
19. Let's jump right to the summary this time. This is the last 12 mos. of all base money growth. Remember, this is "unit" growth. % changes in dollars, euros, or yen, ounces of gold, or bitcoins. Maybe the results are

surprising. The US hasn't printed money in 5 years, in fact.

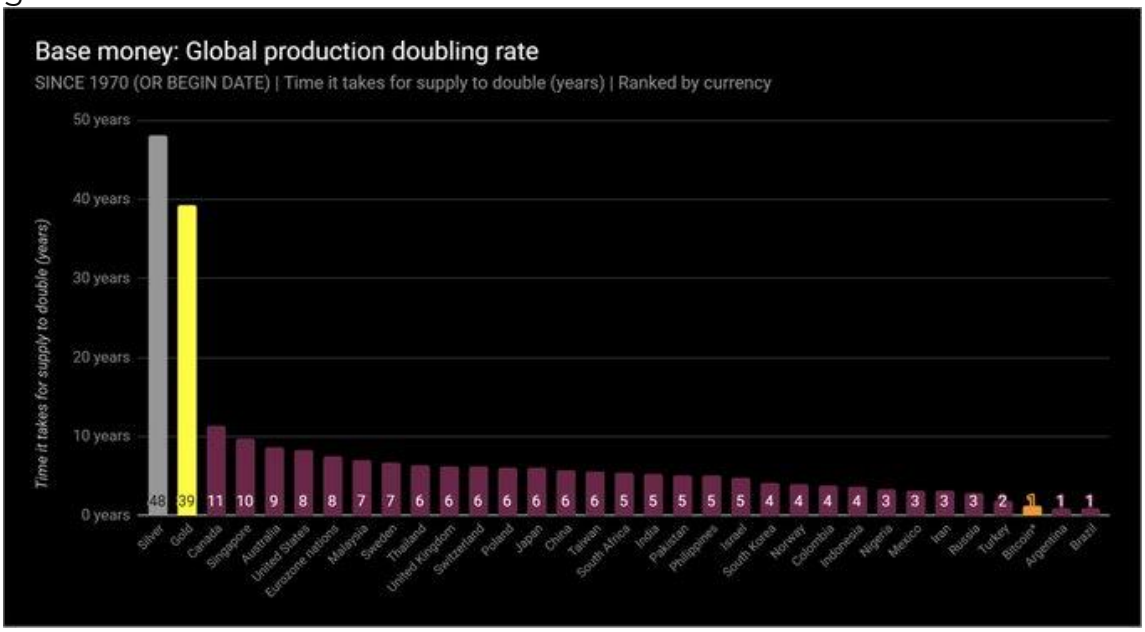


20. But we need to look deeper. It helps to look long-term. Remember the global fiat supply curve? 👆 In 1970, the US$ equivalent of global base money was $100 billion. Today: $19.2 trillion. What does this mean? To understand it, you need to understand compound annual growth.
21. Compound annual growth is an extremely important metric. It's "stronger" than a simple, annual rate (**Compound Returns vs. $ Over Time — Crypto Voices** https://cryptovoices.com/compound-returns-vs-usd-over-time/). We can use this rate to understand investment returns, or long-term trends like population growth. We can also derive doubling time from this figure.
22. So let's start with the compound annual growth rates for the global monetary base since 1970. 50 years of data. About half the countries' data goes back this far. For the rest, % displayed is since their start date.

For bitcoin, the start date is Jan-2009.

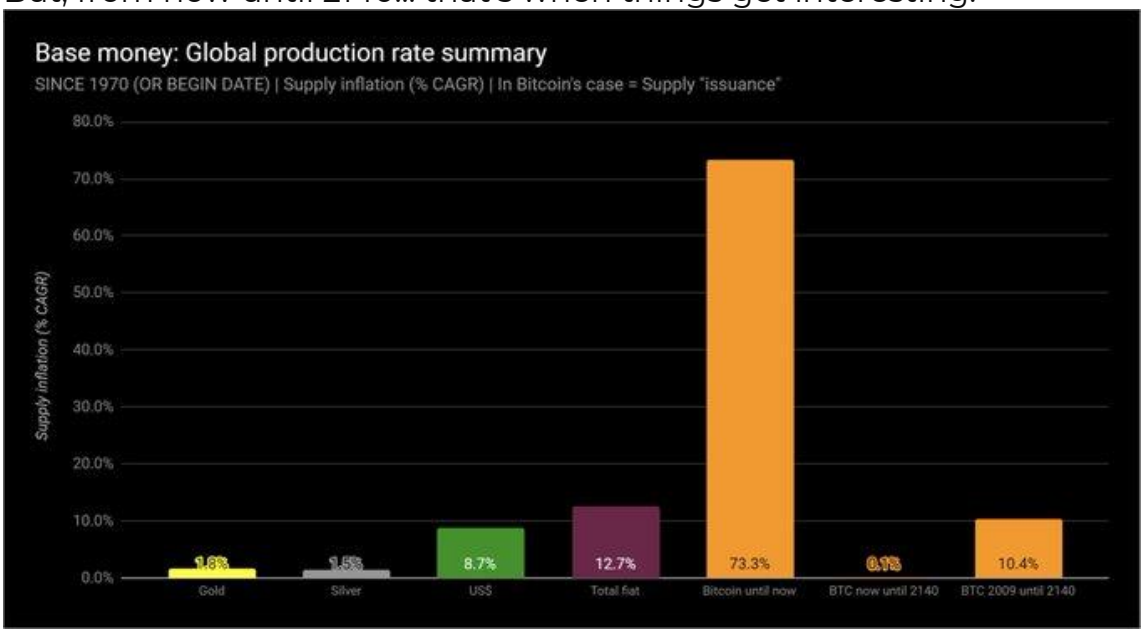


23. Doubling time also helps. From compound growth %, we can determine exactly how long it takes for an asset's supply to double. Here is the exact same chart as just shown, since 1970 (and since 2009 in Bitcoin's case), but displaying doubling time instead of compound growth.

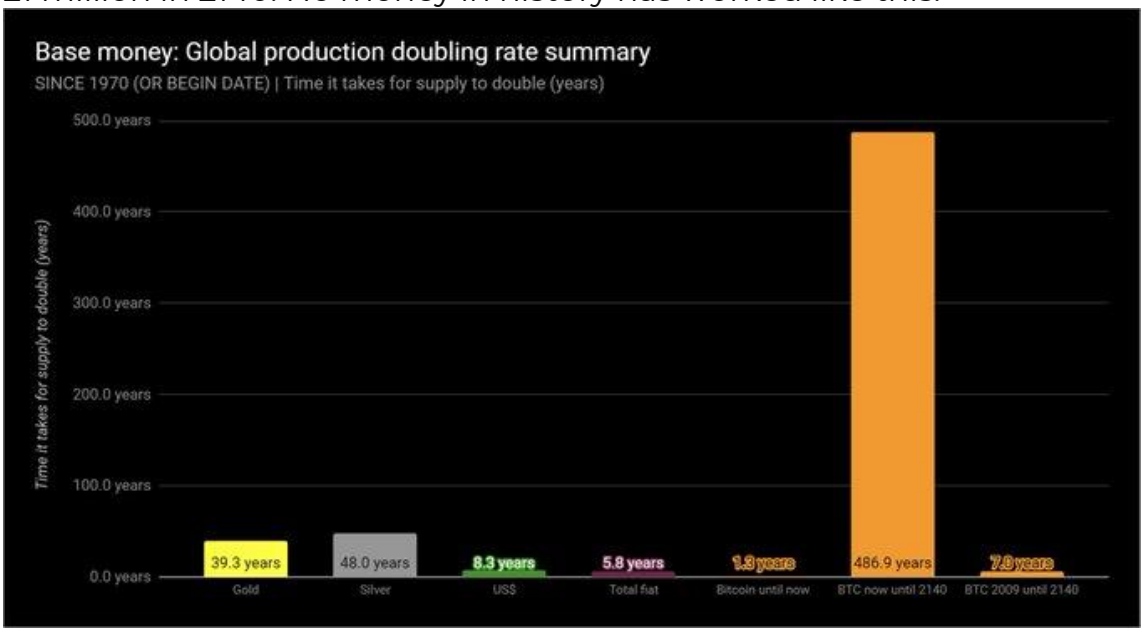


24. It should be clear why gold and silver arose as past base money. 'Twas very difficult to inflate them, and thus with low inflation rates they had long supply-doubling times. Fiat base money has typically been much quicker to double. Bitcoin... needs more explanation.

25. These next 2 charts will make it easier to understand how Bitcoin's supply works. From 2009 until now, yes, 50 bitcoins grew to 17.7 million. That's a 73% compound annual growth rate, or doubling every 1.3 years. But, from now until 2140... that's when things get interesting.



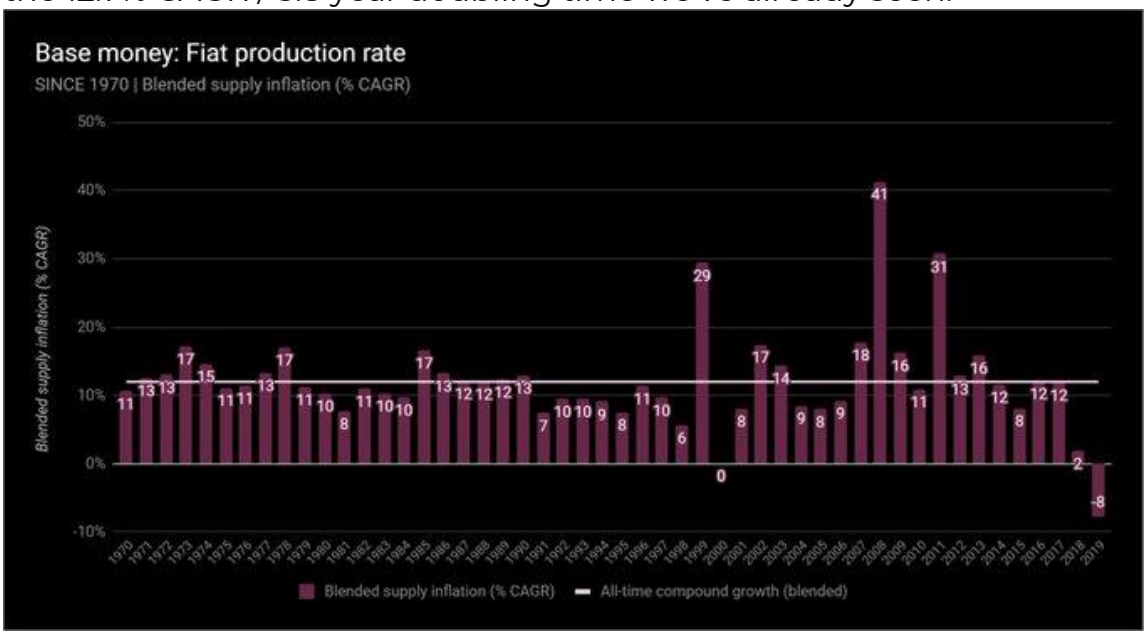
26. Notice how the supply of bitcoins will only grow at 0.1% per year, or double every 483 years. And it gets even more unique, as the Bitcoin protocol won't allow that doubling to happen, as it's supply will cap at 21 million in 2140. No money in history has worked like this.



27. To clarify, these are the long-term trends of past, present, & possibly future base money, since 1970: -Gold: 1.8% (2x in 39 yrs) -Silver: 1.5% (2x in

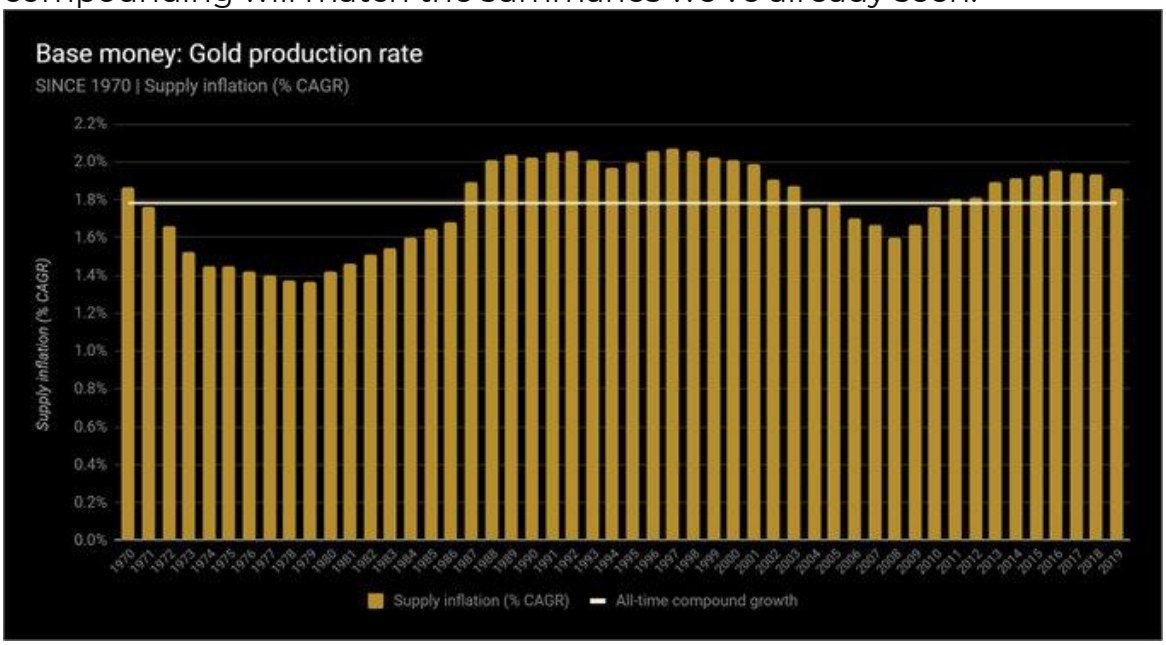
48 yrs) -US$: 8.7% (2x in 8 yrs) -Global fiat: 12.7% (2x in 6 yrs) -50 BTC in yr. 2009 to 21 million BTC in yr. 2140: 10.4%

28. Let's look back on a 50 year time series again, this time w/ inflation rates. Here is the total global fiat base money inflation rate, weighted averaged by each currency's US$ equivalent. Notice it overall matches the 12.7% CAGR / 5.8 year doubling time we've already seen.

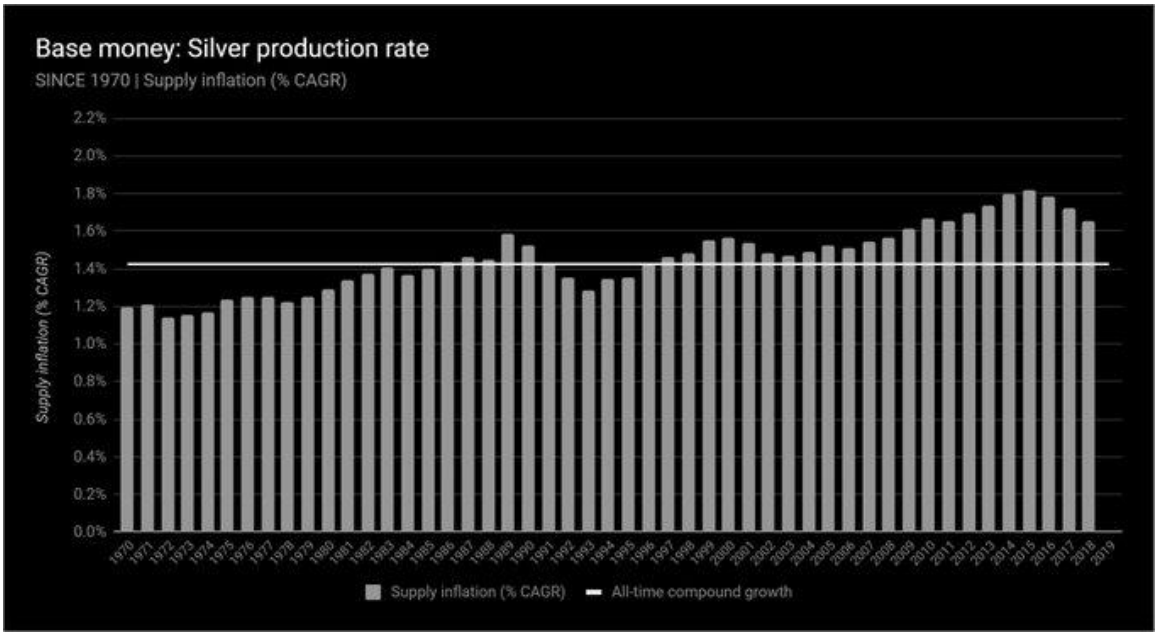


29. Quick note on prior slide. What happened in 1999? Ppl were taking cash out like mad before Y2K. Interesting to note, 2018 and 2019's trend are the lowest (& negative) growth rates of base money ever, as central banks try to unwind the massive stimuli from 2008 through 2013.

30. Here's gold. Same concept. Notice again the series' overall compounding will match the summaries we've already seen.

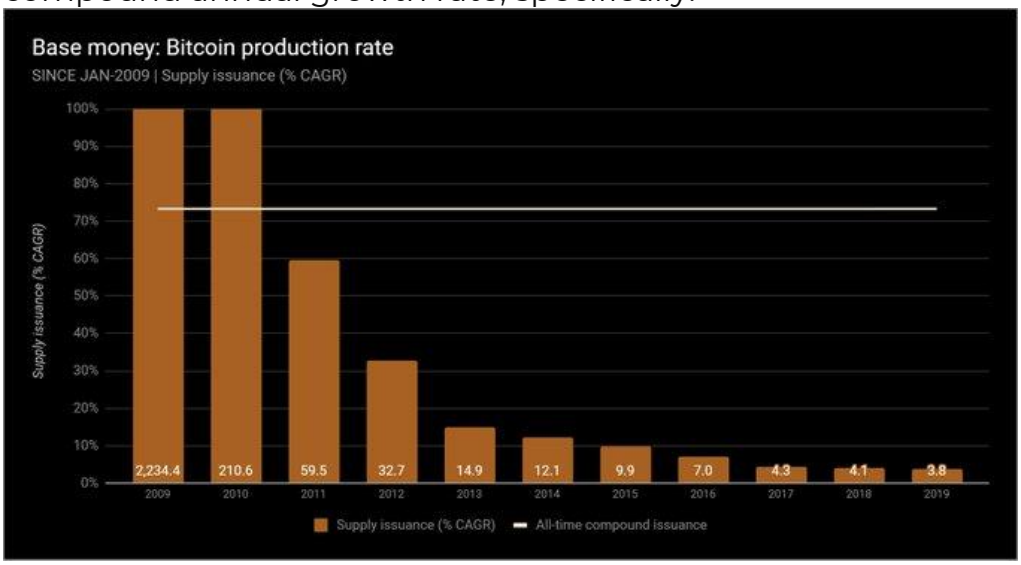


31. And here's silver. Same deal.



32. And now Bitcoin. Remember why the overall compound growth, thus far, is so high, and why it will never be that high again. And now is about the time for a clarification note on the Bitcoin system's

compound annual growth rate, specifically.

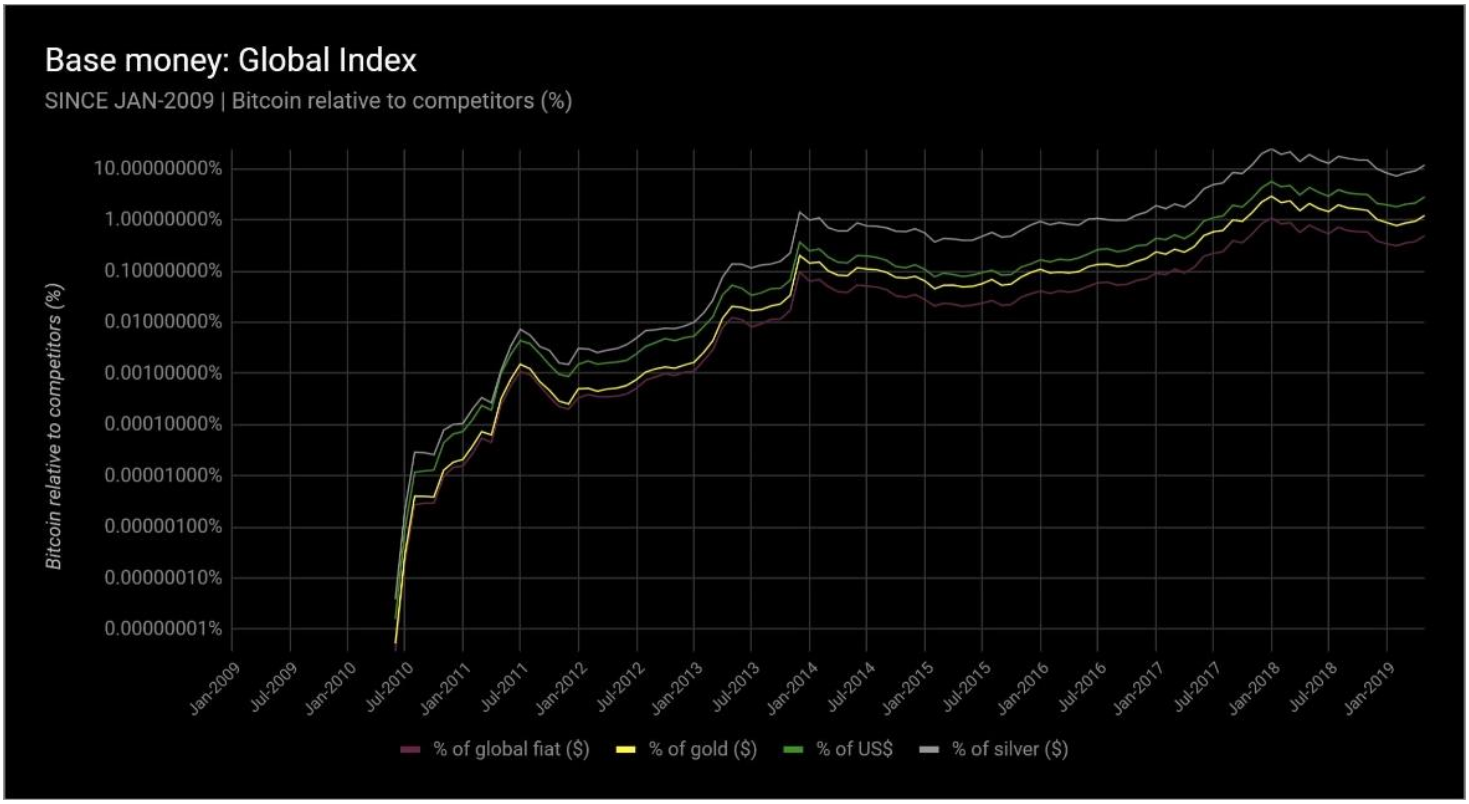


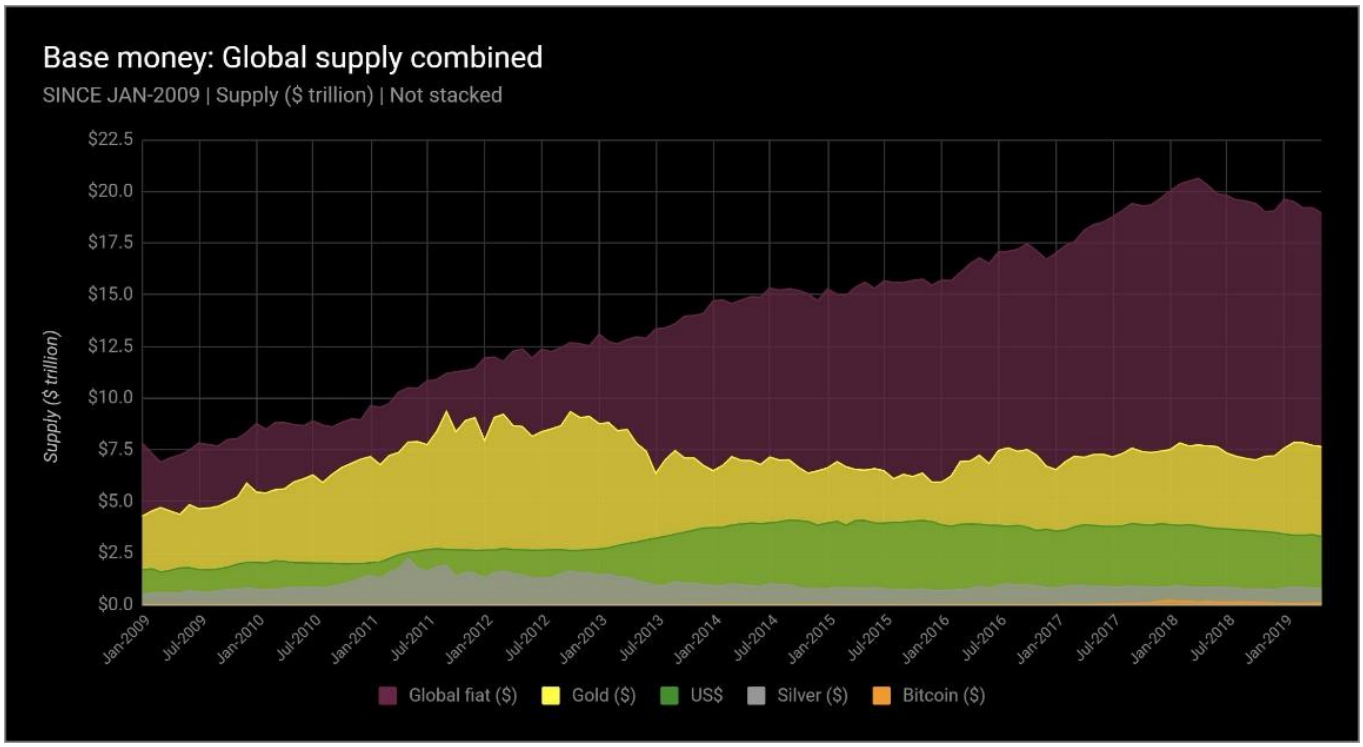
33. Notice the phrase “supply issuance” for Bitcoin’s chart titles, & not “inflation.” Bitcoin’s “inflation,” economically, is already “baked in.” Everyone knows its max supply: 21 million coins. As already demonstrated, we can predict its growth rate & doubling rate until 2140.
34. The fact that it’s predictable makes all the difference. In money or anything, this is unique. So for Bitcoin’s supply growth, “inflation” is not the best term. “Coin issuance” is more apropos, because the total supply is already known by all… unlike fiat, or even gold!!
35. Alright. Now that we’ve seen all the data, let’s finally take a quick detour to some price chat, because even though I told you none of the above covers prices, I know you’re thinking about how all of this monetary inflation has affected or will affect prices.
36. Milton Friedman said, “Inflation is always and everywhere a monetary phenomenon.” He meant price inflation (not graphed above) always and everywhere follows money inflation (painstakingly graphed above).
37. The rub is it is *impossible* to predict how and when price inflation will happen. Hate to be the wet blanket, but it’s true. Hyperinflations (of prices) are impossible to predict. The best we can do is measure the money supply and its growth, as we’ve done here.
38. But we can say this: If the *supply* of base money increases, and if there is no or a lesser increase in the *demand* for that money, then ceteris paribus, prices will rise. Ceteris paribus, a growing base money supply will always undermine that money’s purchasing power.
39. A few notes before the final summary. Almost done! Remember these are the top 30 currencies in the world over the past 50 years. Zimbabwe

& Belarus don't make the cut, but as their market size is so tiny, their hyperinflations would barely move the needle on what's presented.

40. For the euro, its accounting creation began in 1999, and it started circulating in 2002. The ECB estimates a physical currency stock back to 1980. So from 1980 until 1999, we do use this physical currency for euro base money inflation, and then add in bank reserves from 1999.
41. To be absolutely clear on the global fiat blended inflation rate: it's calculated using a weighted factor of each country's base money supply, based on how large their US$ equivalent actually is, during that period. This weight evolves as more currencies are added.
42. As mentioned, only about 15 currencies have data back to 1970. For those that weren't, they didn't factor into that period. For example, the US dollar's weight itself was 63% of the pie in 1970, and only 17.5% today, as (among others), data on China begins only in Dec-1999.
43. Regarding compound annual growth rates: they're always calculated from monthly fiat unit growth, then compounded to annual (to the 12th exponent). This is necessary due to cases like Brazil and Argentina, which had 6 and 4 different currencies respectively, since 1970 alone.
44. Continuing, a compound annual growth rate from a 1970 currency to 2019 currency doesn't make sense for Brazil. So the monthly rate must be taken across time and then compounded, ignoring those 6 months when the central bank reset (slashed zeroes) from the old currency.
45. And finally, the mechanics of this method (compounding monthly growth rates to annual) were of course repeated across gold, silver, and bitcoin's supply curves, for consistency.
46. On our podcast @crypto_voices, @fernandoulrich I explore the varying economic nuances of Bitcoin as a contender for the global monetary base, for global money.
47. To sum it up, this graphic includes all items. Print it out if you like. The base money of 114 nations is reflected inside the top 30 currencies, as well as gold, silver, and the supply of bitcoins. It is a supply-side summary of essentially all base money in the world.
48. The exhibits are located here:**Base Money — Crypto Voices**https://cryptovoices.com/basemoney Fiat base money is sourced from central bank balance sheets, wonderful gold and silver history from Nick Laird, and bitcoin from @coinmetrics and @coinmarketcap.

49. These final graphics show how Bitcoin's supply (US$ equivalent) compares with all other monetary bases, past and present. We have been very pleased that some of #CryptoTwitter has been referring to this as the #RealBitcoinDominanceIndex.





50. More to come in the future, the 2019 Q2 global monetary base will next be released and covered in depth @hodlhodl 's #bh2019 conference in Riga. /fin

The Crypto Voices *Global Monetary Base*

The MONETARY BASE is also known as Base Money, High-Powered Money, Outside Money, and Reserve Money, among other names.
The MONETARY BASE is the ultimate asset of settlement. It is the most irreducible form of "Money."
It is presented here, globally, across three basic time periods: Past, present, and future.

This table summarizes present base money; namely, the global fiat supply:

Fiat production	Fiat unit	Exchange rate regime	*Present* base money: Fiat supply				GDP rank	Compound annualized growth rates			Doubling rate since begin date	Begin date	Latest date
			Fiat trillion	US$ trillion	Fiat weight	Global rank		Latest month (more noise)	TTM (less noise)	Since begin date (least noise)			
United States	dollar	Free floating	$3.40	$3.40	17.7%	5	1	10.4%	-11.0%	8.7%	8.3 years	Dec-1969	Mar-2019
Eurozone nations	euro	Free floating	€3.16	$3.55	18.5%	4	2	-13.8%	4.1%	9.7%	7.5 years	Jan-1980	Mar-2019
China	yuan	Crawl-like arrangement	¥30.37	$4.53	23.6%	3	3	0.6%	-4.5%	12.7%	5.8 years	Dec-1999	Mar-2019
Japan	yen	Free floating	¥506.29	$4.57	23.8%	2	4	24.0%	4.0%	12.2%	6.0 years	Jan-1970	Mar-2019
United Kingdom	pound sterling	Free floating	£0.56	$0.73	3.8%	7	5	-27.7%	-0.2%	11.7%	6.3 years	Dec-1969	Mar-2019
India	rupee	Floating	₹27.70	$0.40	2.1%	9	6	54.5%	14.7%	13.9%	5.3 years	Jun-2001	Mar-2019
Brazil	real	Floating	R$0.29	$0.07	0.4%	16	7	-13.2%	5.2%	104.3%	1.0 years	Dec-1969	Mar-2019
Canada	dollar	Free floating	$0.09	$0.07	0.4%	18	8	3.9%	4.9%	6.3%	11.4 years	Dec-1969	Mar-2019
Russia	ruble	Free floating	15.80 ₽	$0.23	1.2%	10	9	-5.8%	2.3%	28.1%	2.8 years	Dec-1994	Mar-2019
South Korea	won	Floating	₩180.43	$0.16	0.8%	11	10	-1.7%	10.6%	18.3%	4.1 years	Dec-1969	Mar-2019
Australia	dollar	Free floating	$0.11	$0.08	0.4%	15	11	2.2%	4.4%	8.3%	8.7 years	Feb-1975	Mar-2019
Mexico	peso	Free floating	$1.56	$0.08	0.4%	14	12	-12.8%	3.0%	24.0%	3.2 years	Dec-1985	Mar-2019
Indonesia	rupiah	Stabilized arrangement	Rp993.61	$0.07	0.4%	17	13	15.0%	-3.2%	20.7%	3.7 years	Jan-1990	Mar-2019
Turkey	lira	Floating	₺0.17	$0.03	0.2%	27	14	32.0%	8.1%	43.6%	1.9 years	Dec-1980	Mar-2019
Switzerland	franc	Floating	CHF0.56	$0.56	2.9%	8	15	-7.0%	3.0%	11.7%	6.3 years	Dec-1969	Mar-2019
Taiwan	NT dollar	Free floating	NT$4.12	$0.13	0.7%	13	16	-31.3%	5.8%	13.4%	5.5 years	Dec-1969	Mar-2019
Poland	złoty	Free floating	0.26 zł	$0.07	0.4%	19	17	-35.0%	9.4%	12.1%	6.1 years	Dec-1996	Mar-2019
Sweden	krona	Free floating	0.48 kr	$0.05	0.3%	22	18	-66.4%	-1.5%	11.0%	6.7 years	Dec-1969	Mar-2019
Argentina	peso	Floating	$1.35	$0.03	0.2%	28	19	-36.2%	38.7%	103.9%	1.0 years	Dec-1969	Mar-2019
Thailand	baht	Floating	฿1.85	$0.06	0.3%	21	20	-18.5%	1.5%	11.4%	6.4 years	Dec-1970	Mar-2019
Iran	rial	Free floating	Rial2,345.10	$0.01	0.1%	32	21	31.4%	19.4%	24.3%	3.2 years	Jun-1973	Sep-2018
Norway	krone	Free floating	0.09 kr	$0.01	0.1%	33	22	70.5%	-1.3%	19.4%	3.9 years	Dec-1969	Mar-2019
Nigeria	naira	Stabilized arrangement	₦7.25	$0.02	0.1%	30	23	14.1%	8.7%	22.7%	3.4 years	Jan-2000	Mar-2019
Israel	new shekel	Floating	₪0.13	$0.04	0.2%	26	24	164.6%	7.9%	15.4%	4.8 years	Jan-1995	Mar-2019
South Africa	rand	Floating	R0.26	$0.02	0.1%	31	25	20.1%	7.6%	13.7%	5.4 years	Dec-1969	Mar-2019
Singapore	dollar	Stabilized arrangement	$0.07	$0.05	0.3%	23	26	-43.8%	0.0%	7.4%	9.8 years	Jan-1991	Mar-2019
Malaysia	ringgit	Floating	RM0.16	$0.04	0.2%	25	27	-1.9%	3.4%	10.3%	7.0 years	Dec-1975	Mar-2019
Colombia	peso	Floating	$89.77	$0.03	0.2%	29	28	11.6%	7.7%	20.4%	3.7 years	Jan-1982	Mar-2019
Philippines	peso	Floating	₱3.23	$0.06	0.3%	20	29	86.3%	6.9%	14.6%	5.1 years	Jul-1993	Mar-2019
Pakistan	rupee	Stabilized arrangement	Rs5.82	$0.04	0.2%	24	30	1.7%	15.8%	14.5%	5.1 years	Dec-2004	Mar-2019
Global fiat supply				**$19.20**	**100%**			**3.3%**	**-0.5%**	**12.7%**	**5.8 years**	**Dec-1969**	**Mar-2019**

*The above stock of fiat base money is sourced from central bank balance sheets. It reflects the following breakdown, **all except** for the line "Remaining FX regimes:"*

*Exchange rate regime**	*Countries*	*Currencies*	*% of global GDP*	*Notes:*
As included in fiat table	***48***	***30***	***90.3%***	***Actually included in above table.***
No separate legal tender	*13*	*n/a*	*0.3%*	*De facto included in above table.*
Currency board	*11*	*11*	*0.6%*	*De facto included in above table.*
Conventional peg	*42*	*42*	*3.3%*	*De facto included in above table.*
De facto subtotal fiat table	***114***	***83***	***94.4%***	
Remaining FX regimes	*77*	*77*	*5.6%*	*Mostly "managed" FX regimes.*
Global total fiat supply	***191***	***160***	***100%***	

**These categorizations of currency exchange rate regimes are according to the IMF's "Annual Report on Exchange Arrangements and Exchange Restrictions 2018."*

*Fiat base money means, "**Physical currency in circulation**, plus **commercial bank reserves** deposited at the central bank." Both are **monopoly** privileges of a nation's central bank, and exist as **liabilities** on its balance sheet.*

*Fiat base money is thus **debt-based**, or **liability-based**.*

*Any other fiat money supply (M1/M2/M3/shadow banking) is comprised of **claims on base money**, and thus is **simply incomparable** to gold and bitcoin. To be clear, the author does not imply that claims on base money are fraudulent nor economically problematic.*

This table summarizes past base money; namely, the global gold & silver supply:

Gold & silver production	Metal unit	Exchange rate regime	Past base money: Gold & silver supply				Fiat multiple	Compound annualized growth rates			Doubling rate since begin date	Begin date	Latest date
			Troy ounce billion	US$ trillion	% of fiat	Global rank		Latest month	TTM	Since begin date			
Global gold supply	troy ounce	Market	5.96 oz.	$7.71	40.2%	1	2.5x	1.9%	1.9%	1.8%	39.3 years	Dec-1969	Mar-2019
Global silver supply	troy ounce	Market	52.64 oz.	$0.81	4.2%	6	23.6x	1.6%	1.7%	1.5%	48.0 years	Dec-1969	Dec-2018

Note this stock indeed reflects the "all-time, cumulative" supply of gold & silver ounces above ground; however, 10-15% of gold's production (50%+ for silver's) is continuously demanded/recycled by industry (arguably non-monetary). The supply is sourced from Nick Laird, USGS, and WGC.

Gold & silver are demanded naturally in the market. They are thus asset-based.

*$1,295 = **Market** gold price per ounce reflected in this summary.*
*$4,520 = **Theoretical** gold price per ounce **if total absorption of fiat** (existing gold value, plus fiat value, divided by gold supply). **Calculation, not prediction.***
*$15 = **Market** silver price per ounce reflected in this summary.*
*$380 = **Theoretical** silver price per ounce **if total absorption of fiat** (existing silver value, plus fiat value, divided by silver supply). **Calculation, not prediction.***

This table summarizes "possible," future base money; namely, the global bitcoin supply:

Bitcoin production	Digital unit	Exchange rate regime	*Future* base money: Bitcoin supply				Fiat multiple	Compound annualized growth rates			Doubling rate since begin date	Begin date	Latest date
			BTC million	US$ trillion	% of fiat	Global rank		Latest month	TTM	Since begin date			
Global bitcoin supply	bitcoin	Market	฿17.71	$0.14	0.7%	12	138.1x	3.8%	3.9%	73.3%	1.3 years	Jan-2009	May-2019

Note many studies have been conducted on Bitcoin's "actual" supply, some suggesting as many as 4 million bitcoins may have been permanently lost, frozen, or burned. The supply is sourced from Blockchain.info, and market price from CoinMarketCap.

If Bitcoin does indeed become base money of the future, the author envisions converting the "unit of account" in these tables, from US$, to BTC; though this future "date" is not known nor guaranteed, it will occur as bitcoin's "Fiat multiple" converges on 1.0x (and beyond).

*Bitcoin is demanded naturally in the market. It is thus **asset-based**.*

*$7,850 = **Market** price per bitcoin reflected in this summary.*
*$53,729 = **Theoretical** price per bitcoin **if total absorption of silver** (existing bitcoin value, plus silver value, divided by bitcoin supply). **Calculation, not prediction.***
*$443,413 = **Theoretical** price per bitcoin **if total absorption of gold** (existing bitcoin value, plus gold value, divided by bitcoin supply). **Calculation, not prediction.***
*$1,091,916 = **Theoretical** price per bitcoin **if total absorption of fiat** (existing bitcoin value, plus fiat value, divided by bitcoin supply). **Calculation, not prediction.***

Table updated as of: 22-May-2019
This table is for educational purposes only.

Find this interesting?
Come have a listen to our podcast.
We interview experts on money, bitcoin, and economics: *soundcloud.com/cryptovoices*
Crypto Voices is hosted by **Matthew Mežinskis** and **Fernando Ulrich**
Further info and detailed charts on global base money is here: *cryptovoices.com/basemoney*
@crypto_voices

CRYPTO VOICES

Bitcoin could change the game for foreign aid

By Alex Gladstein

Posted May 23, 2019

Today's humanitarian aid model is fundamentally broken. Whether you're a foundation making a donation to a nonprofit abroad, a government distributing aid to another government, or an individual sending emergency funds to family members across borders, your money only gets to where it needs to go after passing through intermediaries. Even in the simplest payment scenario, there's your bank; a coordination network; and the aid recipient's bank. But often, there are even more middlemen, with money moving along complex chains of third parties.

Such a system has obvious flaws. One is that each intermediary between you and the person or organization you are trying to help can delay, surveil, censor or steal your funds. In 2012, the UN's then-secretary general Ban Ki-moon said that "corruption prevented 30% of all development assistance from reaching its final destination."

Corruption aside, aid is at risk of getting eaten up along the way by overhead and administrative costs. In a research study done by Oxfam, only 7% of $28 million in US aid meant for Ghana provably made it into that country between 2013 and 2015 due to a lack of available data. Even if all goes well, it can take several days, weeks or even months for the recipient to finally receive the aid. And in a world where 1.7 billion people don't have a bank account, many can't even ultimately claim your donation.

The way aid moves today is corruptible, inefficient and slow. Research from organizations like the World Bank and the charity organization GiveDirectly suggests that distributing aid via direct cash transfers can be extremely effective. But how can we truly innovate in this area if there are so many intermediaries, even for small payments? Here's where Bitcoin changes the equation.

With Bitcoin, you can send money directly to anyone in the world in a matter of minutes. As your funds move to the recipient, it's not possible for third parties to censor or steal, as payment processing is done through a global competition, not by a centralized institution. To receive Bitcoin, you just need a smartphone with Bitcoin wallet software. According to the latest Pew data,

45% of citizens in emerging economies already own a smartphone today. While that means a large number of people in the world's poorest countries don't have the internet in their pocket yet, the fact that nearly half do is significant and this number will only continue to rise in the coming years. To receive Bitcoin, they don't need a passport or an ID or a bank account, and they don't have to ask permission from a government or a company to accept the funds. It is a true peer-to-peer transaction, done over a global, neutral payment rail. Of course, what isn't guaranteed is that the recipient can turn Bitcoin into local currency so they can buy the food, medicine or help that they need. That's a major challenge, but it's changing in a big way.

According to a global analysis of Bitcoin exchange data, individuals in West Africa, Latin America and East Asia are seeing a significant increase in their ability to sell Bitcoin for local currency. In an interview with researchers at the Open Money Initiative, I learned that the "liquidity time" of Bitcoin in Venezuela today is 15 minutes. Meaning, if you're in Caracas, I can send you Bitcoin from Miami and you can be holding bolivares in your hand within 15 minutes of my Bitcoin arriving on your phone. To give you an idea of the scale of Bitcoin activity in Venezuela today, consider that on April 26, 639 million bolivares were traded on the Caracas Stock Exchange. During that same week, the average daily volume of Bitcoin traded on one online platform alone — LocalBitcoins — was 5.2 billion bolivares.

LocalBitcoins is one of several online marketplaces — like Paxful, Hodl Hodl and Bisq — that work a bit like eBay. For example, if you're in New York and I'm in Lagos and you send me 1 bitcoin (roughly $7,800 at today's price), I'd create an account on the LocalBitcoins website and make a post, saying I'm selling 1 bitcoin for the going rate of around 2.8 million Nigerian naira. When I get a good offer, I click accept. I send my Bitcoin to LocalBitcoins, you send your naira to me, and my Bitcoin is only released to you when I confirm that I've received your naira. Or, we can choose to meet and make the trade in person, where you give me cash and I send you Bitcoin, smartphone-to-smartphone. And — voila — I just received Bitcoin from across the world and turned it into local, spendable currency.

When the highway blockade occurred on the Colombian border, preventing much-needed aid from getting into Venezuela, millions of dollars of Bitcoin were freely moving in and out. A big perk of using Bitcoin is that even when brick-and-mortar banks close, the Bitcoin network never shuts down. As global Bitcoin infrastructure improves and local exchange becomes more widely available, its value proposition for humanitarian aid — especially in

disaster zones and tough political climates — will only increase. If you are one of the billions of people stuck in a country restricted by capital controls, suffering from hyperinflation, trapped behind sanctions or simply lacking identification or a bank account, donors can now use Bitcoin to reach you directly.

If you are a gift-giving foundation, foreign ministry or development advisor, could sending your aid via Bitcoin be a better way? Bitcoin's peer-to-peer digital payments network could be the future of humanitarian aid.

The World Is Growing Tired of Government-Controlled Fiat Currencies

By Douglas French

Posted May 23, 2019

Here in the U.S. the financial markets are focusing on Fed Chair Jerome Powell's herky-jerky monetary messages while politically the news is Trump's two picks for the central bank board have taken themselves out of the running.

Herman "9-9-9" Cain and Stephen Moore couldn't take the heat and either withdrew their names from consideration, or their names where withdrawn via twitter. Both had plenty of baggage, but, what the two had in common was, in their pasts, mentions of returning to the gold standard. That is a no-no. Washington is full of #metoo offenders, but kooky #goldbugs are not allowed.

That kind of talk garners a bipartisan 86ing from serious contention.

Meanwhile, Sputnik News reports that Russia (Vlad and Elvira, Russia's central bank head) continues to ditch dollars in favor of the ancient relic that Washington so despises.

The new purchases continue a trend established at the start of the year, with Russia buying a whopping 31.1 tonnes in February, adding to 6.22 tonnes purchased a month earlier. Russia has now bought some 55.98 tonnes of gold in the first three months of 2019, putting it well on track to matching the average 200+ tonne purchase made annually over the past half-decade.

One wonders what Mr. Putin and Ms. Nabiullina, are up to? By the way, Ms. Nabiullina is not just a pretty face, she was named the best Central Bank Governor in Europe in 2016 by the international financial magazine, The Banker, besting the likes of Mario Draghi.

Her gold buying makes me think she has read Saifedean Ammous's *The Bitcoin Standard: The Decentralized Alternative to Central Banking*. Don't let the title fool you. This book is not the cover-to-cover crypto cheerleading/gold bashing other authors attempt to jam down our throats. Dr. Ammous Is

actually a Professor of Economics, and none other than “Black Swan” author Nassim Taleb wrote the introduction.

Professor Ammous’s *Tour de Force* begins where it should; the origins of money, then monetary metals, the government takeover of money, time preference, Austrian business cycle theory, money and freedom, and finally digital money. For those wanting to know what the heck a Bitcoin is, it may seem like a long wait. Changes in money don’t happen overnight. All of your questions about Bitcoin are answered in Chapter 10. However, with a bibliography loaded with Hoppe, Higgs, Hazlett, Mises, Raico, and Rothbard, don’t skip ahead.

If one didn’t know the title, a reader would swear Professor Ammous is making the case for a return to the gold standard: Not a phony Bretton Woods gold standard, but the real pre-WWI gold standard deal.

What makes gold such a great monetary metal is it’s high stock-to-flow ratio. The author explains all the gold ever mined, a thousand years worth, is still with us. So, gold’s price elasticity of supply is the lowest of any metal. However, with Satoshi Nakamoto’s protocol capping the number of Bitcoin at 21 million, it’s elasticity of supply is even lower.

Anyone who has held a one ounce gold coin knows that transporting any amount of the metal is cumbersome. Thus, paper receipts for the metal generally changed hands and the gold stayed put. Of course, the paper began to trade backed by less and less gold, and here we are. Since Nixon snipped the last thread tying the dollar to gold, the number of dollars has grown exponentially. The gold standard is great, except in the hands of untrustworthy governments, ie. any and all governments.

Satoshi, whoever he, she, or they may be, published the Bitcoin paper in 2009, a response to the 2008 financial crash. However, Professor Ammous, references a book by James Davidson and William Rees-Mogg entitled *The Sovereign Individual*. A book well known in libertarian circles. What Ammous points out is Davidson and Rees-Mogg foresaw Bitcoin technology 12 years prior to Satoshi’s work. They, Ammous writes, “predict with remarkable prescience the form that the new digital monetary escape hatch will take: cryptographically secured forms of money independent of all physical restrictions that cannot be stopped or confiscated by government authorities.”

Bitcoin is a shot across the bow at government’s monopoly control of money. While no one in the US appreciates the direction money is going, having the

world's reserve currency and all, Vladimir Putin and Elvira Nabiullina can see what Professor Ammous understands,

If the modern world is ancient Rome, suffering the economic consequences of monetary collapse, with the dollar our aureus, then Satoshi Nakamoto is our Constantine, Bitcoin is his solidus, and the Internet is our Constantinople.

"The current fiat money system that originates from 1973 may be replaced by digitalised commodity-based currencies in the future," Marc Friedrich, a German economist and bestselling author, told Sputnik. The Bank of International Settlements will introduce a rule on January 1, 2022 allowing central banks to hold up to 20 per cent of their deposits in gold, silver, and even platinum in order to stabilize their balance sheets, according to Friedrich. Bloomberg reports central bank gold buying in the first quarter was the highest in six years led by China and Russia. Rupert Rowling writes,

Global gold reserves rose 145.5 tons in the first quarter, a 68 percent increase from a year earlier, the World Gold Council said Thursday in a report. Russia remains the largest buyer as the nation reduces its U.S. Treasury holdings as part of a de-dollarization drive.

Rowling continues,

The buyers are dominated by countries looking to reduce their dollar dependency, and are typically nations with a lower share of reserves in gold than Western European countries.

The battle is joined: Central Banks and the fiat reserve dollar hegemony won't give up easy, even resorting to a return to precious metals to stave off the threat of individual monetary sovereignty, Bitcoin, and the digital revolution.

Tweetstorm: On Bitcoin Culture

By Neil Woodfine

Posted May 24, 2019

1. Bitcoin deals with money. Separating money from the state. Managing

people's life savings. People's livelihoods depend on it. The path of civilisation is altered by the money its built on. Dangerous, risky stuff. A lot is on the line.
2. In addition to this, the vast majority of the industry surrounding bitcoin is comprised of scammers and their "agnostic" enablers. Fraudsters and charlatans that knowingly exploit the lack of understanding in this new technology to profit handsomely at others' expense.
3. Bitcoin industry culture is therefore *necessarily* one of extreme skepticism, cynicism, rigorous review, and forthright language. Regardless of whether you're discussing bitcoin development, business, or economics, no one is safe.
4. Bitcoin is better for it. Dangerous products are rooted out quickly, catastrophic losses are avoided, people know what's private and what's not, damage caused by scammers is strictly limited, dead ends are avoided early, progress is sustainable. The system keeps running.
5. If you're unhappy with bitcoin culture, sorry, you're the problem. Bitcoin is better off without you—you're not cut out for the challenges ahead. You're not good under pressure, you're too sensitive, and you lack conviction.

6. It is *you* that have to adapt to bitcoin culture. Bitcoin should not be expected to adapt to you. If it did, bitcoin would become weak. Like you. You don't build a historic monetary paradigm shift wearing kid gloves.
7. If you do manage to adapt, you'll discover that the bitcoin industry is a very friendly, kind, supportive, and stimulating place. Everyone has time for each other. People are earnest—you encounter far less of the fakery and empty platitudes found in crypto circles.
8. Try going to a bitcoin-only event. Attendees are typically straightforward, collaborative, and technology-focused. If you somehow find yourself feeling broadly unwelcome, your ideas probably suck. You should revise them and be humble.
9. Of course, you're never going to please everyone all the time. Despite what you may have heard, bitcoiners don't agree on everything. You won't find two bitcoiners that don't passionately disagree on something. But so what. Grow up.
10. And if you still can't accept this reality, you're in luck, because bitcoin is completely permissionless. All you need to get started is available online, where you don't need to interact with any oppressive bitcoiners (who probably wrote the material you're reading).
11. You are free to create as many industry groups as you like, open or closed. Can't bitcoiners just be friendly? Why yes, we can! Within your popular, carefully-managed, strictly-moderated safe space, bitcoiners will be very careful with their thoughts and words I'm sure!
12. Instead of focusing on who said what and how it made you feel when they said it, try doing something. Build something useful. Do you want to change the way money works forever, or not?

Golds Best Use Case Is Bitcoin

Anthony Elia

Posted May 24, 2019

This is in response to the article entitled "Drop Gold and The Myths We're told".

Before I begin I would like to clarify this is not investment advice and that I have no affiliation with Grayscale or Mr. Barry Silbert, or anyone working there for that matter. I do own bitcoin, and I also own gold and silver which I purchased subsequently to owning bitcoin. Co-founder of Tokenbot. I am a crypto native.

Similarly to the author of the article posted above, I also "abhor the phenomenon of bad information spreading its way into public markets, and feel a responsibility to rectify the public record when I identify a didactic void." Please allow me rectify and reorg the public record of the didactic voids you have created.

Unlike the author of the article posted above, I do not have extensive professional investing experience in global financial markets. I have not managed an investment fund, although I have access to many top ears on Wall Street. I have founded a total number of zero publicly traded companies, which still result in zero dollars in wealth for institutional and retail investors around the world. I do not claim to and have not been actively involved with Bitcoin and cryptocurrencies from their inception in 2009. In fact it was not until late 2016 until I started reading about bitcoin, and was ultimately early 2017 before I reached my rabbit hole. I own zero cryptocurrency patents. I did not steal the name of an early attempt at a decentralized digital currency and make it the name of my website, even though I had also read it being mentioned in Satoshi's original Bitcoin Whitepaper. I eventually realized, after reading the gold article further, that there is no way Nick Szabo wrote this article, and that I had just missed the fact that the name of the cryptocurrency he created now had a .com after it. Clever. I hope he is getting royalties.

Also unlike our "purely intellectually desired" author, I did not purchase millions of dollars of Antminer S9s at an average price of $2400 which can

now be purchased for $379 or less. Which, might I add is a bigger loss than Bitcoin had itself. I also did not create a company logo that resembled a prominent, REAL, blockchain company:

Also not to be confused with the former firm of Michael Novogratz: Fortress Investment Group

I also did not pivot my company in Ocotober 2017 to capitalize on the Bitcoin or Blockchain name, like so many did, including Natural Resource Holdings Ltd (another Gold company?) which had a couple name changes and merged with a Canadian Mining firm, Backbone Hosting Solutions. Of course the hype drove the stock price up thousands of percent within 60 days! Name changes include Blockchain Mining Ltd and subsequently, Bitfarms. I guess the name Bitmain would have been a little too suspect at this point huh?. At least it was actually mining, and not a Long Island Iced Tea company.

One would think, that claiming to be involved with bitcoin since its inception, you would understand the full grasp of what is actually happening here and the vast potential that was created when Satoshi solved the Double spend problem as well as a probabilistic solution to the Byzantine General's Problem. But no. Instead, you call a bubble in the spring of 2017 and decide to dump millions of dollars of bitcoins. Talk about bad timing! I was probably buying some, so thanks. To make matters worse, while I, the guy with no financial investment expertise in global markets is calling a bull run almost to the day...

https://twitter.com/huobi/status/1085265576577118209

https://twitter.com/huobi/status/1095333829504454657

> I have sold my bitcoin today from the prior trade. No crypto exposure currently other than my stake in Bitfarms.
> — Roy Sebag (@roysebag) March 6, 2019

You are selling yet again less than 3 weeks after the return to the upside....

I dont know if you are a day trader, but I hope you were not hodling all crypto winter just to sell in the $3800 range. We are now over 100% from when you sold. I know a few good cartoon characters on Twitter that I can introduce you to if you like. And I'm beginning to see another reason why this is called the greatest wealth transfer in human history.

Lastly, I am not associated, nor have ever been, with any gold company or brokerage firm specializing in precious metals. And I certainly do not have a new Gold Jewelry startup either! Which by the way, I immediately sent a message to Grit Capital to notify them when @jack had just tweeted about one of their clients, which happens to sell gold, so you're welcome. Thats what a real "global cooperative civilization" looks like. Not the misinformation didactic voids you are creating. None of your actions have been for the collective good. This just leads me to believe that when you say things such as the paragraph below, you are hoping we, as a society, rely on YOUR flawed beliefs, for your benefit only. Your article was solely to come to the defense of gold, which is in your best interest, and that is fine. Someone other than Peter Schiff or the Gold Council should step up once in a while.

"When society relies on flawed beliefs and dogmas that can be easily proven to be unfounded, untested, and unexamined, the collective intellect becomes restrained, leading towards significant misallocations of societal resources. Such misallocations have long-lasting effects, which transcend cultures and borders, weakening the social contract we are all party to as members of a global cooperative civilization."

The DropGold Campaign

Regardless of what anyone thinks about the campaign, its clear and to be expected, that as the investment manager of the GBTC exchange traded fund, Mr. Silbert would do everything legally possible to provide the best return to shareholders. That goes for any investment manager. The significant premium placed on GBTC is also not without some merit. I would not recommend my Mom to store bitcoin herself unless I thought she was ready for the massive responsibility it takes to hold and control your own wealth with no recourse if you simply "lose the password". GBTC allows investors to use investment accounts they are already familiar with and gives them exposure to Bitcoin without the underlying risk of accidentally losing their bitcoin or having it stolen. The current storage costs incurred I would imagine are much higher than that of gold considering the risk. Its much easier to steal bitcoin, as we have seen over and over, than it is to steal physical gold. The 2% annual fee reflects this compared to a normal fund

around .4% give or take. GBTC is certainly worth a premium, the question is how much exactly? I believe the premium will be a reflection of retail education and should trend downward as the years go on. Once you are comfortable storing your own wealth, then there is less incentive to pay a premium.

The amount of the premium also allows investors somewhat of an arbitrage as the previous author mentioned. For instance on May 13th, the dollar amount of bitcoin held per share was $7.38 with a market price of $10.21 creating a premium of about 38.3%. By May 16th the dollar amount of bitcoin held per share was about $7.91. With a higher amount of bitcoin held per share price you would think that the market price would also rise, after all, you would own more bitcoin now right? There are a few variables to consider. The price of Bitcoin, the amount of shares outstanding, and the number of bitcoin held by Grayscale. In this instance, the market price actually fell to $9.94 that day which means that GBTC might have liquidated some bitcoins, but more than likely it was a combination of retail sell pressure combined with the rising price of bitcoin over those days. But rarely do you see the per share of bitcoins rise, while the market price drops, during a price run of bitcoin. This move dropped the premium from 38% down to 25%! A great buying opportunity right? Again, not so fast. The next 2 reported days (20th and 23rd) showed declining price per bitcoin share with a more or less constant market price, thus increasing the premium back up 32%. With Bitcoin price being somewhat stable during this period and a steady decline of price per share of bitcoin, coupled with steady increase in the premium, you could speculate that Grayscale was either buying bitcoin or selling shares during this time.

To refer back to how GBTC was marketing the DropGold campaign, I thought it was beautifully crafted, in my humble opinion and I believe it will age quite well! I do find it ironic however that someone who would go to the lengths of pivoting their entire business to capitalize on being seen as a blockchain or bitcoin company has the audacity to be critical of a longtime unwavering pillar in the crypto community.

” Frankly, I’m surprised that Grayscale Securities’ counsel approved the type of marketing language that has been employed while relying on such weak primary research. In my humble opinion, and based upon my first-hand experience, risk factors are not enough when making statements of facts that compel an investment in securities.”

I'm curious what statements you or your company made exactly when you decided to pivot and the stock price subsequently went up thousands of percent within 60 days?!!

It is at this point of the article where I start to get confused as to whether or not you are defending gold or in fact defending bitcoin. Arguing the theatrical weight and value density portrayed as insufficient is a giant reach for a defense of gold (I personally was not counting the bars to see if it was physically possible, just as I was not up in arms about how gold is not transported by dollys, or how Ferraris dont drive like that in the city, or how helicopters dont really fly between buildings either). If anything you are strengthening the case that gold is even heavier as shown, meaning bitcoin weighs even less than portrayed. I'll look forward to seeing this rectified in future commercials as well. Thank you for pointing that out.

A few major points to discuss...You mention predictability as a way to measure and plan for the future. Well there is an inflation schedule set for bitcoin for well over the next 100 years. What is the inflation schedule for Gold next year alone? No one can know exactly. And if someone decides to print more money to devote more resources to mining gold then more gold will be produced. There is no amount of money that can increase the production of more bitcoin every 10 minutes than is already scheduled. The same amount will be produced, it will just be more difficult. The key here is that no one controls the supply. You cannot get any more predictable than that! This also instills a sense of future which you mentioned. Can also be conveyed as having a Low time preference. I'll admit I did not know what that term meant before bitcoin.

One increasing argument is the amount of energy that is consumed and will have to be consumed for bitcoin to continue on. Bitcoin will be the sole reason that leads us to develop more efficient energy sources than we have today. It will be paramount! Besides, with increased energy consumption, comes increased civilization and more developed societies. If we are going to bank the unbanked, then this is inevitable. This will also increase the continued cooperation through time amongst society, further incentivizing nodes to continue to operate the ledger.

The lack of imagination and creativity to abstractly think how things might be done in the future is astounding to me. Your ignorance is apparent with the assumption that nature already perfected a system. Bitcoin is not trying to simply mimic what nature has "already perfected". It is pushing the envelope and asking what else is possible. We do not know the supply of gold, well then the metabolic energy that was spent to mine that gold is

inefficient. The continued investment of energy is exactly what gives bitcoin value. Bitcoin taxes metabolic energy rather than preserving it so we as a cooperating society can know the supply, who owns what, transact across continents and even planets, and have a predictable supply schedule that cannot be manipulated, but only made more efficient. Just ask Satoshi what does a better job of maintaining the energy embodiment through time.

The reason no one came to golds defense is because there is no existential need for anyone to put forth any more energy, which is a flaw, not a feature. You keep eluding to cooperation, well what kind of cooperation is that?! To concede that something is already perfected is the first of many backwards steps.

The effort of making the attempt is progress. Which also includes every altcoin out there trying to do things that have never been done. We are not in 1994 of bitcoin. We are in 2019 of the internet. Digitally native assets will always be more secure than physical assets. It took thousands of years for gold to reach the end of its monetary use, but it is still necessary to propel us into the future as you so reminded us. Bitcoin mining equipment needs gold. There is a clear step of continued cooperation here. I predict the price of gold will eventually be dictated on the price of bitcoin and how much bitcoin an ounce of gold can help produce.

Bitcoin does not need another intrinsic form of value like jewelry. Bitcoin's intrinsic value is knowledge. It's best at being transparent, a medium of exchange, a store of value. Gold will be best used for one thing, the production of Bitcoin.

Bitcoin will best at being one thing.....Sound Money!

DropGold BuyBitcoin

Satoshi's vision for bitcoin as told by its predecessors

By Tony Sheng

Posted May 28, 2019

While bitcoin often gets credit for being "first"[1] , there were a number of predecessors[2] that contributed to Satoshi's thinking. Most notably:

- David Chaum's E-cash in 1982
- Haber & Stornetta's Linked Time-stamping in 1991
- Wei Dai's b-money in 1998
- Adam Back's Hashcash in 2002
- Szabo's Bit Gold in 2005

Technological breakthroughs occur in context, and the context for bitcoin was in part shaped by these foundational works. This 2017 paper by Clark and Narayanan titled "Bitcoin's Academic Pedigree" offers a wonderful synthesis of all the works that enabled Satoshi's design of bitcoin. They found:

nearly all of the technical components of bitcoin originated in the academic literature of the 1980s and '90s. This is not to diminish Nakamoto's achievement but to point out that he stood on the shoulders of giants The work of Satoshi's predecessors made bitcoin possible on the technical front, but how much did Satoshi's societal intentions for bitcoin mirror those of his predecessors?

In this post, I take a look at the stated intentions of foundational "cryptocurrency" work and compare that with bitcoin's original intentions. And then I reflect on where we are today.

The stated objective of bitcoin

The first few lines of the original bitcoin whitepaper introduce the intentions of the technology: removal of trusted third parties.

A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. Satoshi does not bury the lede. Bitcoin allows

"online payments to be sent directly from one party to another without going through a financial institution." One no longer requires the help of a trusted third party to send and receive money.

Such a system would make non-reversible transactions possible and reduce fraud. Because users don't have to trust third parties and merchants don't have to trust users, a payment system based on bitcoin would minimize the quantity of personal information that gets captured to combat fraud. And less fraud would reduce costs.

In sum (taking the whitepaper at face value), Satoshi thought bitcoin would:

- Enable a new type of service: "non-reversible transactions"
- Reduce fees
- And increase privacy[3]

Bitcoin predecessors

How similar or dissimilar were the stated objectives of bitcoin's predecessors?

E-cash (1982)

Compared with bitcoin, Chaum's E-cash focused less on removing third parties entirely and more on privacy. It tries to tackle the fundamental challenge with crypto-anarchy: a system where individuals are unlinkable to actions makes it impossible to marginalize any group (good) but also makes it impossible to punish evil actors (bad).

He writes:

The ultimate structure of the new electronic payments system may have a substantial impact on personal privacy as well as on the nature and extent of criminal use of payments. Ideally a new payments system should address both of these seemingly conflicted sets of concerns. His goals were to create a cryptocurrency with the:

1. "Inability of third parties to determine the payee, time or amount of payments made by an individual"
2. "Ability of individuals to provide proof of payment, or to determine the identity of the payee under exceptional circumstances"
3. "Ability to stop use of payments media reported stolen"

The paper itself focuses mostly on a concept called "blind signatures" which would allow accounting for transactions without revealing the behaviors of individual actors. It doesn't spend much (any?) time on the system's ability to stop use of payments or reveal personal data in exceptional circumstances.

But it's clear that Chaum wanted a digital cash that was as private as possible that still operated well within the bounds of legacy systems. In contrast, satoshi designed bitcoin to operate outside the legacy systems.

Linked time-stamping (1991)

Haber and Stornetta observed that time-stamps were easy to forge and tamper with in the digital world.

What is needed is a method of time-stamping digital documents with the following two properties. First, one must find a way to time-stamp the data itself, without any reliance on the characteristics of the medium on which the data appears, so that it is impossible to change even one bit of the document without the change being apparent. Second, it should be impossible to stamp a document with a time and date different from the actual one They proposed a design called "linked time-stamping." Documents are created and broadcast to a network. Each new document asserts a time of creation and signs the document and the previously broadcast document, creating a linked list of documents, forming a sort of time-chain.

This data structure is the basis of bitcoin's ledger.

Haber and Stornetta were not focused on financial use-cases. They created their design to help with copyright and patent law, law enforcement, and verification of media authenticity. Still, their work was a breakthrough in trustless verification of data, and proved invaluable to the cypherpunks to follow.

Hashcash (1997, updated in 2002)

Note: while the original Hashcash paper was published in 1997, we review an updated version from 2002 that references b-money.

Back's Hashcash was originally proposed to prevent overuse of free internet resources like email, deterring "denial of service" attacks by making it costly. The paper focuses much more on the technical mechanisms than the

potential applications. It doesn't have strong design objectives beyond a "proof of work" mechanism.

In the short "Applications" section of the paper, Back alludes to the possible application of Hashcash for cryptocurrencies:

hashcash as a minting mechanism for Wei Dai's b-money electronic cash proposal, an electronic cash scheme without a banking interface The clear parallel to the bitcoin whitepaper is a desire to disintermediate the "banking interface" or obviate "trusted third parties."

b-money (1998)

Note: discussed b-money in my popular post "Let's ditch decentralization". Also, while there are many common themes between bitcoin and b-money, there is no evidence that Satoshi was aware of b-money when he write bitcoin whitepaper.

Dai's b-money has many similarities to bitcoin: a peer-to-peer digital money that is minted through proof-of-work, held and used by pseudonymous accounts, and publicly verifiable by all.

The notable thematic difference between b-money and bitcoin is Dai's focus on privacy. He opens the paper with his fascination of "crypto-anarchy" (a fascination I share, as readers will know):

I am fascinated by Tim May's crypto-anarchy. Unlike the communities traditionally associated with the word "anarchy", in a crypto-anarchy the government is not temporarily destroyed but permanently forbidden and permanently unnecessary. It's a community where the threat of violence is impotent because violence is impossible, and violence is impossible because its participants cannot be linked to their true names or physical locations. To Dai, b-money was a way for crypto-anarchic societies to coordinate. It afforded a monetary system that did not require exposure of personal information.

(Of course, we know today that just because a system *can* operate with perfect anonymity does not mean that it will. Users will dox themselves by linking their addresses to third-party gateways like exchanges. Or simply reveal their address to the public. There's also the possibility of systematic "unraveling" of privacy and anonymity.)

Bit Gold

The intention behind Szabo's Bit Gold is best articulated in the third paragraph[4] :

it would be very nice if there were a protocol whereby unforgeably costly bits could be created online with minimal dependence on trusted third parties, and then securely stored, transferred, and assayed with similar minimal trust. Bit gold. Unforgeably costly bits, minimal dependence on trusted third parties, securely stored, transferred, and assayed with minimal trust. Sounds like bitcoin!

The thematic difference between the Bit Gold and bitcoin papers is Szabo's relative focus on the societal implications of a trustless digital money and zero mention of privacy.

In summary, all money mankind has ever used has been insecure in one way or another. This insecurity has been manifested in a wide variety of ways, from counterfeiting to theft, but the most pernicious of which has probably been inflation. Bit gold may provide us with a money of unprecedented security from these dangers. Modern discourse of the benefits of bitcoin tend to build on the Szabo-ian focus on "secure" money or "sound" money. For this reason (and many others), many speculate Szabo is Satoshi or at least strongly influenced Satoshi.

More similar than different

With the exception of E-cash, which prioritizes privacy over trustlessness, all of these papers tend to focus on trustlessness (or as Szabo would put it, trust minimization). Linked time-stamps introduces a data structure well suited for trustless digital money. Hashcash establishes technical foundations for proof-of work. B-money and Bit Gold apply concepts like proof-of-work to describe monetary systems where users can transact with one another without a trusted third party.

We can see strong influences from Timothy May's crypto-anarchy movement; explicitly in Dai's b-money and implicitly in the treatment of default pseudonymity in the others. However, with over a decade in hindsight, we we can see that pseudonymity at the account level is insufficient to protect the identities of most users given the proliferation of third-party gateways (like exchanges).

Interestingly, there's also almost no mention of "programmability" in these early works–a feature that spawned Ethereum and the many other "smart

contract protocols." Perhaps this is a case of "walk before you can run," but many would argue this focus on just pure money features is intentional. Szabo describes it as limiting the surface area of attack .

How do we fulfill Satoshi's vision?

Most debates within bitcoin communities (inclusive of forks like BCash and Bitcoin SV) and between bitcoin communities and other cryptocurrency communities (e.g. bitcoin vs ethereum) are about vision. What properties should a cryptocurrency have to best satisfy Satoshi's true intentions? What would Satoshi want to see (how would they change their vision) if they knew what we knew today?

A coarse literature review reveals a shared focus on a single property: trust minimization. And perhaps an assumption of other properties like overall cost reductions to the system and user anonymity. There is no mention of "programmability" in these works, though we know early bitcoin communities (including Satoshi) discussed versions of programmability often. (I believe Satoshi had some ideas for more features on top of bitcoin like debt, lending, and gambling but Hal Finney convinced him against it. I can't find this source so if you have it, please send it to me and I'll revise.)

One can understand the nature of conflicts within bitcoin and between bitcoin and other cryptocurrencies as negotiating trade-offs between trust-minimization and other properties. Bitcoin Cash trades trust-minimization for bigger blocks, which theoretically leads to cheaper and faster transactions. Ethereum trades for programmability. Zcash and Monero trade for privacy (this one I'm less sure of, feedback welcome).

But while the vision for bitcoin core has changed over the years , it seems to have remained true (at least in a relative sense) to the singular focus of trust minimization. And in doing so, bitcoin has achieved a valuable strength unassailable by competitors[5] .

parties involved and the trusted third party. The necessity to announce all transactions publicly precludes this method, but privacy can still be maintained by breaking the flow of information in another place: by keeping public keys anonymous." Keep your public keys anonymous and don't reuse addresses. I wonder whether he'd feel the same today given sophisticated chain analytics companies.

Thanks to Nic Carter for his valuable feedback on this post.

1. When I asked twitter for the irreplicable properties of Bitcoin, I got a lot of "first." ⮌
2. Hat tip to Multicoin Capital and other contributors to the very useful Crypto Archives. ⮌
3. Something I hadn't noticed before in my dozens of readings of the whitepaper. Satoshi makes these comments on privacy: "The traditional banking model achieves a level of privacy by limiting access to information to the ⮌
4. Though Szabo is a joy to read and his historical set-up is worth reading. Particularly his three self-links on trust in a third party,private bank note issue, and precious metals and collectibles ⮌
5. Which does not mean that others cannot find their distinct markets by offering distinct design spaces. I still think this adoption will follow a curve like I described in this post. The big question for investors is will the singular focus on trust minimization yield the largest and most valuable market. ⮌

How Fiat Could Fall and Bitcoin Could Soar

By Taylor Pearson

Posted May 28, 2019

Argentina's Failed Peg

In the 1990s, the Argentine peso was pegged to the U.S. dollar. This meant that the Argentine government guaranteed that anyone could exchange one Argentine peso for one U.S. dollar. If you had 1,000 Argentine pesos in your bank account, you could walk into the bank and ask for US$1,000 and the teller would hand it over.

By 2001, the peg had become unsustainable and the government of Argentina abandoned it. As a result, the exchange rate went into freefall.

Imagine if you looked at your bank account and the value of your assets had gone down by 75 percent over the course of a year without you spending a dime. That's effectively what happened to the citizens of Argentina in 2001.

In less than a year, the exchange rate went from 1:1 to 4:1. If you had $10,000 worth of pesos in your bank account in 2001, a year later you would have had only $2,500.

Attempts to withdraw U.S. dollars as the exchange rate plummeted were thwarted for most citizens because the run on the bank meant there were no U.S. dollars left to hand out.

I spent a year living with a retired woman in Córdoba in the 2000s who recounted to me the feeling of watching her retirement savings slashed by 75 percent as she slept on the street outside the bank, hoping to be able to withdraw it.

Though few of us who grew up in the developed world can relate, this story is not unique to Argentina in 2001.

The Debut of Paper Money

As Jack Weatherford details in his book, *The History of Money*, the story of fiat began in the 17th century, which marked the debut of paper money on the modern world scene. As long as this paper money was supported by some form of commodity money, like gold or silver, all seemed well. Carrying and

holding paper seemed just as reliable, and far more convenient, than holding the actual precious metals that backed them.

Invariably, however, the government or bank in charge of printing the money issued more paper than it had metal to back it. Whether or not this was the "right" thing to do is a matter of debate, but once the devaluation process began, it inevitably spiraled, with more and more bills being issued at less and less value.

An analysis of fiat currencies in the 20th century found that there were 56 episodes of hyperinflation. Another study found that the average life expectancy for a fiat currency is 27 years: 20 percent failed through hyperinflation (37 currencies experience hyperinflation in the 20th century), 21 percent were destroyed by war, 12 percent were destroyed by independence, 24 percent were monetarily reformed, and only 23 percent are still in circulation.

Of those that remain in circulation, all have lost huge amounts of their original value as measured in commodity money like gold or silver. Founded in 1694, the British pound Sterling is the oldest fiat currency in existence. At the ripe old age of 325 years, it must be considered a highly successful fiat currency. Yet, the British pound was originally defined as 12 ounces of silver, so its worth today is about half of 1 percent of its original value.

The U.S. dollar was taken off of the gold standard in 1971 when it was 1/35th an ounce of gold. By 2011, it had already lost 97 percent of its value.

In his book, *The Ascent of Money*, historian Niall Ferguson relates that one of the main ways this seems to have happened is that rulers were forced to print money to finance wars. Once one ruler started doing this, it became a classic prisoner's dilemma and others had to follow suit. It would be better for everyone if no one fired up the presses, but as soon as one ruler or government warmed them up, then everyone else had to keep up or they risked being conquered.

Part of the reason Germany lost World War I and suffered worse inflation of their currency than the Allies was because the German and Austrian bond market was much less developed than the French, English and American markets, which had access to far more capital. Unable to raise money through bond issuances, Germany was forced to print money faster than other powers to finance their war effort.

It's also worth noting that in a democratic society, politicians are often unwilling to raise taxes or balance the budget because of the expected voter

anger. For them, inflation and the devaluation of the currency are preferable because they constitute a hidden tax.

The consequences of poor decisions about monetary policy can take decades to show up, but politicians' terms only last a few years — kicking the can down the road to finance their constituents and donors favorite projects is a time tested way to get elected.

When you make choices about your personal spending, you inevitably run into difficult decisions — you could take out a bigger mortgage and buy a bigger house but that would mean working an extra five years before you could retire, is that worth it? The ability to print money meant that politicians could, in effect, buy the bigger house for themselves or their constituents today and make someone else work an extra five years in the future to pay for it.

Bitcoin's Case Against Fiat

Ultimately, all the reasons for devaluation boil down to mismatched incentives between the politicians or others in control of the monetary policy and the individuals holding the currency. Any time a system lets somebody change history with a keystroke, you have no choice but to trust that everyone who can make that keystroke will be both perfectly honest and perfectly competent. Alas, humanity, much less politicians, don't have the best track record on either of those fronts.

When the Bitcoin network went live in January 2009, Satoshi embedded the headline of a story running that day in *The London Times*:

"The Times 03/Jan/2009 Chancellor on brink of second bailout for banks" Though we can't know for sure what was going through Satoshi's mind(s) at the time, the most likely explanation is that Satoshi was commenting on the decisions being made in response to the 2008 global financial crisis by the small group in charge of global monetary policy. Though many people around the world were affected by these decisions, very few had any say in the matter.

Instead of impactful decisions about the monetary system, like a bailout or quantitative easing, depending on the perfect honesty and competency of a single individual or small group, Satoshi envisioned Bitcoin as a more robust monetary system, with a more distributed power structure that would make it impossible for a single individual or small group of individuals to act unilaterally.

Instead of impactful decisions about the monetary system like a bailout being reliant upon a single individual or small cabal, like the Chancellor of the Exchequer and Chairman of the Federal Reserve, Satoshi and the Bitcoin proponents that followed him, envision bitcoin as having a more distributed power structure, beyond the control of a single individual.

Viewed as money, bitcoin has many gold-like properties. We know exactly how many bitcoins will be created — 21 million — and the rate at which they will be created. Just as gold mining is limited by gold's geological properties, the ability to change these variables in bitcoin is outside of the control of any one person or small group of individuals. This gives bitcoin a predictable stock-to-flow ratio. No single individual can decide to create twice as much bitcoin tomorrow, even if it is politically expedient.

However, bitcoin also as a few properties gold lacks. For one, it is easily divisible and transportable. Someone in Singapore can send 1/100th of a bitcoin to someone in Canada in less than an hour.

It is also extremely difficult to censor bitcoin transactions. If I have an internet connection and agree to pay the network's fee, effectively nothing can stop me from sending bitcoin to anyone I want.

This doesn't mean, of course, that bitcoin is not primarily a highly volatile tool of speculation today — it is — but it points to why many of those speculators are in the market. If central banks in any country fail to unwind their balance sheets gracefully and inflation sets in, savers will go looking for a safe place to store their wealth.

In this scenario, bitcoin, an easily divisible and transferable "digital gold," may shine.

Understanding (and Mitigating) Re-Orgs

By Anthony Lusardi

Posted May 21, 2019

Applying Proof of Work (PoW) to digital currency is an amazing innovation that was first actualized by Satoshi Nakamoto and builds on ideas from Wei Dai, Nick Szabo, Adam Back, and many others.

Unfortunately the importance of this innovation is exceeded only by woeful misunderstanding of how PoW works. This article seeks to clarify how they happen, when they negatively affect payment recipients **(they rarely do)**, deterring double spends, and whether re-orgs are a Good Thing™.

This is the first of many articles on this topic, with future ones taking a deeper look at some of the ideas proposed below. If you have any thoughts, comments, or feedback please feel free to reach out.

What Is A Re-Org?

A re-org is simply what happens when your node is aware of Chain A, but then sees a bigger Chain B and switches to it. This happens on occasion and most of the time it is a non-issue. However, Chain B might have parts of its transaction history that don't match Chain A and this can, **under certain conditions**, cause issues for those receiving transactions on a blockchain.

What Happens to Transactions in Chain A?

Most transactions from Chain A will be placed by miners onto Chain B, they'll get the fees from the transactions, and most users won't even notice that their transaction "moved" from the shorter Chain A to the longer Chain B.

Most importantly is that Chain A and B will share the overwhelming majority of the same history, so if you have Chain A and Chain B split at 10 AM today and you received coins last night then your coins are entirely unaffected.

Typically only a small bit of the tip of the chain can be re-org'd off, with it becoming cost prohibitive to remove parts of the chain that are even a couple days old.

When Is A Re-Org Bad?

This depends on who you are, re-orgs will affect HODL'rs, Exchanges/Payment Processors, and Miners in different ways.

Firstly, re-orgs without double spends are occasional and uneventful things. Here's a partially complete list of them on Bitcoin.

Re-orgs are only bad when someone creates a double spend to defraud someone they've sent a payment to. Creating a double spend is akin to writing a bad check for a large amount of money, receiving the goods, and letting the check bounce.

When a double spend is created through a re-org it largely affects recipients of a transaction. There may be some collateral issues with old transactions being pushed out of the chain but these are often remined, and unless your exchange is actively trying to steal from you they'll rebroadcast your missing transaction.

How Does a Double Spend (or Re-org) Affect You?

HODL'rs: A double spend is almost never bad for you, the longer your coins are in your wallet the more work that is piled on top of it and the less likely it is you'd ever be double spent. On Bitcoin ~1,900 BTC ($11 million) of new work is added to the chain **every single day**. After 3 months it's going to cost **over a billion dollars** for someone to double spend you. Much better than the FDIC insurance on your bank account in my non-fiduciary opinion.

Exchanges/Payment Processors: Double spends are the worst for you and you're the primary target of them, but I probably don't need to tell you this. What you should be aware of is that there are many ways to mitigate double spends without immediately resorting to nuclear options (though they are still options).

Miners: Are largely unaffected by double spends themselves but can be negatively impacted by the re-org used to achieve the double spend. In this case they lose block rewards (block subsidy + transaction fees).

How May an Exchange Deter Double Spends?

1. **Wait Longer**: Exchanges can simply wait longer before confirming transactions, by waiting more blocks they increase the initial cost of a double spend attack, the higher the initial cost the more money an attacker needs to spend in order to achieve a successful attack. Risking

> 2 BTC ($11,600) to get away with 200 BTC ($1,160,000) is a low-risk theft. Risking 1,000 BTC ($5,800,000) to get away with 200 BTC is much higher risk.

Cost of re-orgs varies substantially between chains. To get an idea of confirmation equivalents between chains check out howmanyconfs.com which normalizes all chains to ~6 Bitcoin blocks and read their GitHub README which has a substantial amount of information and thoughts on this topic.

Important to note is that you **do not need to harm UX/usability of your exchange; you can improve it while simultaneously becoming more secure.** You can take the approach that many exchanges do when handling cash deposits. Credit them almost immediately, allow trading, and wait an appropriate amount of time/confirmations before allowing withdrawals.

Account for Transaction Value: A 2 BTC transaction is not equivalent to a 1,000 BTC transaction. The amount of confirmations you decide to wait should be proportional to the underlying value of the transaction. A simple, but by no means complete, metric is to wait until total block rewards exceed transaction value for the payments you've received in a given block. For example, if you receive 100 total BTC in block 575,000 on Bitcoin then you will want to wait at least 8 blocks (100/13.25) before confirming that 100 BTC. 13.25 is currently the average total block reward for successfully mining a block on Bitcoin and only used for example purposes. This particular method of deterrence warrants more investigation and may benefit from an additional "safety multiplier". Game theorists please DM me on Twitter.

Be Mindful of Hardware Sets; especially GPUs: Presently there are two hardware sets that mine Cryptocurrencies, ASICs dedicated to a specific hashing algorithm, and GPUs. This means that the Dagger-Hashimoto PoW algorithm on the Ethereum network is presently the majority for the GPU hardware type. All other GPU-mined chains, regardless of their PoW algorithm, are minority chains as switching costs between algorithms are trivial.

Currently market inefficiencies create the perception that GPU-mined algorithms are distinct from each other. However this is only due to open market places (ie. Nice Hash, Genesis Mining) selling hashrate at the algorithm and chain level rather than the general GPU level. You can observe the ease of switching between GPU-mined algorithms by taking a look at auto-switching mining pools (ex. MiningPoolHub) which allow miners to automatically switch their hashrate between networks and GPU-mined

algorithms. It is inadvisable to rely exclusively on market inefficiencies to prevent exploitation of minority GPU-mined blockchains.

Are Re-orgs a Good Thing™?

Re-orgs are simply a vital component of PoW/Nakamoto Consensus, they are not in and of themselves good or bad. Re-orgs are necessary and irremovable from Nakamoto consensus because they remove trusted middlemen so that someone receiving a blockchain only needs to verify that it's the longest one they're aware of.

In exchange for re-orgs we get PoW blockchains that are expensive to disrupt, and make long term censorship and DoS attacks impossible because they require sustained spending and consumption of finite resources.

In Summary

PoW is an incredible experiment in game theory and financial motivations the likes of which we have not seen before. If you're interested in this industry then you should take at least some effort to understand the innovation that is PoW, learn its limitations, its unexplored dimensions, and enjoy watching this all play out. Ultimately PoW is the only consensus algorithm that we have which allows for a maximally decentralized, permissionless, and censorship-resistant network which naturally resists concentration of power. PoW doesn't solve technological issues, it solves human issues.

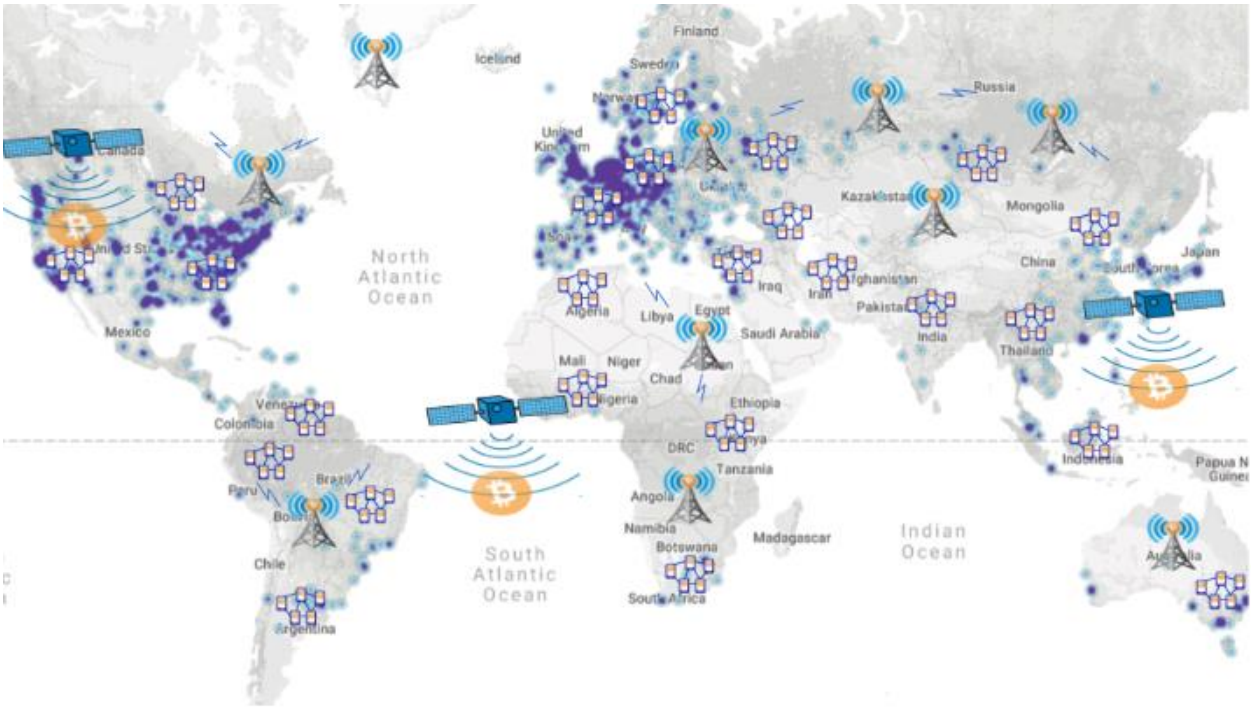
You can read more on these topics, and similar ones at: nakamotoinstitute.org, the cryptography mailing list archives, and the libbitcoin wiki.

Decentralizing Bitcoin's Last Mile With Mobile Mesh Networks

How you can use Bitcoin without relying on centralized Internet Service Providers

By Richard Myers

Posted May 29, 2019



The "Expert Views" series of publications allows legal and technical practitioners in the cryptocurrency space to share their insight and opinions on cutting edge policy questions. The views expressed here are those of the author and not necessarily those of Coin Center. Bitcoin has been designed to be resilient against not just technological attacks, but also political ones. Cryptography, incentives and decentralization are all tools used to give the Bitcoin network a high level of resiliency. Here I will discuss how communication decentralization is important for Bitcoin's resiliency and how this feature can be enhanced with alternative last-mile communication technologies such as mobile mesh networks.

Centralized communication systems are prone to failure in the case of natural (or man made) disasters. For example, Hurricane Sandy downed one-third of all communication infrastructure in a 10-state area back in 2012. After a natural disaster, centralized systems are slow to recover.

Puerto Rico struggled for many months after Hurricane María when 80% of landlines became inoperative. Marginalized communities and places with failing or nonexistent infrastructure are also not well served by centralized providers.

Modern economies increasingly rely on electronic payments and suffer when communication systems are unavailable. This is true not just for Bitcoin, but also for Visa and Mastercard. Where Bitcoin is unique is in its goal of also being resilient against deliberate state-level financial censorship and surveillance.

Network decentralization gives Bitcoin protection against censorship on a global scale, but local Internet Service Providers (ISPs) are in a position where they can unilaterally monitor and block users of the Bitcoin protocol. Examples of politically motivated internet censorship and surveillance from China to Turkey are easy to find. It is not hard to imagine regimes applying these techniques to people using Bitcoin. Even in the United States, Edward Snowden revealed that the NSA had a program in 2013 to intensely track Bitcoin users.

Within any particular location, users must access the Bitcoin network using ISPs and mobile carriers which are dominated by regional and national monopolies. ISPs like Comcast have been shown to throttle and block the popular decentralized file sharing protocol BitTorrent. When the IRS requested Coinbase's user records in 2016, they also requested detailed IP logs of their users that could be matched up with ISP IP logs. Anti-piracy groups like Prenda Law have previously used IP address information obtained from ISPs to target BitTorrent users for legal harassment. Someday, Bitcoin users could be targeted in a similar way. It's much easier for a government or powerful corporation to pressure a single monopoly with huge infrastructure investments to surveil and censor people in an automated fashion than it is to try to target citizens individually. Software privacy tools alone are not enough. Before Snowden revealed himself, he built a personal map of open WiFi hotspots that were not near his home in Hawaii. He understood that even using Tor did not eliminate the risk that came from using an internet access point somehow connected to his true identity.

Centralized ISPs are the single point of failure for all of these attacks; either from direct censorship or meta-data logging. Even sending a chat message to someone a few feet away involves data traveling to a distant base station and through centralized servers. Mobile phones are technically capable of forming decentralized mobile mesh networks, but current spectrum license holders have no economic incentive to allow it. Instead, peer-to-peer connectivity is limited to a few dozen feet of Bluetooth range which has limited practical utility in the real world.

Fortunately, alternatives to centralized ISP networks are starting to appear. Local mesh radio networks, satellites, and long-range radio have all been proposed as ways to enable decentralized peer-to-peer communication—both for Bitcoin transactions and for resilient communication generally.

In 2014, the Kryptoradio project pioneered transmitting Bitcoin data using a terrestrial digital television transmitter in Finland. The trial lasted 2 months and reached ~5 million people, or about 95% of all Finns. For the first time, you could validate transactions without an internet connection. But this system still relied on regionally centralized broadcast infrastructure.

In 2017, Blockstream started satellite-based Bitcoin transaction broadcasts that now cover virtually the entire world's population. This enables decentralized transaction verification in countries that might ban Bitcoin and also enables Bitcoin use in locations without reliable or affordable internet. But this system only receives transaction information from the Bitcoin network. How can an offline user add a new transaction to the ledger?

At Scaling Bitcoin 2017, Nick Szabo and Elaine Ou from Global Financial Access proposed transmitting transactions using low-cost digital shortwave radio. Their system uses long-range skywave transmissions to route around censorship and across borders. Their proposed system is semi-mobile for use in censored countries and supports two-way communication over hundreds of miles. This is a promising technology but requires further development before it can be widely deployed.

The goTenna Mesh radio powers the world's first consumer mobile mesh network. It's focused on relaying short-burst data over great distances, in a totally decentralized, off-grid manner: no cell, WiFi, or satellites required.

In a mobile peer-to-peer mesh network, devices communicate directly with each other if they are within range, or relay from device to device to device if the destination is further away.

All of this happens automatically with no centralized routing or infrastructure needed. Bitcoin nodes communicate using a similar flat peer-to-peer network without any special nodes that coordinate their connections. Unfortunately, the Bitcoin peer-to-peer network is only a virtual overlay on a physical internet that is dependent on centralized ISPs and mobile carriers. Unlike nodes in a mobile mesh network, nodes connected to centralized networks have a fixed location or identity that can be targeted for censorship and surveillance.

Privacy activists from the Samourai Wallet team were inspired by Blockstream's satellite project to create an open-source initiative called Mule Tools to support similar alternative communication projects. In 2018, goTenna collaborated with Samourai Wallet to create the open-source TxTenna App for Android phones. With TxTenna, you can send signed Bitcoin transactions over the goTenna Mesh network directly from an offline mobile phone. This enables people to broadcast Bitcoin transactions in a decentralized way, without depending on local ISPs. The goTenna Mesh network enhances financial privacy by removing any physical link between a person and their bitcoin. TxTenna can also route around local censorship by using gateways to reach distant, uncensored internet connections.

How does it work?

From an offline phone, Samourai Wallet creates a signed Bitcoin transaction. The signed transaction is sent automatically to the TxTenna App. TxTenna broadcasts the transaction to nearby goTenna Mesh nodes. They relay the transaction data from node to node until it reaches a mesh node running TxTenna with uncensored internet access, which can send the transaction to the Bitcoin network.

A Python-based version of TxTenna has also been made for computers and Internet-of-Things devices, enabling them to broadcast signed Bitcoin transactions or act as an internet gateway between the goTenna Mesh network and the Bitcoin network. The goTenna Mesh radio can also be combined with a Blockstream Satellite receiver to create an off-grid system that combines the best off-grid features of both. Such a system can both receive Bitcoin blockchain updates from the Blockstream Satellite receiver and broadcast signed Bitcoin transactions over the goTenna Mesh network without any direct internet connectivity.

Conclusion

In time, we expect low-cost gateway devices will support multiple alternative communication modalities. These will include mobile mesh, satellite, long-range High Frequency Radio, WiFi, and mobile phone networks. In the case of an ISP failure, natural disaster or political oppression, Bitcoin transactions will simply fail over to an alternative network. In this way, transactions on the Bitcoin network can be made even more unstoppable. *Richard Myers is a decentralized applications engineer at goTenna, co-founder of Bytabit AB, and has been interested in both the technology and political implications of bitcoin for many years. Richard is passionate about tools that empower decentralized societies. Follow him on Twitter at @remyers_*

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