

WORDS

December 2018

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

Contents

Contents.....	1
Goals and Scope.....	2
Support WORDS.....	3
Skeptic's Guide to Bitcoin: Unpacking Bitcoin's Social Contract.....	4
The "Bitcoin mining death spiral" debate explained.....	10
Beware of Lazy Research: Let's Talk Electricity Waste & How Bitcoin Mining Can Power A Renewable Energy Renaissance.....	13
Skeptic's Guide to Bitcoin: Bitcoin and the Promise of Independent Property Rights	27
Introducing Realized Capitalization.....	33
Who Controls Bitcoin Core?.....	39
Bitcoin Data Science (Pt. 3): Dust & Thermodynamics	50
The Lightning Network.....	65
Philosophical Teachings of Bitcoin.....	74
Bitcoin's Incentive Scheme and the Rational Individual.....	82
Bitcoin is a Decentralized Organism (Mycelium)—Part 1/3.....	89
Bitcoin is a Social Creature (Mushroom)—Part 2/3	100
Disclaimer:.....	112

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.

 Send Bitcoin

 tippin.me

 Send CashApp

 Send PayPal

Spread the word

Have a website or use social networking sites like Twitter, Facebook, or LinkedIn? Please consider sharing the content found on *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 noconiners, sarcastic remarks, and other things regarding development of this site.

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

 Twitter

Subscribe to our newsletter

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

[Subscribe](#)

Our pledge

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

Skeptic's Guide to Bitcoin: Unpacking Bitcoin's Social Contract

A framework for skeptics

By Su Zhu and Hasu

Posted December 3, 2018

This is part 2 of a 4 part series. See additional articles below

- Part 1 Skeptic's Guide to Bitcoin: An Honest Account of Fiat Money
- **Part 2 Skeptic's Guide to Bitcoin: Unpacking Bitcoin's Social Contract**
- Part 3 Skeptic's Guide to Bitcoin: Bitcoin and the Promise of Independent Property Rights
- Part 4 Investing in Bitcoin



Left: Illustration: engraving by Abraham Bosse via [Wikimedia](#)

Bitcoin is a novel social and economic institution. It is so different from our existing institutions that we should be skeptical and ask as many hard, pressing questions as we can before trusting it with any economic value. Some answers will only reveal themselves with time (or Lindy, as the cool kids say), but that doesn't mean we

can't come up with theories or frameworks. One such framework that has helped me a lot in understanding bitcoin is social contract theory.

First, fiat money is the result of a social contract: The people give the state control over the supply and other vital functions of money. The state, in turn, uses that

power to manage the economy, redistribute wealth, and fight crime. But many don't realize that bitcoin works through a social contract as well.

The social layer and its rules are the heart of bitcoin.

And that social contract framework can be used to answer some essential questions: Why did bitcoin come into existence? Who decided its properties? Who controls it today? Can a critical bug kill bitcoin?

Social Contract Theory

Social contract theory starts with a thought experiment: It assumes a hypothetical *state of nature* full of violence, that is unbearable for people to live in. Driven by a desire to improve their situation, they come together and collectively agree to empower Leviathan, the sovereign government, to protect them. Each gives up some of their freedom (to, you know, steal, and murder and stuff) while the Leviathan is granted the power to create laws, enforce them, and protect the people from violence.

But the theory is not constrained to the relationship between the people and the state. We can apply the same thought experiment to economics. If enough people are unhappy with the barter economy, they can collectively agree to use money, credit, or something else to improve the quality of their trading.

The process of money or credit happens implicitly. Every person asks the question of what outcomes they prefer and how they can achieve them. If many people in a society want the same outcome, we can call the result a "Schelling point" or social contract.

Money as a Social Contract

Throughout history, governments that controlled money have abused their power in all kinds of ways: They confiscated accounts, blocked certain people or groups from transacting, and printed more money and inflated the supply—sometimes to the point of hyperinflation.

Whenever governments crossed a line in abusing their power, the people lost trust in the social contract that granted the government this power. They returned to an agreement that preserved most of the benefits (having a common medium of exchange, store of value, and unit of account) without the worst of problems (government abuse): a commodity money.

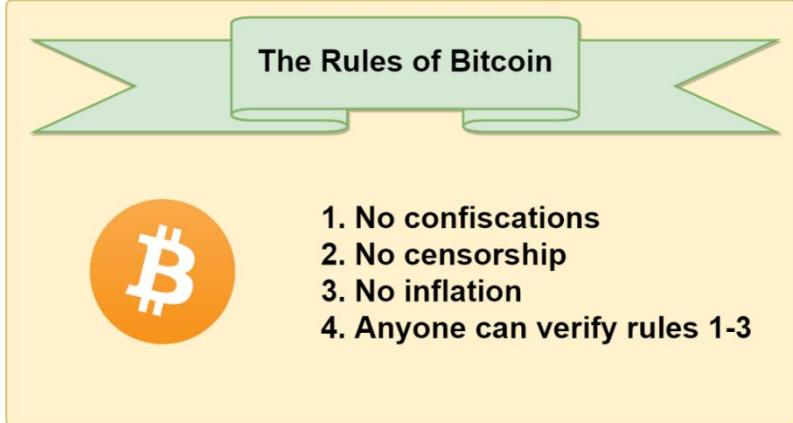
Money presents an important lesson: The larger and more valuable a social institution gets, the more it attracts others to seek control over it.

The problem with the new commodity money contract, however, was that it turned out equally unstable. Let's take, for example, the gold standard. Physical gold was too inconvenient to divide, move, and store. So people quickly invented another layer on top of it and traded with representative paper money, while the physical gold no longer moved. Because paper money is easy to produce, there had to be a trusted central party to watch over the supply. From there it was a small step for governments to decouple the value of the paper money from the underlying commodity to establish fiat money once again.

Herein lies a valuable lesson: 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.

The Rules of Bitcoin

When Satoshi Nakamoto invented bitcoin, he did not invent a new social contract. Satoshi did something else—he leveraged technology to solve many problems of past implementations and implemented the old contract in a new and better way. He settled on the following rules:

- Only the owner of a coin can produce the signature to spend it (confiscation resistance)
 - Anyone can transact and store value in bitcoin without permission (censorship resistance)
 - There will only be 21 million bitcoins, issued on a predictable schedule (inflation resistance)
 - All users should be able to verify the rules of bitcoin (counterfeit resistance)
- 
1. No confiscations
 2. No censorship
 3. No inflation
 4. Anyone can verify rules 1-3

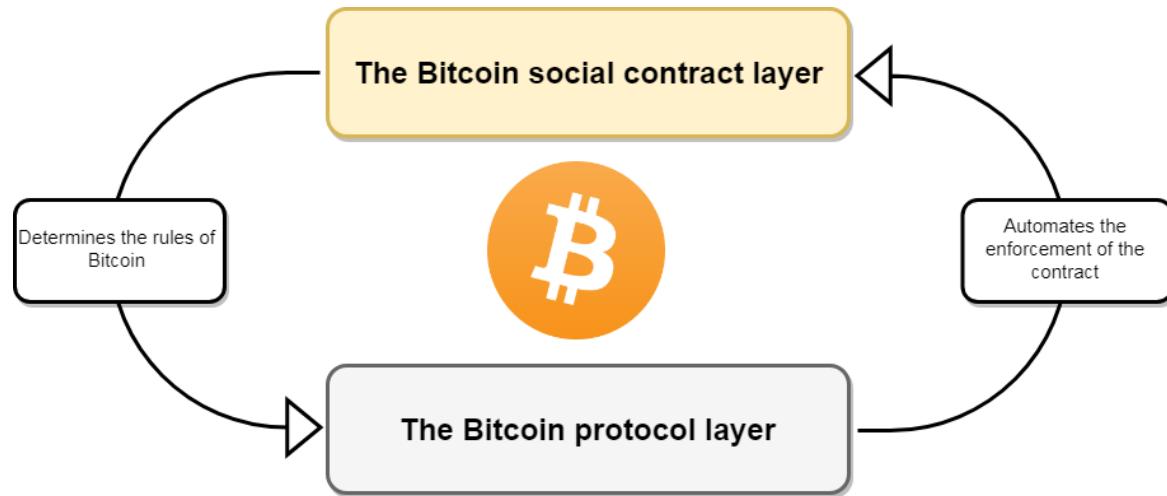
Bitcoin as a New Form of Social Institution

Money presents an important lesson: The larger and more valuable a social institution gets, the more it attracts others to seek control over it. So the institution needs protection, which it can only get from that other powerful entity: the state. Over time, protection turns into control and then into abuse. When the social

institution loses its benefit for the people, it is replaced by a new institution, and the cycle starts over again.

Satoshi attempted to break this vicious cycle in two ways: First, instead of getting its security from a powerful central party (like a government), bitcoin creates a hypercompetitive market for its own protection. It turns security into a commodity and the security providers (miners) into toothless commodity producers. And, second, Satoshi found a way for these competing security providers to come to consensus over who owns what at any given time.

The bitcoin protocol automates the contract agreed upon on the social layer, while the social layer determines the rules of bitcoin, based on the consensus of its users. They are symbiotic: Neither of them would be sufficient without the other. The social layer and its rules are the heart of bitcoin. But the protocol layer makes them enforceable for the first time, while simultaneously making the social contract more credible to outsiders. Seeing bitcoin as a social contract, enabled and automated by a technical layer, has many benefits. And it can help us answer the philosophical questions about bitcoin.



Who Can Change the Rules of Bitcoin?

The rules of the contract are decided and renegotiated continuously on the social layer. The bitcoin protocol implementation only automates them. Bitcoin, as a computer network, comes into existence when many people run bitcoin implementations on their computers that follow the same set of rules (think of them as speaking the same language).

You stay in the network as long as you follow the same set of rules as everyone else. If I were to change the rules of bitcoin unilaterally on my local computer, it would not affect the rest of the network—it only gets me evicted because we no longer understand each other (I now speak a different language).

The only way to change the rules of bitcoin is to propose a change to the social contract. Every such proposal has to be voluntarily accepted by other people in the network because it only becomes a rule if enough people actively include it in their local ruleset. Convincing millions of people is an incredible amount of (grassroots) work and practically rules out any contentious changes, which could never get broad social consensus. This is why the bitcoin network can be upgraded in ways that reflect the wish of its members but is at the same time incredibly resilient to changes from bad actors.

Can a Software Bug Kill Bitcoin?

In September 2018, a software bug arose in the most popular implementation (local ruleset) of bitcoin. The bug had two potential attack vectors: It allowed an attacker to shut down other people's bitcoin clients (making it so they could no longer verify the rules, breaking the counterfeit resistance) and to potentially spend the same bitcoin twice (breaking the rule of inflation resistance).

Bitcoin developers quickly fixed the bug by providing the network an updated ruleset that closed these possible attack angles. While the bug was found in time and was never exploited by an attacker, it left some people asking: How much damage could it have done? Would the bitcoin network have to live with the inflation once it happened, effectively breaking the trust in that rule?

Social contract theory can answer that with a resounding "no." Bitcoin's rules are made on the social layer, and the software only automates it. Where the social contract and the protocol layer diverge, the protocol layer is wrong—always. A failure of the protocol layer to temporarily enforce the rules of the contract has no permanent bearing on the validity of the contract itself.

The bitcoin token itself has no value. The value exists purely on the social layer.

Instead, here is what would have happened: The potential bug exploit would have been mended by reorganizing the blockchain in a way that undoes the damage done by the attacker. That would have split the bitcoin network into two networks, each having their own token: one with the bug and one without it. Every bitcoin owner would have an equal number of tokens in each network, but the value of these tokens would be exclusively determined by the market, i.e., how much the next person was willing to pay for them.

At this point, it's important to understand that the bitcoin token itself has no value; it's nothing more than a number in a ledger. The value exists purely on the social layer. Hence, it is also social consensus that decides which of the two tokens, going forward, would receive economic support. It's likely that all economic value would migrate to the new, mended network.

When the bitcoin software successfully automates the rules of the social contract, the two layers are synchronized. And when the software temporarily goes out of sync, it always has the social contract as a guiding beacon of light to return to. This most recent bug will not have been the last. Social contract theory gives us assurance that bugs can happen and don't threaten the social institution of bitcoin.

Do Bitcoin Forks Endanger the No-Inflation Rule?

Another famous philosophical question centers around the concept of "forks." Since bitcoin's software is open-source (allowing users to verify that their ruleset does what it says), anyone can copy it and make changes. That is called "forking." But, as established earlier, these changes are only made to the protocol layer, not the social layer. Without changing rules on the social layer first, the only result from forking bitcoin is that you evict yourself from the network.

If you wanted to fork bitcoin—and not have the new network die immediately—you would have to fork the social contract first. You would need to convince as many people as possible that your ruleset is better for them, so they update their rules together with yours. These kinds of forks are scarce and hard to pull off because they require the buy-in of thousands of people. Using this process to create value is akin to running a presidential campaign as a financial investment.

Again, the key is in understanding that all value for tokens is purely a social construct. The tokens do not have any value; they receive their value from social consensus. Forking the protocol doesn't equal forking the social contract, so the new token is worthless by default. In the rare case that the social contract itself splits (like when bitcoin cash split off from bitcoin), you end up with two weaker social contracts—each agreed to by fewer people than the old one.

Money in general and Bitcoin in particular can be seen as social contracts between people in society. Bitcoin is not a new contract either; it's just a new implementation of a contract that can be traced back hundreds of years. In comparison to previous attempts, the bitcoin implementation is a dramatic improvement because it creates a hypercompetitive market for its own security. Bitcoin's social layer and the protocol layer are mutually reinforcing, and their relationship gives us insight into little-understood concepts like rule changes, forks, or protocol bugs.

The “Bitcoin mining death spiral” debate explained

By Arjun Balaji

Posted December 4, 2018

Quick Take

- Bitcoin is not going into a miner-induced death spiral
- In an extremely unlikely scenario if hash rate dropped a lot, miners can be kept running by increasing fees
- If that wasn't enough, as a last resort, there could be an emergency fork to manually lower difficulty

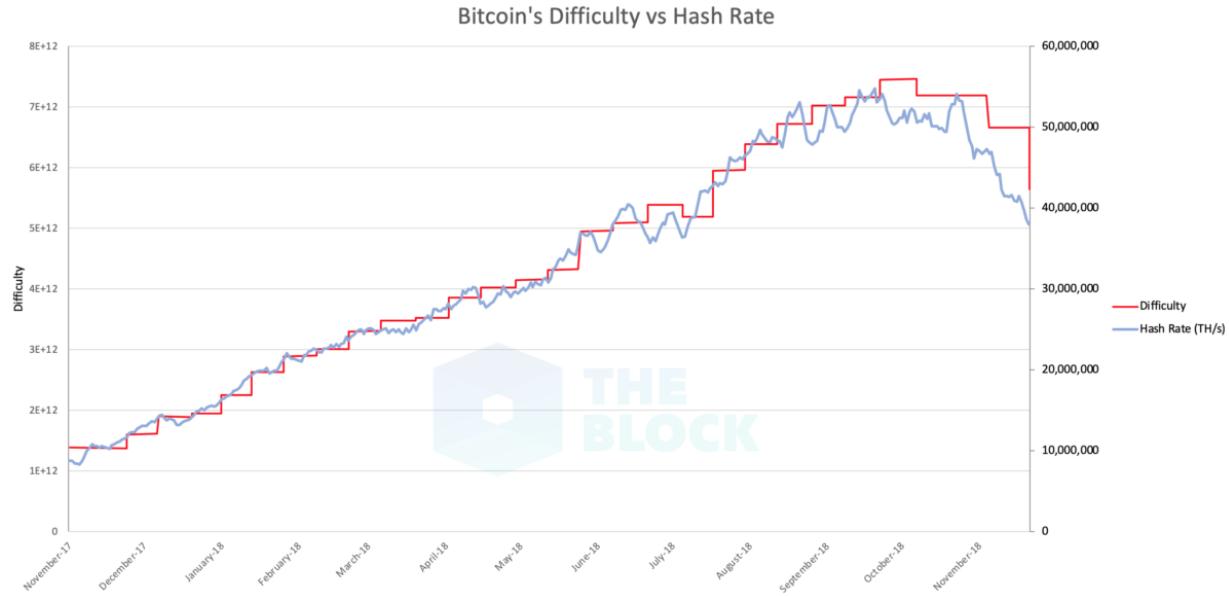
Bitcoin is not going into a “mining death spiral.”

Now that we've gotten that out of the way... rather than fear-mongering, *The Block* is committed to clarifying comments and concerns posed by crypto-fund managers and enthusiasts alike with level-headed technical clarity.

The case that Bitcoin is going into a miner-induced death spiral is intuitively compelling: Bitcoin prices drop materially, eventually marginally profitable miners shut off, ad infinitum, until all the miners are gone and no one mines Bitcoin (cue: Bitcoin is dead, redux). The argument is crutched on a few core assumptions often relied on by critics: \$BTC would have to trade sub-\$1000, with hash rate dramatically dropping off before the difficulty adjustment, the variable representing the difficulty of mining a new Bitcoin block. Miners, who are strictly rational short-term, would then choose to shut off all their miners or mine alternative cryptocurrencies rather than take losses mining Bitcoin unprofitably.

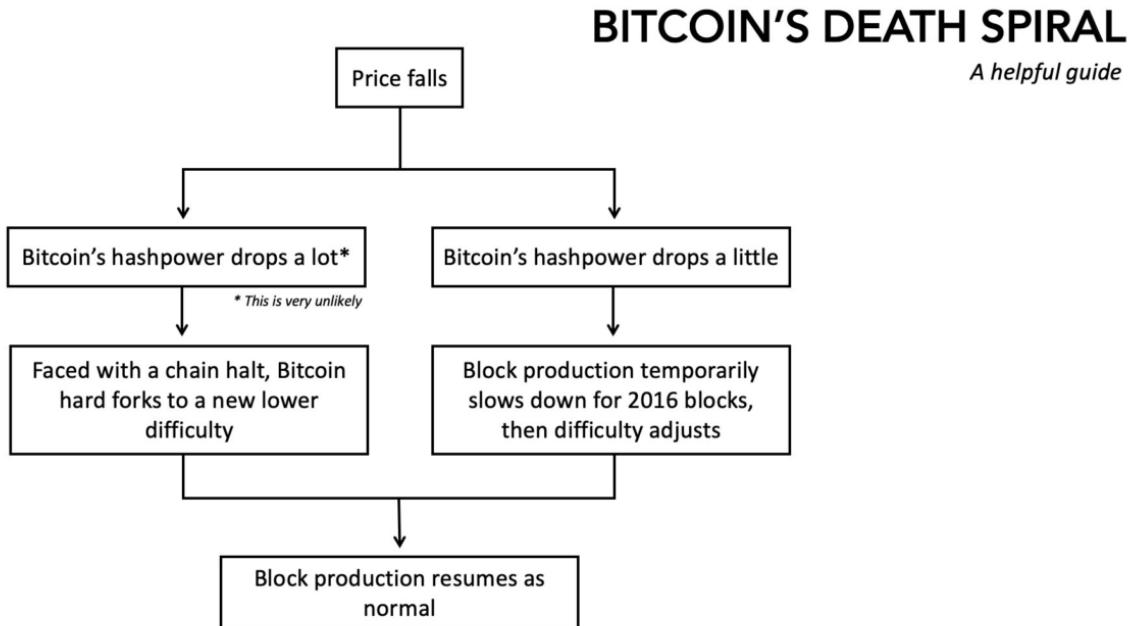
For context, Bitcoin's difficulty adjustment doesn't happen every two weeks. The difficulty of mining a Bitcoin block is naturally adjusted by the system every 2016 blocks, which probabilistically averages to two week intervals.

This tends to follow the hash rate, as seen below:



The biggest issue with the mining death spiral case is that we've seen this before. The narrative was first entertained on Bitcointalk forums as early as 2011. More recently, there was a resurgence in the ASIC era with the last cycle of Bitcoin mania. As now Messari CTO Dan McArdle noted in a January 28th, 2015 tweet: “What happened to everyone arguing that price-drop -> miners leaving -> systemic incentive fail spiral? Did it not happen after all? #duh”

Of course, while industrialized mining has changed the landscape materially, the fundamental game theory Bitcoin relies on have not. Bitcoin analyst Nic Carter elegantly explains the possibilities:



Before the proposed death spiral, Bitcoin could have an emergency fork to a manually adjusted lower difficulty (to speed up the process to the next natural adjustment). Of course, this is very undesirable and should be considered a last-resort.

The third possibility and likely possibility isn't covered on Nic's original chart out of simplicity: when hash rate drops off precipitously in between difficulty adjustments, higher fees can serve as a market-funded incentive to force miners to stay on.

Prior to proclaiming Bitcoin's demise due to the death spiral, it's important to understand a few common misconceptions about miners and their relationship with the difficulty adjustment:

- **The “break-even cost of mining” is much lower for many miners than is often quoted by analysts** (who focus on the average miner). Many of the most profitable miners have a “cost per Bitcoin” (opex + capex) that asymptotically approaches 0. This is the combined result of heavily-subsidized electricity (often free or even negative-cost) and extremely low cost of ASICs for the largest miners, who are often vertically integrated or receive favorable deals from hardware manufacturers.
- Similar to producers in other markets (e.g., traditional commodities), **miners have a set of constraints that may rationally force them to mine at a loss** — this is a situation accounted for by miners. These constraints include long-term power purchase agreements, hardware purchase agreements, facility leases, and other financial arrangements. With these constraints and

strategically-planned cash reserves, miners can mine at a loss for an extended period.

- Contrary to mining other commodities, where mining at a loss results in sustained price suppression (due to increased supply in the market), **rational miners want to mine Bitcoin to accelerate the time to the next difficulty adjustment** (which more accurately reflects the “real” difficulty of mining). The miners that endure a crypto “bear market” are at a massive competitive advantage, as we saw with miner consolidation in the last market cycle.

The nuances of Bitcoin’s game theory — the fee market, miner incentives, etc. — are often mis-understood and mis-represented with appeals to narrative, rather than historicism and pragmatic analysis.

Be better than the narrative. *Disclosure: Arjun Balaji is an analyst, engineer, and technical advisor to The Block. He founded Shomei Capital and holds bitcoin.*

Beware of Lazy Research: Let's Talk Electricity Waste & How Bitcoin Mining Can Power A Renewable Energy Renaissance

Bitcoin mining update—Part 2 of 2

By Christopher Bendiksen

Posted December 6, 2018

This is part 2 of a 2 part series

- Part 1 An Honest Explanation of Price, Hashrate & Bitcoin Mining Network Dynamics
 - Part 2 Beware of Lazy Research: Let's Talk Electricity Waste & How Bitcoin Mining Can Power A Renewable Energy Renaissance
-

If you're reading this, then perhaps you've read the [latest CoinShares Research report on the bitcoin mining network](#), [my previous commentary on creation costs](#), or even better: both!

Or maybe you haven't read either and came straight for the hot sauce.

Either way, at this point you probably haven't missed it: the hottest narrative in the anti-Bitcoin playbook is the environmentalist attack on Proof-of-Work (PoW) consensus algorithms. Exhibit A:

Oh dear...



Nouriel Roubini  @Nouriel

I could gloat about Bitcoin collapsing 10% in a day to \$5700. But that is still some way to ZERO where Bitcoin belongs. Actually since Bitcoin is The Mother of All Toxic Pollutions & Environmental Disasters its true fair value is highly NEGATIVE with the right externality tax

1,129 1:04 PM - Nov 14, 2018

963 people are talking about this >

While it's encouraging that Bitcoin detractors are clearly running out of ideas, it is nevertheless a powerful narrative—especially for younger generations whose future prosperity not only rests on the reintroduction of sound money, but also on a relatively benign global climate.

Thus we feel compelled to address this narrative with data and methodologies that hold up against both internal and external scrutiny. In our view, this is more than can be said for most (not all) of the research underpinning the narrative that we hope to debunk, once and for all.

Bitcoin is boiling the oceans!

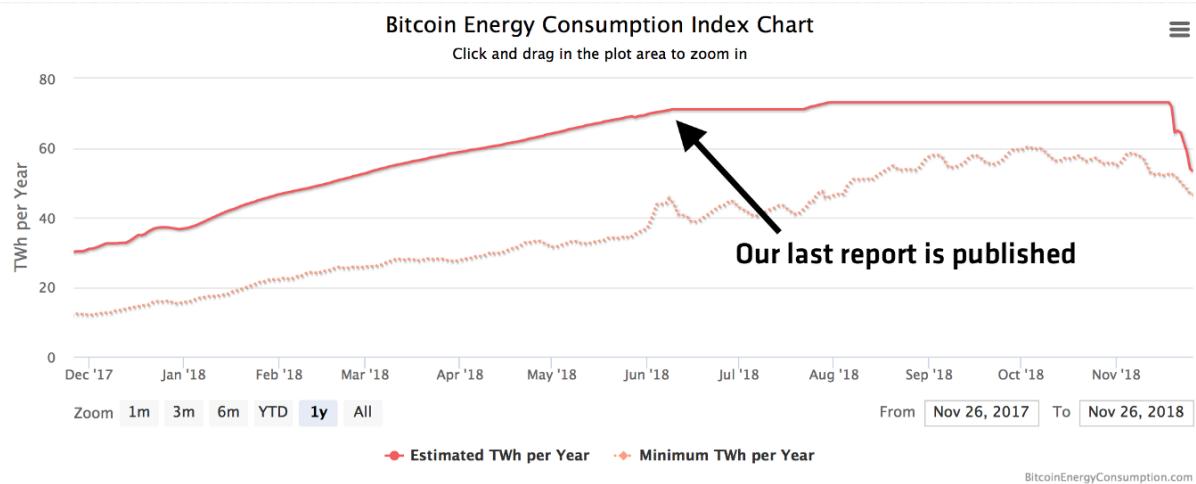
You've surely heard it. Where did this idea originate?

As with many dubious claims, it shouldn't come as a surprise that much of it is underpinned by a single, leisurely researched source: Digiconomist.

In fact you'd be hard pressed to find many articles in the press pushing the environmentalist, anti-PoW narrative that do not link back to that one source. But hey, can you really blame them in today's sound bite media environment? Research is hard and time consuming.

Without spending too much time on Digiconomist, I cannot avoid pointing out that within days of releasing our last mining report—which offered a more granular methodology for estimating the total power draw of bitcoin miners—and after being

called out in no uncertain terms by [Nic Carter](#) on Twitter, the [Bitcoin Energy Consumption Index](#) on the website mysteriously flatlined **even though** the hashrate continued growing. Strange.



Screenshot of the Digiconomist website.

I also need to give some praise here though: it takes courage to admit you were wrong. I respect that.

For any journalists who happen to read this—please consider your sources before treating their unsubstantiated opinion as fact in your coverage!

The typical anti-PoW argument

So let's reconstruct the environmentalist argument, which usually goes something like this:

A1—Bitcoin mining is highly energy intensive.

A2—The vast majority of bitcoin miners are located in China.

A3—Bitcoin miners in China are mostly using dirty, coal-based power.

C1—Bitcoin mining has a comparatively extreme carbon footprint.

C2—Bitcoin is bad.

The first assumption is true, we all know that. It's one of the fundamental reasons the Bitcoin network is so incredibly secure!

The second assumption used to be true, and is still not **that** far from the truth—but it's inaccurate nonetheless. (For the sake of this post we'll call it true, because it doesn't really matter all that much.)

The third assumption however, is false, which ruins both conclusions.

How do we know that? Because unlike certain other frequently cited sources, we actually did the research. And to be clear, ***this was grueling, backbreaking research.***

As of writing, we've now spent over a year getting to the bottom of this claim, and it wasn't easy by any measure.

We've talked to everyone that would talk to us, and pestered those that wouldn't. Rejections left and right. Our mining analyst Samuel Gibbons has trawled every forum, every message board, every channel, every press release, every public company release and every news article we could find. Some in English, many in Chinese.

So I completely understand the temptation to use hypothetical top-down assumptions for these calculations, I really do. Especially if it fits a certain narrative that one wants to push. I mean, if it looks like it could make sense, who would ***actually*** take the time to check, right?

Well, we did check and feel confident that this assumption has been soundly proven wrong. As such, we hope the assertiveness is scaled back a few notches while the methodologies are revisited and more work invested in the process.

And while we're on the subject, we'll be the first to admit —***our results likely have significant error margins*** (although we chose to use assumptions that should place us at the conservative end of this margin and not the other way around). **We would appreciate any additional efforts directed towards double- and triple-checking these conclusions.**

Poor research—whether the result of lazy ignorance or outright dishonesty—works to everyone's detriment. We **need** higher quality research in this space.



The reality of Bitcoin's energy mix

Bitcoin mining is mainly driven by renewable energy—hydro (by far the largest component), solar, wind and geothermal. Period.

In fact, we've estimated the lower bound of renewables penetration in the bitcoin mining energy mix to be 77.6%.

We actually think it's significantly higher than that, but in the name of defensible conservatism, we won't say what that number is.

Everyone seriously involved in bitcoin mining already knows this—and has known for years—but it's been surprisingly hard to quantify so we've kept our heads down in case we were all somehow wrong. The mining industry is notoriously secretive which makes it exceptionally tough to find or extract quality data.

So how'd we do it?

First, we decided to turn the commonly employed top-down methodology on its head and go bottom-up instead.

This means that instead of picking a single or couple mining units and using their specs as a proxy for the entire network—essentially pretending the entire network is simply a multiple of the same unit(s)—we went the other way around and figured out approximately how many units of each mining hardware exist in the current network.

Over the last year we painstakingly assembled a model of all mining gear produced in quantities exceeding 1000 units. We collected performance specs, volume weighted average purchase prices, batch sizes and total deployment numbers.

From that dataset we calculated that the bitcoin mining network currently draws approximately 4.7 GW, or 41tWh on an annualised basis.

At the time of writing, this figure is falling—and has been since late September. The estimate also includes a 20% excess for cooling, a figure we consider highly conservative.

For reference, there are approximately 85m PlayStation 4, 40m Xbox One and 15m Nintendo Wii U consoles distributed among global households (see our report for full list of sources). Their weighted average gameplay power draw is approximately 120W.

Assuming these gaming systems are played on a modern 40" LED TV drawing only 40W, for 4 hours a day, and idling for 20 hours a day, at a weighted average of 10W, they alone draw more power (4.9GW) than the entire bitcoin mining network.

This doesn't even consider the renewables penetration in their energy mix, which assuming they are globally distributed, is a measly 18.2%.

As Dan Held would implore: somebody call the electricity police!

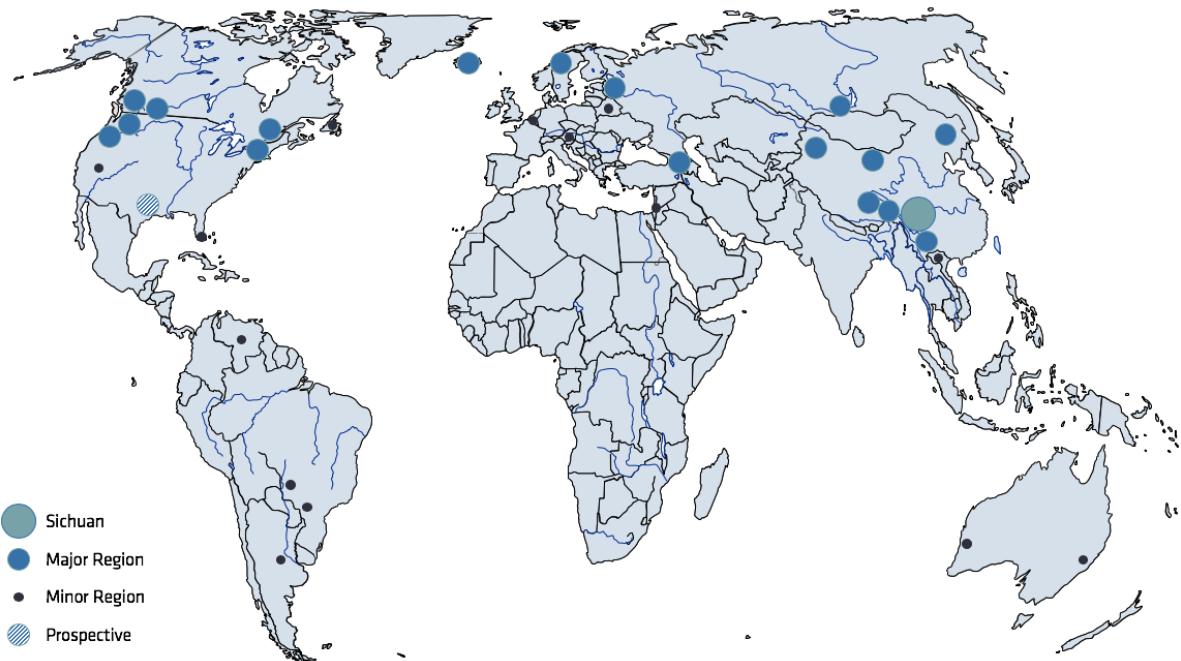
Here's another one for ya.

The screenshot shows a tweet from Dan Hedl-onaut (@danheld) with the handle @danheld. The tweet contains the text "Electricity Police assemble! 🚨" and a link to a Phys.org news article: "US Christmas lights use more energy than entire countries" (phys.org/news/2015-12-c...). The tweet was posted at 10:37 PM - Nov 22, 2018, with 418 likes. Below the tweet is a photograph of a house decorated with numerous Christmas lights, including nutcracker figurines and wreaths. The caption under the photo reads: "US Christmas lights use more energy than entire countries" and "American household Christmas lights, a favorite holiday tradition, use up more electricity than some poorer countries—such as El". At the bottom of the screenshot, it says "131 people are talking about this".

You were talking about renewables though?

I was indeed. This was a tough nut to crack. And while we searched and prayed for shortcuts to quantify the renewables penetration in the energy mix of miners, there is none. So we had to do it manually.

Over that same year, we also mapped out every relevant global mining region. The result looks like this (full source list in the report):



We then teamed up with some friends at [Three Body Capital](#), who were able to source provincial-level curtailment rates and renewables penetrations in China. We combined this with publicly available renewables data for the non-Chinese regions and thus were able to arrive at a lower bound for the renewables penetration. What did we find?

Not only does the Bitcoin network consume much less power than its detractors claim, it is mainly driven by renewables—77.6% lower bound versus global avg. of 18.2%

By inference, Bitcoin is therefore 'cleaner' than almost every other industry.

(I know I keep saying this, but for a full overview of our numbers and figures, please check out the paper itself)

Doesn't this just displace other demand onto fossil electricity?

The short answer: for wind and solar, possibly—but this is only if miners that rely on them wish to mine 24/7 and are located in fossil-dependent regions(miners like that might exist, but are rare in the industry).

For hydro, this is much less of a concern. And here's why:

In reality, there is really no clean separation between electricity sources on the grid. *Overly simplified**, every producer contributes their production to the same grid, from which all demand is drawn.

(*Sidebar—this is not technically true as there are often incompatible and/or semi-isolated grids operating in areas that you would assume were economically integrated from an electricity standpoint)

Assuming this was the case for simplicity's sake, then you could argue that Bitcoin simply displaces other competing demand onto fossil fuels.

While this may seem reasonable on the surface, in reality it is not so straightforward. The reasons for this are slightly complicated, but it roughly comes down to a matter of geography and physics.

I will restrict this discussion to hydro power as this is the largest component of global renewables generation and an even bigger component of Bitcoin mining. Most of this also applies to geothermal power which suffers from many of the same geographical issues as hydro.

Working with nature

Hydro power, while awesome, comes with the enormous drawback that you cannot build it wherever you want.

This should be obvious. The most productive hydropower is often found where there's a combination of powerful rivers in mountainous terrain or highlands. Most humans, however, live in lowlands where it's easier to grow food.

Fossil fuel power plants are therefore built close to the population centres they are intended to serve. Hydro plants, on the other hand, must be built where nature produces the prerequisite conditions to sustain them, which is often far away from demand centres.

This issue persists in China, the US, Siberia, Scandinavia, and Central South America: the best areas for hydro development is simply not where most people actually live.

For example, in the United States most hydro power is generated in—you guessed it—the mountains. More specifically, it is largely produced in the Columbia River basin of the Pacific North West, which according to the [EIA](#), provided 44% of all hydroelectric power in the US in 2012.

Americans, however, do not tend to live in the mountains—they live predominantly on plains in California, around the Gulf of Mexico, Mississippi Basin and along the East Coast.

This causes a problem. You simply cannot transmit electricity from the Pacific Northwest to California, Texas, or the East Coast while maintaining the same cost profile.

Why not?

Whenever electricity is sent through a medium, *electrical resistance* will cause the medium to heat up while consuming some of the electrical power (unless the medium is a superconductor). This is how incandescent light bulbs and many electrical heaters work—it is also the reason your computer gets hot.

The [EIA](#) lists transmission losses for High Voltage Direct Current (HVDC) lines at 3% per 1000 km, versus 7% per 1000 km for High Voltage Alternating Current (HVAC) lines.

HVAC is cheaper than HVDC and is normally used for short distances, whereas the latter is more expensive and used for longer distances. Lest you get the wrong idea though, they are both expensive, just one even more so than the other. Also, transmitting power over long distances often involves a bit of both.

HVDC lines act as 'superhighways' of power transmission and run along certain highly trafficked routes, while HVAC 'access roads' connect them to the wider region. Further driving up the cost—nobody wants them nearby. They're ugly, and some people believe they cause all sorts of exotic pathological conditions.

The best locations for hydro plants are not necessarily well-connected to this transmission network—or even anywhere near it—and there are other factors limiting the economic viability of building new transmission lines such as mountain ranges or national parks. This makes remote power plants particularly vulnerable to transmission losses.

Transmission losses effectively increase the cost of electricity as you transport it away from its source.

Electricity prices can be seen as a spectrum, increasing as you move further away from its sources. The cheapest price is always right at the power plant, which is precisely why Bitcoin miners cluster as close to their sources as possible.

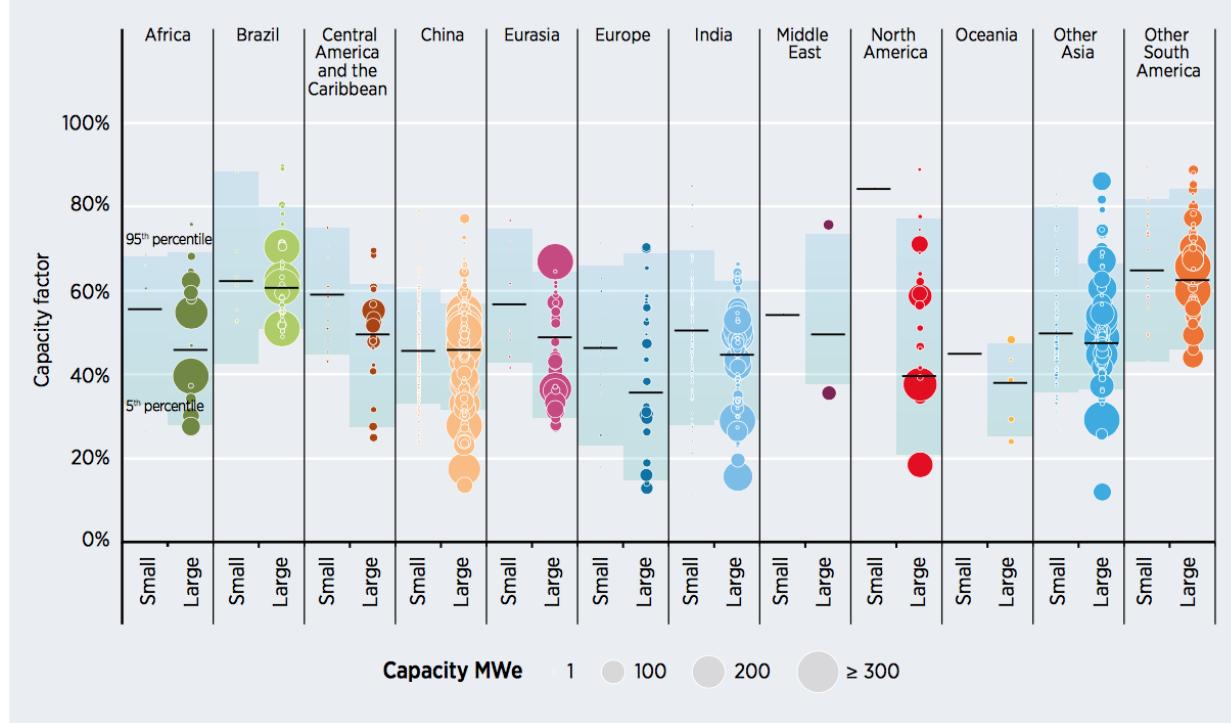
Stranded hydro

Often then, before hydro power can reach large population centres, transmission losses can make its price rise above that of competing fossil or nuclear power plants.

The net effect is that a significant amount of hydro power becomes **stranded**, meaning some of its potential output cannot be sent to demand centres while retaining a competitive price.

While this is unfortunate from an environmental standpoint, consumers tend to prefer cheap electricity to expensive electricity (for obvious reasons).

We can gain some insight to the overall usage of already installed hydro power plants by looking at their *capacity factors*. According to the International Renewable Energy Agency, global hydro capacity factors between 2010 and 2016 were 49%, meaning that global hydro plants _on average produced at **less than half** of their capacity.



https://www.irena.org/-/media/Files/IRENA/Agency/Publication/2018/Jan/IRENA_2017_Power_Costs_2018.pdf

Now this does *not necessarily* mean that out of the total global installed hydro power capacity of 1,121 GW, more than half is wasted (for comparison, remember that the Bitcoin network currently draws 4.7 GW, or 0.4% of that).

Plants may be built to accommodate variable daily demand peaking with human waking hours, or seasonal supply of water peaking with cyclical rainy seasons. This is also one of the reasons we chose to use annual net power produced — **not installed capacity** — in our calculations, as the latter skews the numbers in favour of renewables.

Wasted hydro

That being said, there are still multiple sources that *do* suggest that **enormous amounts of hydro power is actually wasted** (by simply letting water flow over the dams) every year.

The magnitude in China alone is staggering. According to Reuters, citing the provincial governor Ruan Chengfa, in Yunnan Province **alone** 30 TWh of hydro power is wasted every year. Again, **the entire** Bitcoin mining network draws an annualised approximate 41 TWh at current rates.

Things are not much better in neighbouring Sichuan — home of an estimated 42% of all Bitcoin hashpower — where another Reuters article explains that the province's total hydro capacity of 75 GW (versus Bitcoin's 4.7 GW draw), is more than double the capacity of its grid! The implication being that power on the order of hundreds of TWh are wasted every year.

By the way, if you're curious how this economic quagmire came to be, first consider the information asymmetry between central planning committees and the distributed free market; then go read this excellent piece by our colleagues at BitMEX Research.

But wait, there's more

I'll preface by saying that we have not been able to conclusively prove this thesis (yet), but it has been postulated by other researchers and deductive reasoning suggests it is indeed true.

While there is anecdotal evidence supporting it (sources in report) and we would prefer harder proof before we claim this to be conclusive, consider the following:

Because bitcoin mining is highly mobile compared to overall power demand, it might actually be a boon for global stranded renewables. Whereas traditional

industrial and residential power demand is largely geographically captive—be it by proximity to cities, resources, transport links or whatever other factors determine the location of such entities—bitcoin mining can be undertaken pretty much anywhere.

As discussed above, nature-driven energy production is necessarily bound to where natural energy sources are located. Unlike fuel-based generation, they cannot be placed wherever demand is strongest and fuel can be sourced. This is important for two reasons.

1. High voltage grids are expensive to construct, which means they are only economically viable if the size of the generating plant(s) is large enough. The farther away the power plant is, the more expensive the grid connection will be.
2. Long-range energy transmission incurs losses for producers as a significant percentage of the electricity is lost to heat dissipation during grid transmission. This effect worsens with distance.

Combined, these two factors have a dampening effect on renewable energy development. Rivers, deserts and windy spots are where they are and cannot be moved. Building up renewables projects to the necessary scale required for grid connection is capital intensive and often prohibitively risky if unconnected to cornerstone demand.

This means that some of our most promising sources of renewable energy remain untapped due to their remote locations.

Again, this energy is effectively ***stranded***.

We also see this problem in projects that are already built. For various reasons, many renewables projects today are significantly under-utilised. Most often because: (a) they are located far away from large demand centres; (b) previous cornerstone clients have moved or shut down; or (c) the anticipated demand never materialised as hoped.

These projects generate electricity supplies in excess of demand, which forces down the price of excess supply, especially immediately around the power plant .

Such projects act as magnets for bitcoin miners. Unlike traditional industries, bitcoin mining is highly mobile and both ***can*** and ***must*** move to wherever power is cheap. All miners need is an internet connection and roads in—almost all modern power generation developments have both.

Bitcoin mining can thus serve as the cornerstone demand for the lowest cost renewables, wherever they may be. This both reduces the need for government subsidies and increases profitability.

Increased profitability makes reinvestment more attractive, which in turn can increase the scale of projects. Larger scale projects may then enable grid connection.

As soon as these projects are connected to legacy industries or retail demand, they will tend to bid prices up closer to regular market prices and bitcoin miners will be forced to move on to the next project.

Bitcoin mining is a relentless race to the lowest electricity costs and therefore—as explored by Dan Held and Nic Carter—acts as an electricity buyer of last resort.

In this manner, bitcoin mining—which offers the possibility of immediate electricity monetisation independent of grid connection—can play a vital part in the renewables development cycle.

The Takeaways

- Contrary to what you've heard in the media, bitcoin mining is not an environmental disaster. In fact, it is one of the cleanest billion-dollar industries on the planet.
- The combined total bitcoin mining network draws less power than global gaming consoles running 4 hours per day.
- Bitcoin mining is mainly powered on renewable energy, at levels more than four times higher than the global average (>77.6% vs ~ 18.2%).
- Every year, enough hydro power is wasted in Yunnan and Sichuan alone to power the Bitcoin mining network many times over.
- Bitcoin miners are highly mobile and can therefore serve as cornerstone demand for low-cost stranded renewables.
- By increasing profitability and lowering reliance on subsidies, bitcoin mining can positively contribute to the development and scaling of renewable energy projects wherever conditions are the most favourable.

Disclaimer

Please note that this Blog Post is provided on the basis that the recipient accepts the following conditions relating to the provision of the same (including on behalf of their respective organisation).

This Blog Post does not contain or purport to be, financial promotion(s) of any kind.

This Blog Post does not contain reference to any of the investment products or services currently offered by members of the CoinShares Group.

Digital assets and related technologies can be extremely complicated. The digital sector has spawned concepts and nomenclature much of which is novel and can be difficult for even technically savvy individuals to thoroughly comprehend. The sector also evolves rapidly.

With increasing media attention on digital assets and related technologies, many of the concepts associated therewith (and the terms used to encapsulate them) are more likely to be encountered outside of the digital space. Although a term may become relatively well-known and in a relatively short timeframe, there is a danger that misunderstandings and misconceptions can take root relating to precisely what the concept behind the given term is.

The purpose of this Blog Post is to provide objective, educational and interesting commentary. This Blog Post is not directed at any particular person or group of persons. Although produced with reasonable care and skill, no representation should be taken as having been given that this Blog Post is an exhaustive analysis of all of the considerations which its subject matter may give rise to. This Blog Post fairly represents the opinions and sentiments of its author at the date of publishing but it should be noted that such opinions and sentiments may be revised from time to time, for example in light of experience and further developments, and the blog post may not necessarily be updated to reflect the same.

Nothing within this Blog Post constitutes investment, legal, tax or other advice. This Blog Post should not be used as the basis for any investment decision(s) which a reader thereof may be considering. Any potential investor in digital assets, 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.

This Blog Post is subject to copyright with all rights reserved.

Thanks to CoinShares.

Skeptic's Guide to Bitcoin: Bitcoin and the Promise of Independent Property Rights

A framework for skeptics, part 3

By Su Zhu and Hasu

Posted December 13, 2018

This is part 3 of a 4 part series. See additional articles below

- Part 1 Skeptic's Guide to Bitcoin: An Honest Account of Fiat Money
- Part 2 Skeptic's Guide to Bitcoin: Unpacking Bitcoin's Social Contract
- **Part 3 Skeptic's Guide to Bitcoin: Bitcoin and the Promise of Independent
Property Rights**
- Part 4 Skeptic's Guide to Bitcoin: Investing in Bitcoin

Right: Photo by Thought Catalog
on Unsplash

In the second part, we showed how Bitcoin is a novel social and economic institution. But the question remains: **Who is going to use it?** Is there a place for Bitcoin among other institutions, and if so, where is it? Is Bitcoin just a terribly inefficient competitor to PayPal and Visa, like the media wants you to believe, or something more?



To put Bitcoin on the map with other institutions, let us first understand why humanity built social institutions in the first place.

Humans don't scale. Sure, we can learn, but we can't upgrade our brains and bodies like we can upgrade the hard drives and processors in our computers and machines. In fact, our physical and mental capacities have remained virtually unchanged since we roamed the earth as hunter-gatherers. Instead, we scale through cooperation. All

scientific breakthroughs, all increases in productivity and prosperity, can be traced back to our ability to cooperate with each other.

Cooperation has a Scaling-Problem

But because our world is fundamentally uncertain, cooperation doesn't come easy for us. We spend massive amounts of efforts on predicting how other people are going to react to our actions, and if those actions could affect us negatively.

When we can't reliably predict the behavior of others, our lives become a prisoner's dilemma. Should we cooperate with someone else to hunt down a stag, or stick to a rabbit which we could hunt alone? How can we trust him not to hit us over the head with a club and steal the stag? The path for humanity to "scale" and prosper is to find a way to break these prisoner dilemmas and cooperate anyway.

Game theory gives us two solutions to the prisoner's dilemma. The first is to turn the one-time-game into a repeated (or "iterated") game. If you and your potential hunting partner meet again tomorrow, you are more likely to behave, as each of you has to worry about the other's retaliation. But such repeated social interactions—or experience—are only possible with a limited group of people at the same time, as proposed by the anthropologist Robin Dunbar.

Dunbar's number is a suggested cognitive limit to the number of people with whom one can maintain stable social relationships. Its proponents assert that numbers larger than this generally require more restrictive rules, laws, and enforced norms to maintain a stable, cohesive group.

Cooperation through Institutions

The second rule, which Dunbar alludes to, is to "tie our own hands" and restrict ourselves from taking negative options that could hurt others. One such way is by adopting a shared morality and making sure these rules are socially enforced. But for groups that exceed Dunbar's number, we need institutions.

The most basic of all institutions is a monopoly of violence. By empowering a specialized group of people to a focus on protecting your town, you can more easily engage in productive enterprises because you don't have to worry if you can protect the fruits of those enterprises. Establishing a strong and benevolent monopoly on violence also strengthens the shared morality and formalize it to a formal legal system. The rules become more credible, after all, if there is a party strong enough to overpower any individual and make sure no one is "above the law".

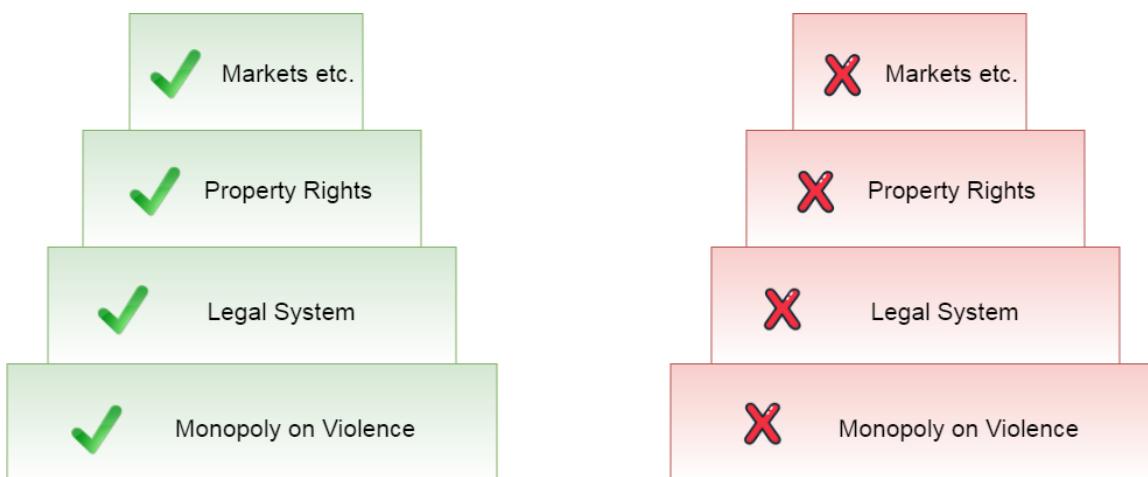
On the shoulders of the monopoly on violence and the legal system, rests the most important institution of all: the right to private property. A private property system,

protected by the state, gives you the exclusive right to your own resources and to use them as you see fit. Research has found that prosperity and property rights are inextricably linked.

Property Rights

Having well-defined and strongly protected property rights is the basis for all higher institutions: Markets are match-making systems between buyers and sellers that allow for specialization and the division of labor, while money allows for the creation of accurate price signals to producers and consumers.

We need a monopoly on violence to have a legal system, and we need a legal system to have property rights. We need property rights to have markets and firms, and we need markets and firms to have capitalism. It is through the invention of new institutions, each building on the existing ones, that civilization advances. Here is a simplified image of the institutional stack:



Simplified example of a stable institutional stack:

A strong foundation ensures the stability of the whole.

Examples: North America, Europe

An unstable stack in comparison:

Stability of higher layers can't develop on an unstable foundation.

Examples: Parts of Africa, South America, Middle East

By streamlining human interactions, social institutions break the prisoner's dilemma and have us worry less about being harmed by others. The resulting increase of mutual predictability allows us to extend our trust to strangers and enable cooperation beyond Dunbar's number.

The Bitcoin Institution

If we see bitcoin as a novel institution, which rights does it unlock? Let's remember the rules of the Bitcoin social contract: Anyone can use the bitcoin network without permission (no censorship) and only he who owns money can spend it (no confiscation). Further, there is no central party that can print more money ahead of schedule and steal purchasing power from others (no inflation). Finally, anyone can verify that the rules are being followed before they accept a payment (no counterfeiting).

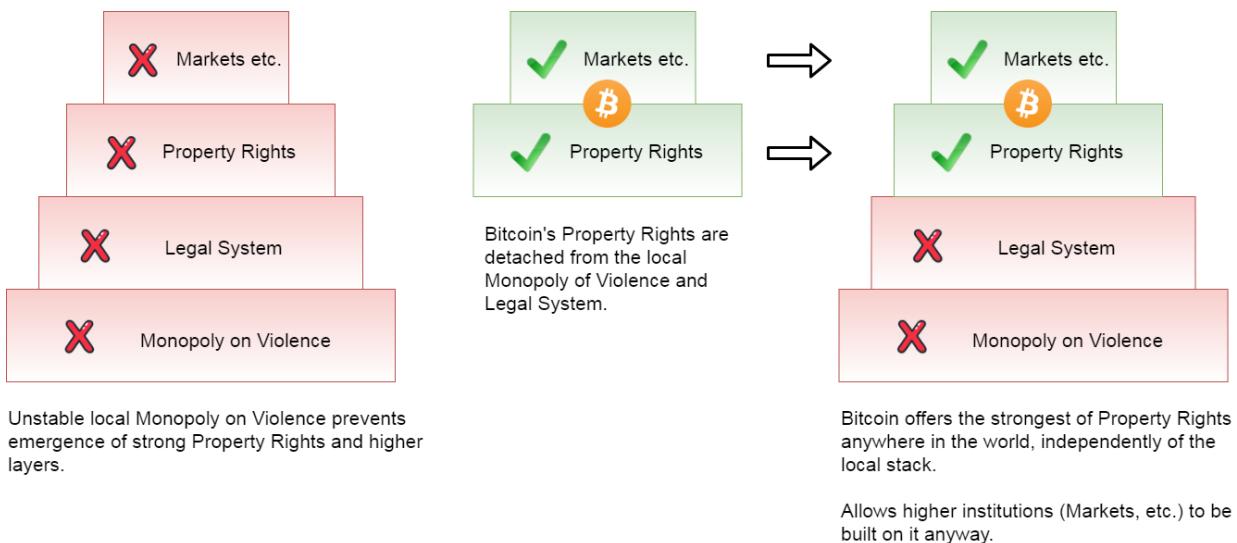
Do these rules stand the test of reality? In his excellent paper "How Bitcoin functions as property law", Eric D. Chason states that "Satoshi Nakamoto has created a form of property that can exist without relying on the state, centralized authority, or traditional legal structures."

I will go one step further and say that the bitcoin network, and, by extension, its money token **enable the highest form of property rights of any socio-economic institution in the history of man.**

A New Era in Property Rights

That is the key innovation of Bitcoin: **It detaches property rights from the legal system and the monopoly on violence.** For the first time, we can have property that does not rely on a local authority to enforce and protect. It is easy to conceal, defend, divide, move, and verify—all by yourself, granting you the highest level of personal sovereignty.

Property rights used to depend firmly on other layers of the social institution stack, specifically the monopoly on violence and the legal system. If the bottom of this stack is shaky, you cannot have strong property rights. But because Bitcoin stands entirely on its own, it can bring the highest level of property rights to anyone in the world, no matter the quality of their lower-level institutions, the government or legal system.



Bitcoin unlocks a different dimension of value. In the same way that boats unlocked transport over water, and airplanes through the air, Bitcoin unlocks a new, alternate layer to store and move value—as the first native digital asset. It is the ability to exist solely in that digital world, from which Bitcoin derives all of its properties. It cannot be attacked in the physical space the way that physical assets can.

The implications of this will only reveal themselves over time, but we can already speculate who bitcoin maybe be tremendously useful for:

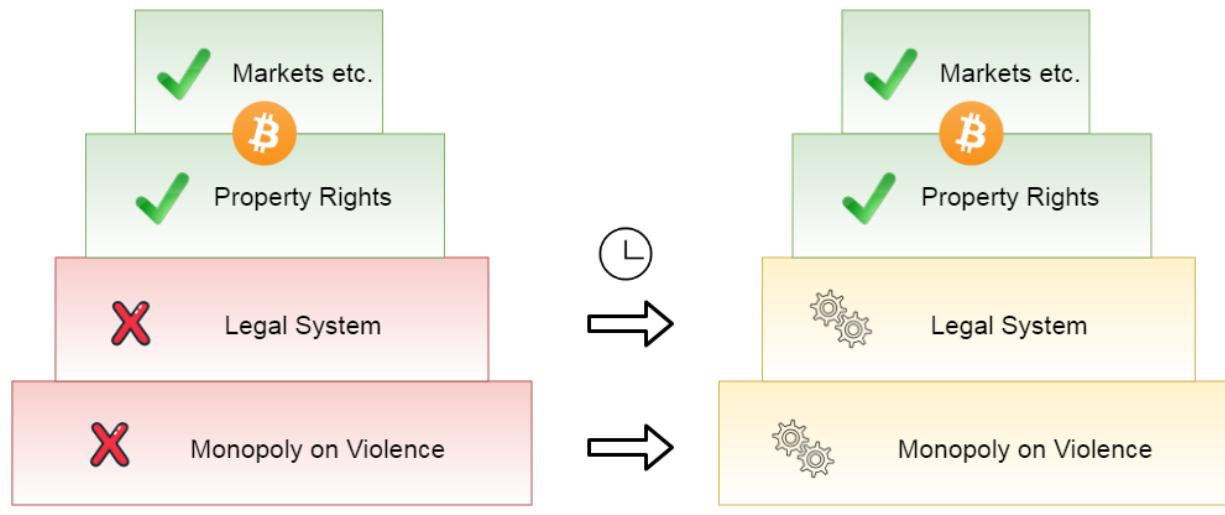
1. Anyone living in places with weak local property rights
2. Anyone subject to discrimination from the existing financial system
3. Anyone living in places with a weak local currency, with high (risk of) inflation
4. Anyone looking to store or move meaningful amounts of value (the highest value requires the highest amount of security)

Using Bitcoin gives these people the ability to cooperate more effectively, increase their productivity and, as a result, their prosperity. It allows them to save money for the future, to build capital that can be invested in more productive enterprises and let them partake in global trade with others all around the world.

Progress through Competition

Bitcoin can also benefit those who never use it. As a hedge against central bank error, it makes the global financial system more resilient. Ironically, it can also improve other monetary and property systems around the world. *What?* Yes, that is the effect that competition has on a market. If you are a customer of Apple, you

benefit from Samsung releasing a new phone, because it forces Apple to improve the quality of their product to stay competitive.



Through competition, Bitcoin can put pressure on bad local authorities to better themselves.

Over a long enough period of time, the incentive to abuse citizens could decrease (because wealth gets harder to confiscate or steal via inflation).

As a result, we could witness a quality improvement in monetary and property systems, because bitcoin opened the door for competition and created a market. This also shapes our understanding of what Bitcoin is NOT: a competitor to VISA or PayPal. It competes with local governments, legal systems and property rights—the fundamental layers of the existing stack—not with the payment processors that sit on top of it.

Civilization scales through cooperation, but cooperation between strangers is inherently hard. Social institutions can solve this prisoner's dilemma and allow us to cooperate on a larger scale. At the bottom of the stack, we need a stable and benevolent monopoly on violence, to enforce the rules of the legal system and establish property rights. Until now, it was impossible to have strong property rights in places with a weak local government. Bitcoin does not depend on the existing system in any way and can give us the highest form of property rights, no matter who and where we are.

Acknowledgments

I want to thank Yassine Elmandjra, Nic Carter and Miles Suter for their contributions.

Introducing Realized Capitalization

By the Coinmetrics Team

Posted December 14, 2018

The motivation for the creation of Realized Cap was the realization that "Market Capitalization" is often an empty metric when applied to cryptocurrencies. Market Capitalization, borrowed from the world of equities, is calculated for cryptocurrencies as

circulating supply * latest market price

However, unlike with equities, large fractions of cryptocurrencies tend to get lost, go unclaimed, or become otherwise inert through bugs. By design, there is no Depository Trust and Clearing Corporation which keeps track of everyone's stock certificates. So when tokens or virtual coins get lost, they stay lost. In Bitcoin, this means that roughly 15% of supply is assumed to be permanently lost and out of circulation. Market Cap does not consider these nuances, instead aggregating the value of all coins ever mined and assessing them at the last market price.

We wanted to create a measure that reflected this, at least for UTXO chains. Our design goals were as follows:

- De-emphasize lost coins
- Where possible, maximize generalizability (so reduce reliance on idiosyncratic adjustments)
- Do not deviate from Market Cap by more than a single order of magnitude

The eureka moment came when Pierre Rochard asked for data on a historically-weighted UTXO market cap for Bitcoin. This was mentioned to Coinmetrics engineer Antoine Le Calvez, who figured out an appropriate methodology and also dubbed it "Realized Capitalization." (It was previously called "Effective Cap".) Realized Cap seemed to fit the bill:

- It reduces the contemporary impact of long-lost coins
- It is trivially generalizable to UTXO chains, and, with some effort, generalizable to account chains
- It doesn't deviate from Market Cap by too much
- It is automated: it doesn't require (much) human oversight or intervention

When we first worked out the numbers in September, Bitcoin's Market Cap was \$115 billion and its Realized Cap \$88 billion. That seemed to make sense. Deriving new metrics from scratch is always tricky, so they need to pass the smell test too. Realized Cap seemed to do just what it said on the tin: weight coins according to

their actual presence in the Bitcoin economy. It is one of a new generation of economic measures which hybridizes market and on-chain data.

Of course, exotic new measures are not without risks. There are a few challenges here: dealing with deep-cold-storage coins, interpreting Realized Cap for coins with little turnover, and generalizing it to account based coins.

First, imagine Satoshi's ~ 700k-1m coins really were just in deep storage, and our dear leader was planning on spending them all on Bitcoin's 10th birthday – Jan. 03 2019. In that case, Realized Cap would be seriously underweighting the economic weight of Bitcoins in circulation, since it prices those long-lost coins at 2009 values... of \$0 per BTC. Realized Cap has a hard time differentiating between truly lost/abandoned coins and coins that are merely in yearslong deep cold storage. However, even the coldest of storage schemes do require periodic awakenings – to renew a multisig scheme, to take advantage of a fork, or to cash out a portion. So many of these accounts will have some amount of churn anyway.

Another issue is Realized Cap on smaller chains. Outside of the industry "blue chips," there are many chains with relatively little turnover. This poses a challenge for Realized Cap, as it is the sending of new coins that triggers the upwards (or downwards) revaluation at a new price. One common phenomenon we observed was price spikes, with many coins getting sent back and forth to exchanges, and an increase in Realized Cap, followed by a slow, low-velocity grind down where Realized Cap hardly moves. In this case the high Realized Cap was more of an artifact of the low turnover rather than a fair reflection of the network's pricing.

So how is Realized Cap calculated?

The realized cap attempts to improve on the market cap by trying to discount coins that might be lost. Its crux is to value different part of the supplies at different prices, instead of using the daily close as market cap does.

For UXTO coins, this consists in valuing outputs at the price at the time of their creation. For example, for a UTXO currency of supply 10 and market price of \$10, its market cap would be \$100. But if the UTXO set is as follows:

Value	Time of creation	Price at time of creation	USD Value at time of creation
-------	------------------	---------------------------	-------------------------------

8.3	2009-02-01	\$0.00	\$0.00
1.2	2011-03-17	\$1.00	\$1.20
0.5	2018-11-15	\$10.00	\$5.00

Its realized cap would be $\$0.00 + \$1.20 + \$5.00 = \6.20 or 6.2% of its market cap as 83% of the supply hasn't moved for years.

Extension to account based chains

Extending this metric to account based coins is a bit more complex. Instead of a list of unspent coins, the state in this case is represented as a list of accounts:

Account Balance

oxabc 8.3

oxdef 1.2

oxfad 0.5

Compared to the UTXO model, it is not possible to always assign a time of creation to a balance which makes assigning it a price, and thereby a value, hard.

Let's take an example transaction history for an account and see what methods can be used to accurately value its balance. We'll assume the current time is 2018-11-01 and the market price is \$150.00

Time	Change in balance	Price at time	Balance
2015-08-01	+1,000.00	\$0.01	1000.00
2016-02-01	+100.00	\$10.00	1100.00
2017-05-01	-50.00	\$50.00	1050.00
2017-12-17	-100.00	\$1200.00	950.00
2018-04-01	+20.00	\$200.00	970.00

From this data, several approaches can be used to value the balance:

Last movement price

We use the price at the last movement on the account: here \$200.00, this gives a realized balance of **\$194,000**.

This values accounts when they are active at all on the network. However, if someone sends dust to a lost account, its whole balance is re-valued at the current market price.

Last outgoing movement price

To avoid lost accounts being re-valued when someone sends money to them, we can use the price of the last time it had an outgoing movement (defaulting to the creation of the account if no outgoing payment).

In our case, this price is \$1200.00, the realized balance would be **\$1,164,000**.

Virtual UTXO

One downside of using the last movement price is that an account which has a very high balance and sends a tiny amount out would trigger a re-valuation of the whole balance at market price.

While it's the desired effect (after all, we just want to discount lost coins), it is unfair to UTXO based chains where the whole balance of an address is not taken into account for the realized cap, but just the coins used.

To reduce this undesirable effect, we can simulate a UTXO set for account based systems:

- each incoming payment creates a new coin attached to the account, the coin is valued at the price of the movement
- each outgoing payment triggers a coin selection on the coins attached to the account, the change is valued at the current market price

Let's replay the example account's history while maintaining this virtual UTXO, the coin selection we'll use is largest coins first:

Time	Change in balance	Price at time	Balance	Virtual coins	Realized balance
2015-08-01	+1,000.00	\$0.01	1000.00	(1000.0 at \$0.01)	\$10.00
2016-02-01	+100.00	\$10.00	1100.00	(1000.0 at \$0.01), (100.0 at \$10.00)	\$1,010.00
2017-05-01	-50.00	\$50.00	1050.00	(100.0 at \$10.00), (950.0 at \$50.00)	\$48,500.00
2017-12-17	-100.00	\$1200.00	950.00	(100.0 at \$10.00), (850.0 at \$1200.00)	\$1,021,000.00
2018-04-01	+20.00	\$200.00	970.00	(100.0 at \$10.00), (850.0 at \$1200.00), (20.00 at \$200.00)	\$1,025,000.00

This gives this account a realized balance of **\$1,025,000**.

Using Realized Cap on Coinmetrics

Right now, Realized Cap is only available for UTXO chains – we are still refining it for account-based chains.

For charting, you can find it on the chart as **Realized Network Value** (in keeping with our naming convention of using “Network Value” rather than Market Cap). If comparing Realized Cap to Market cap, we recommend hitting **settings** and selecting **no** on **Compare on different axes**.

Show all | Zoom out | Prev zoom | 1m | 3m | 1y | ytd | Full screen

Chart settings

Show Y-axis zero: Yes Nevermind

Compare on different axes: Yes No

Stack series: Yes No

Show crosshair: Yes No

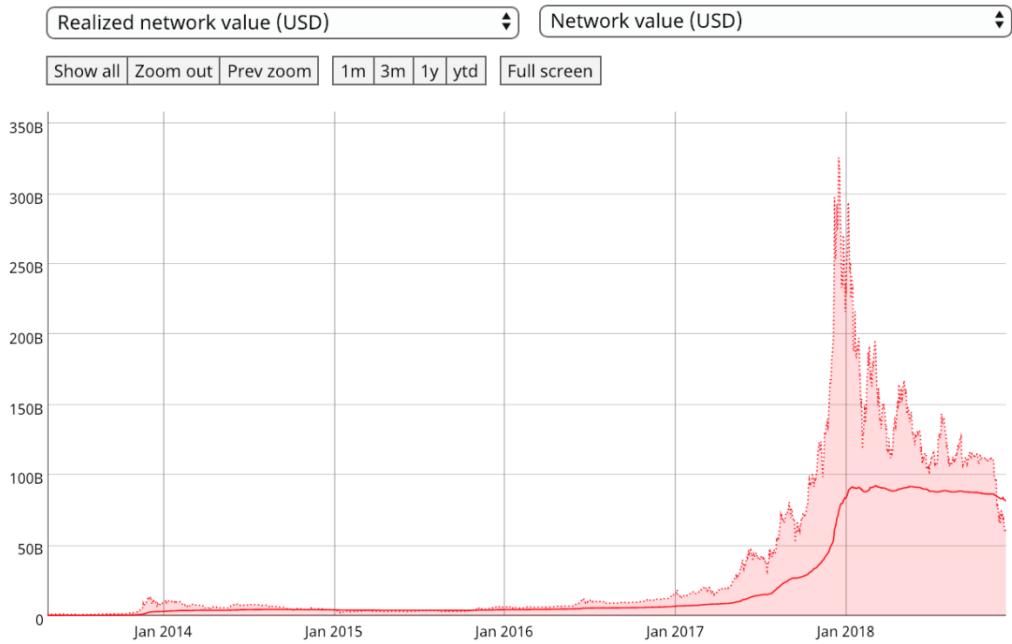
2

1

1-2009 | 6-2011 | 12-2013 | 6-2016 | 12-2018

Log | Lin | No avg | 7d | 14d | 30d | 50d | 90d | 200d | Basic | Formula |

This lets you create nice comparisons like this:



Bitcoin realized network value (solid red line) and network value (shaded area). [Link here](#) Keep in mind that on our charts builder page, the command for realized cap is

`Ticker.realizedCapUsd`

You can also create a ratio of the two.



Market cap to realized cap ratio The reasoning behind the ratio has been explored by Murad Mahmudov and David Puell [here](#).

Who Controls Bitcoin Core?

By Jameson Lopp

Posted December 15, 2018

The question of who controls the ability to merge code changes into Bitcoin Core's GitHub repository tends to come up on a recurring basis. This has been cited as a "central point of control" of the Bitcoin protocol by various parties over the years, but I argue that the question itself is a red herring that stems from an authoritarian perspective—this model does not apply to Bitcoin. It's certainly not obvious to a layman as to why that is the case, thus the goal of this article is to explain how Bitcoin Core operates and, at a higher level, how the Bitcoin protocol itself evolves.

The History of Bitcoin Core

Bitcoin Core is a focal point for development of the Bitcoin protocol rather than a point of command and control. If it ceased to exist for any reason, a new focal point would emerge—the technical communications platform upon which it's based (currently the GitHub repository) is a matter of convenience rather than one of definition / project integrity. In fact, we have already seen Bitcoin's focal point for development change platforms and even names!

- In early 2009 the source code for the Bitcoin project was simply a .rar file hosted on SourceForge. Early developers would actually exchange code patches with Satoshi via email.
- On October 30 2009, Sirius (Martti Malmi) created a subversion repository for the Bitcoin project on SourceForge
- In 2011, the Bitcoin project migrated from SourceForge to GitHub
- In 2014 the Bitcoin project was renamed to Bitcoin Core

Trust No One

While there are a handful of GitHub "maintainer" accounts at the organization level that have the ability to merge code into the master branch, this is more of a janitorial function than a position of power. If anyone could merge into master it would very quickly turn into a "too many cooks in the kitchen" scenario. Bitcoin Core follows principles of least privilege that any power bestowed to individuals is easily subverted if it is abused.

 **Peter Todd**
@peterktodd

Replies to @ummjackson @starkness
Core is transparent about the list that matters: the PGP keys who can sign merge commits.

The lesson to be learned here is to not trust GitHub! Even Bitcoin Core doesn't know the full list of people who can change the repo, as that extends to probably dozens of GitHub employees.

34 9:23 AM - Oct 4, 2018

[See Peter Todd's other Tweets](#)

From an adversarial perspective, GitHub can not be trusted. Any number of GitHub employees could use their administrative privileges to inject code into the repository without consent from the maintainers. But it's unlikely that a GitHub attacker would also be able to compromise the PGP key of a Bitcoin Core maintainer.

Rather than base the integrity of the code off of GitHub accounts, Bitcoin Core has a continuous integration system that performs checks of trusted PGP keys that must sign every merge commit. While these keys are tied to known identities, it's still not safe to assume that it will always be the case—a key could be compromised and we wouldn't know unless the original key owner notified the other maintainers. As such, the commit keys do not provide perfect security either, they just make it more difficult for an attacker to inject arbitrary code.

The Keys to the Kingdom

At time of writing, these are the trusted PGP fingerprints:

71A3B16735405025D447E8F274810B012346C9A6
 133EAC179436F14A5CF1B794860FEB804E669320
 32EE5C4C3FA15CCADB46ABE529D4BCB6416F53EC
 B8B3F1C0E58C15DB6A81D30C3648A882F4316B9B
 CA03882CB1FC067B5D3ACFE4D300116E1C875A3D

These keys are registered to:

Wladimir J. van der Laan <laanwj@protonmail.com> Pieter Wuille
 <pieter.wuille@gmail.com> Jonas Schnelli <dev@jonasschnelli.ch> Marco Falke
 <marco.falke@tum.de> Samuel Dobson <dobsonsa68@gmail.com>

Does this mean that we are trusting these five people? Not quite. Keys are not a proof of identity—these keys could potentially fall into the hands of other people. What assurances do you really get if you run the verify-commits python script?

```
python3 contrib/verify-commits/verify-commits.py Using verify-commits data from
bitcoin/contrib/verify-commits All Tree-SHA512s matched up to
309bf16257b2395ce502017be627186b749ee749 There is a valid path from "HEAD" to
82bcf405f6db1d55b684a1f63a4aab4376cdad7 where all commits are signed!
```

The [verify-commits](#) script is an integrity check that any developer can run on their machine. When executed, it checks the PGP signature on every single merge commit since commit 82bcf405... in December 2015—over 3,400 merges at time of writing. If the script completes successfully, it tells us that every line of code that has been changed since that point has passed through the Bitcoin Core development process and been “signed off” by someone with a maintainer key. While this is not a bulletproof guarantee that no one has injected malicious code (a maintainer could go rogue or have their keys stolen), it reduces the attack surface for doing so enormously. What are maintainers and how did they attain this role? We’ll dig into that a bit later.

Layered Security

The integrity of Bitcoin Core’s code must not rely solely upon a handful of cryptographic keys, which is why there are a multitude of other checks in place. There are many layers of security here to provide defense in depth:

Pull Request Security

1. Anyone is free to propose code changes to improve the software by opening a pull request against the master branch on [bitcoin/bitcoin](#).
2. Developers review pull requests to ensure that they are not harmful. Anyone is free to review pull requests and provide feedback—there is no gatekeeper or entrance exam when it comes to contributing to Bitcoin Core. If a pull request gets to the point that there are no reasonable objections to it being merged, a maintainer makes the merge.
3. Core maintainers set [this pre-push hook](#) to ensure that they don’t push unsigned commits into the repository.
4. Merge commits are optionally securely timestamped [via OpenTimestamps](#)
5. The [Travis Continuous Integration system](#) regularly runs [this script](#) to check the integrity of the git tree (history) and to verify that all commits in the master branch were signed with one of the trusted PGP keys.
6. Anyone who wants to can run [this script](#) to verify the PGP signatures on all of the merge commits going back to December 2015. I ran it while writing this article and it took 25 minutes to complete on my laptop.

Release Security

1. [Gitian](#) deterministic build systems are run independently by multiple developers with the goal of creating identical binaries. If someone manages to create a build that doesn’t match the builds of other developers, it’s a sign that non-determinism was introduced and thus the final release isn’t going to happen. If there is non-determinism, developers track down what went wrong, fix it, then build another release candidate. Once a deterministic build

has succeeded then the developers sign the resulting binaries, guaranteeing that the binaries and tool chain were not tampered with and that the same source was used. This method removes the build and distribution process as a single point of failure. Anyone with the technical skills can run their own build system; the [instructions are here](#).

2. Once the Gitian builds have completed successfully and been signed off by the builders, a Bitcoin Core maintainer will PGP sign a message with the SHA256 hashes of each build. If you decide to run a prebuilt binary, you can check its hash after downloading and then verify the authenticity of the signed release message with the hashes. Instructions for doing so [can be found here](#).
3. All of the above is open source and auditable by anyone with the skills and desire to do so.
4. Finally, even after going through all of the above quality and integrity checks, code that is committed into Bitcoin Core and eventually rolled into a release is not deployed out onto the network of nodes by any centralized organization. Rather, each node operator must make a conscious decision to update the code they run. **Bitcoin Core deliberately does not include an auto-update feature, since it could potentially be used to make users run code that they didn't explicitly choose.**

Despite all of the technical security measures that are implemented by the Bitcoin Core project, none of them are perfect and any of them can theoretically be compromised. The last line of defense for the integrity of Bitcoin Core's code is the same as any other open source project — *constant vigilance*. The more eyes that are reviewing Bitcoin Core's code, the less likely that malicious or flawed code will make it into a release.

Code Coverage

Bitcoin Core has a lot of testing code. There is an integration test suite that runs against every PR and an extended test suite that runs every night on master.

You can check the code coverage of the tests yourself by:

1. Cloning the Bitcoin Core GitHub repository
2. Installing the [required dependencies](#) for building from source
3. Running [these commands](#)
4. Viewing the report at `./total_coverage/index.html`

Alternatively, you can view the coverage report Marco Falke [hosts here](#).

Current view:	top level	Hit	Total	Coverage	
Test:	total_coverage.info	40570	45807	88.6 %	
Date:	2018-11-24 10:18:32	Functions:	5571	6585	84.6 %

Directory	Line Coverage	Functions
src	 85.7 %	13866 / 16188 81.6 % 2860 / 3505
src/compat	 97.0 %	32 / 33 100.0 % 8 / 8
src/consensus	 95.7 %	155 / 162 100.0 % 21 / 21
src/crypto	 76.8 %	1705 / 2221 92.7 % 76 / 82
src/index	 58.7 %	149 / 254 78.0 % 32 / 41
src/interfaces	 4.8 %	22 / 454 9.8 % 18 / 184
src/policy	 91.2 %	568 / 623 96.4 % 53 / 55
src/primitives	 94.1 %	225 / 239 97.1 % 102 / 105
src/rpc	 88.2 %	2843 / 3223 94.3 % 233 / 247
src/script	 94.0 %	2276 / 2421 86.1 % 290 / 337
src/support	 95.1 %	154 / 162 85.7 % 24 / 28
src/support/allocators	 100.0 %	14 / 14 100.0 % 2 / 2
src/test	 97.9 %	11037 / 11276 98.6 % 1021 / 1035
src/util	 94.6 %	857 / 906 82.7 % 210 / 254
src/wallet	 85.8 %	5663 / 6597 90.7 % 498 / 549
src/wallet/test	 99.9 %	804 / 805 100.0 % 83 / 83
src/zmq	 87.3 %	200 / 229 81.6 % 40 / 49

Generated by: [LCOV version 1.13](#)

Code Coverage Report

Having such a high level of test coverage means that there is a higher level of certainty that the code functions as intended.

Testing is a big deal when it comes to consensus critical software. For particularly complex changes, developers sometimes perform painstaking mutation testing—that is, they test the tests by purposely breaking the code and seeing if the tests fail as expected. Greg Maxwell gave some insight into this process when he discussed the 0.15 release:

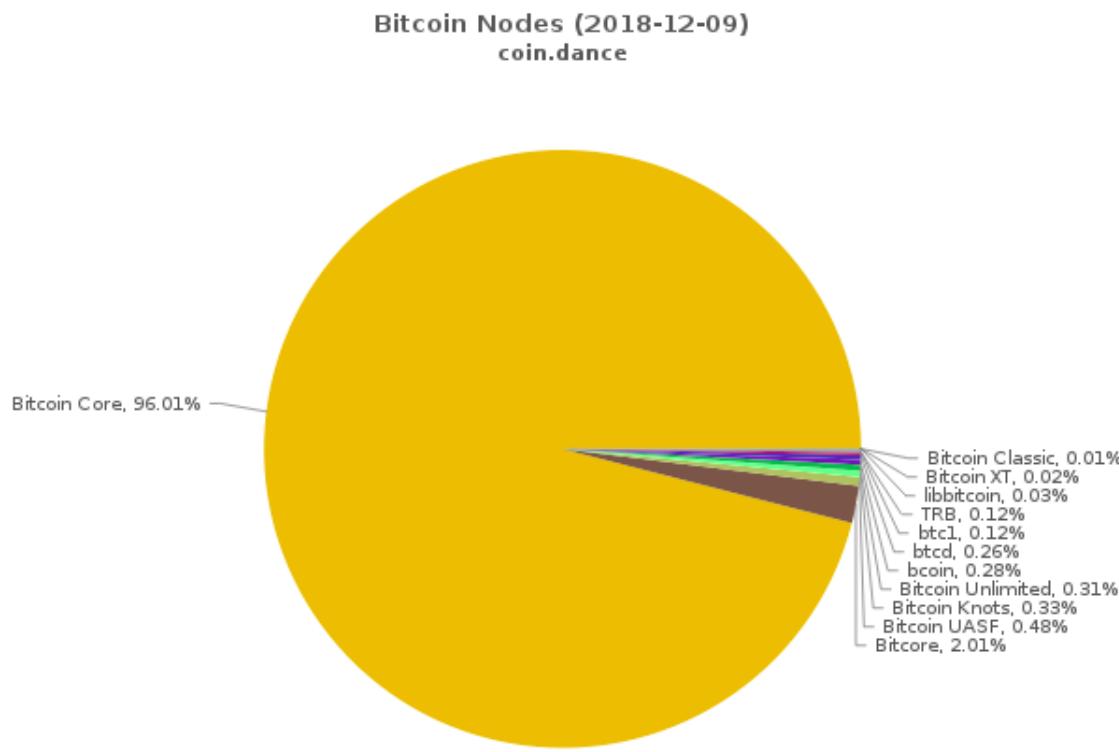
"The test is the test of the software, but what's the test of the test? The software. To test the test, you must break the software."—Greg Maxwell

Free Market Competition

BitMEX wrote a great article about the ecosystem of Bitcoin implementations. There are over a dozen different Bitcoin compatible implementations, and even more "competing network" implementations. This is the freedom of open source—anyone who is dissatisfied with the efforts of the Bitcoin Core project is free to start their own project. They can do so from scratch or they can fork the Core software.

[**Competing with Bitcoin Core**](#) Abstract: We examine the power and dynamics of the "Bitcoin Core" software project and we draw distinctions between the...[blog.bitmex.com](#)

At time of writing, 96% of reachable Bitcoin nodes are running some version of Bitcoin Core. Why is this the case? How can Bitcoin Core have near-monopoly status over the network of nodes if the effort required to switch to another software implementation is minimal? After all, many other implementations provide RPC APIs that are compatible with, or at least highly similar to Bitcoin Core.



I believe that this is a result of Bitcoin Core being a focal point for development. It has orders of magnitude more developer time and talent backing it, which means that the code produced by the Bitcoin Core project tends to be the most performant, robust, and secure. Node operators don't want to run the second best software when it comes to managing money. Also, given that this is consensus software and the Bitcoin protocol does not—and arguably can not—have a formal specification because no one has the authority to write one, it's somewhat safer to use the focal point implementation because you're more likely to be bug-for-bug compatible with most of the rest of the network. In this sense, the code of the development focal point is the closest thing to a specification that exists.

Who Are the Core Developers?

People who are unfamiliar with the [Bitcoin Core development process](#) may look at the project from the outside and consider Core to be a monolithic entity. This is far from the case! There are frequent disagreements between Core contributors and even [the most prolific contributors](#) have written plenty of code that has never been

merged into the project. If you read the guidelines for contributing you may note that they are fairly loose—the process could be best described as “rough consensus.”

Maintainers will take into consideration if a patch is in line with the general principles of the project; meets the minimum standards for inclusion; and will judge the general consensus of contributors.

Who are the Bitcoin Core maintainers? They are contributors who have built up sufficient social capital within the project by making quality contributions over a period of time. When the existing group of maintainers believes that it would be prudent to extend the role to a contributor who has exhibited competence, reliability, and motivation in a certain area, they can grant commit access to that person's GitHub account. The lead maintainer role is for someone who has oversight over all aspects of the project and is responsible for coordinating releases. It has been voluntarily passed along over the years:

- Satoshi Nakamoto: 1/3/09 -2/23/11
- Gavin Andresen: 2/23/11 -4/7/14
- Wladimir van der Laan: 4/7/14—present

Acting as a Bitcoin Core maintainer is often referred to as janitorial work because maintainers don't actually have the power to make decisions that run contrary to the consensus of contributors or of the users. However, the role can be quite taxing due to the extra attention from the ecosystem at large. For example, Gregory Maxwell gave up his maintainer role in 2017 for personal reasons, likely due to the public pressure he experienced during the scaling debate. Wladimir wrote a thoughtful post about the stress of being a Core maintainer and why it was appropriate to remove Gavin's commit access, which upset a lot of people.

Dazed and confused, but trying to continue I'm happy with the job I'm doing, happy to work with a few very smart people on an extremely interesting project...laanwj.github.io

Similarly, when Jeff Garzik was removed from the GitHub organization, he and others were upset about it, but he had not contributed to Core in two years. Leaving his GitHub account with write access to the repository was providing no benefit to the project—it was only creating a security risk and violated the principle of least privilege to which Wladimir referred in his post.

Others may look at Core and believe it to be a technocracy or ivory tower that makes it difficult for new entrants to join. But if you speak to contributors, you'll find that's not the case. While only a dozen people have had commit access over the years, hundreds of developers have made contributions. I myself have made a few

small contributions; while I don't consider myself a "Core developer" I *technically* am one. No one can stop you from contributing!



Matt Corallo
@TheBlueMatt



Replies to @TuurDemeester

In 2011, as a high school student who didn't understand what a pointer was, the [@bitcoincoreorg](#) developer community (especially people like Greg Maxwell, [@pwuille](#), etc) worked with me to make my shitty patches worth merging and made it a great environment to learn in.

310 5:59 PM - Nov 18, 2018



41 people are talking about this



John Newbery
@jfnewbery



Replies to @TheBlueMatt and 3 others

In 2016, [@TheBlueMatt](#) organised a residency at [@ChaincodeLabs](#). I'd been reading everything about Bitcoin I could lay my hands on but hadn't dared submit a PR. Matt, Alex and Suhas were extraordinarily generous with their time in teaching us about Bitcoin and how to contribute.

115 6:35 PM - Nov 18, 2018



See John Newbery's other Tweets



Jeff Rade f'
@jeffrade



Replies to @TuurDemeester

I started making small commits to [@bitcoincoreorg](#) and was in awe of the engagement on my PRs by [@MarcoFalke](#) [@pwuille](#) [@orionwl](#) [@LukeDashjr](#) and [@jfnewbery](#) Such a welcoming project!

8 1:58 PM - Nov 19, 2018



See Jeff Rade f's other Tweets



somehow make it into Core, some developers would fork the software, remove the controversial change, and make it available for users. You could argue that this is exactly what happened when Amaury Sechet forked Bitcoin Core and removed the Segregated Witness functionality to create Bitcoin ABC. Alternatively, if Core rejects

One of the most difficult things for people to wrap their mind around seems to be that the focal point for Bitcoin development is **not** simply the structure that is defined by the Bitcoin Core GitHub account. While Bitcoin Core has some structure (it uses centralized communications channels in order to coordinate), the project itself is not subject to being controlled by any of its participants—even those who have escalated privileges on the GitHub repository. While it is *technically* possible for a maintainer-organized coup to hijack the GitHub repository, censor dissenting developers, and perhaps even maintain the brand name of "Bitcoin Core," the result would be that Bitcoin Core would stop being the development focal point. Developers who disagreed with the actions of the maintainers would simply fork the code and shift their work to a different repository over which the Bitcoin Core maintainers had no administrative privileges.

Even absent a "coup" per se, if a controversial change did

Jameson Lopp (@lopp) on Twitter: "I hold allegiance to no man, to no dev team in Bitcoin. My intention is to run the code that I judge best protects my financial sovereignty." (4:18 PM - Mar 18, 2017). 77 people are talking about this.

- Core to create Bitcoin Unlimited
- Jeff Garzik forked Core to create BTC1

Forking the code is easy. Shifting the focal point of Bitcoin development is hard—you must convince contributors that their time is better spent contributing to a different project.

It's also hard to convince many people that users do not blindly follow Bitcoin Core's changes—this may be a self reinforcing belief, because if users don't participate in the consensus process by staying aware of their options, they are ceding some of their power to developers. However, the power of the users was exercised during the UASF (User Activated Soft Fork) movement of 2017. An anonymous Bitcoin developer using the pseudonym shaolinfry proposed BIP 148, which would force miners to activate Segregated Witness functionality at a block height that would occur near August 1. However, BIP 148 proved to be too controversial to be adopted by Bitcoin Core, so shaolinfry forked Core and made "Bitcoin UASF" software available. This software implementation gained a nontrivial amount of traction and seemed to create sufficient pressure to convince miners to adopt BIP 91 to activate the fork before the BIP 148 deadline.

In my opinion the best Bitcoin Core contributors are those who practice extreme ownership. Case in point—while John Newbery did not write the code that contained this particular consensus bug, he feels responsible for not preventing it from being merged via careful review and for not finding it later while writing test cases.

proposed changes that some people want, developers can fork it and add those changes. This has happened many times, such as when:

- Mike Hearn forked Core to create Bitcoin XT
- Andrew Stone forked

 **Jameson Lopp** 
@lopp

I hold allegiance to no man, to no dev team in Bitcoin. My intention is to run the code that I judge best protects my financial sovereignty.

Heart 295 4:18 PM - Mar 18, 2017

77 people are talking about this >

We are all Satoshi.

Visualization of Bitcoin Core development

Contributing to Bitcoin Core

It can feel daunting to start contributing to Core, though there are

plenty of resources available to help aspiring developers. The guidelines for contributing [can be found here](#) though you may wish to start off with [Jimmy Song's](#) gentle introduction:

A Gentle Introduction to Bitcoin Core Development If you're a developer and you own any Bitcoin at all, contributing to Bitcoin Core can be one of the best things you... [bitcointechtalk.com](#)

Core developer [Eric Lombrozo](#) also penned a piece about understanding how changes take place within the Core repository:

The Bitcoin Core Merge Process A major point of confusion, especially among people who have not worked a lot on free open source software development... [medium.com](#)

[Alex B.](#) wrote an excellent article about the philosophy behind Bitcoin development—anyone who wants to become a serious contributor can save themselves a lot of time by reading this.

The Tao Of Bitcoin Development Over the last few years, the buzz generated by Bitcoin's scaling debate has drawn unprecedented attention towards the... [medium.com](#)

A specific example may be helpful—while writing this article I encountered difficulties while trying to run the verify-commits.py script on my machine in order to audit the integrity of the GitHub commit history. In order to save future developers from having to deal with these issues, I [opened a pull request to improve the documentation](#). As you can see from the PR history, 4 different developers chimed in with suggestions for how I could improve my pull request. This ranged from using different wiki markup to a simplified bash command to a new parameter that could be used in the verify-commits.py script. I agreed that all of the suggestions made sense, so I incorporated them into my code and pushed an updated version for my pull request. At that point, the developers who were participating in the review acknowledged that they found the PR to be acceptable, and maintainer [Marco Falke](#)

tagged it for inclusion in the 0.18 release. After several more days went by with no objections from developers, the code was merged into Core by maintainer Samuel Dobson.

Who Controls Bitcoin?

As I've argued extensively over the years, it's practically impossible to fully comprehend Bitcoin as a system. The definition (control) of Bitcoin the protocol is like the definition of a language. 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. No one is forced to agree with the definition of a given word in a dictionary, neither are they forced to agree with code in a given Bitcoin implementation by running it.

Languages are not governed by democracy and neither is Bitcoin; while you may hear people make references to miners, nodes, developers, or users "voting" there is no such mechanism that can enable a majority vote of any kind to coerce a minority of dissenters into accepting changes with which they disagree. Bitcoin is anarchy—without rulers, but not without rules. The rules are defined and enforced by individual participants on the network .

While changes to the Bitcoin protocol itself are usually made via the Bitcoin Improvement Proposal process, even this is only a recommended best practice and no one can be forced to follow it. It is merely a more formalized way of trying to guide a change through a process of peer review and consensus building.

As difficult as this is to explain and understand, it is a crucial aspect to Bitcoin's antifragility—if there was a single point of control, it would also be a single point of failure that would be exploited by powerful entities that are threatened by Bitcoin's success. Ultimately, each node operator governs themselves by ensuring that no one else on the network is breaking the rules to which they agree. This security model is the foundation for Bitcoin's bottom-up governance.

How self governance results in emergent consensus.

No one controls Bitcoin.

No one controls the focal point for Bitcoin development.

Thanks to John Newbery.

Bitcoin Data Science (Pt. 3): Dust & Thermodynamics

By Dhruv Bansal

Posted December 18, 2018

This is part 3 of a series

- Bitcoin Data Science (Pt. 1): HODL Waves
 - Bitcoin Data Science (Pt. 2): The Geology of Lost Coins
 - Bitcoin Data Science (Pt. 3): Dust & Thermodynamics
-

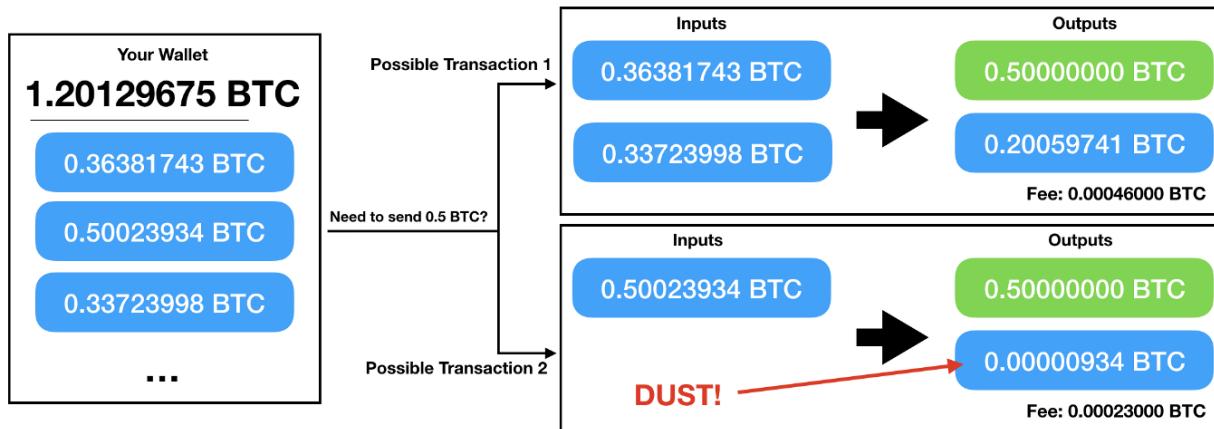
tl;dr: We examine the history and future of *dust*: containers (UTXOs) of bitcoin that cost more to spend in fees than they hold.

The amount of dust in the blockchain is determined by the current UTXO set and transaction fee market. At peak fees (~ December 2017), between 25–50% of the UTXOs in the Bitcoin blockchain could have been called dust! At the same time, the amount of BTC contained in these dusty UTXOs was small: only a few tens of millions of dollars. So, depending on how you measure it, dust is either a huge problem or a trivial one. Either way, we discuss possible solutions for minimizing new dust and cleaning up existing dust.

Proof-of-work strongly anchors bitcoin in the physical world and makes it subject to the laws of thermodynamics. **Energy expended by miners secures the blockchain, but this useful work is accompanied by an increase in entropy and the production of waste heat.** If the Bitcoin blockchain were an engine, dusty UTXOs would be a part of the waste heat it exhausts. As no engine is perfectly efficient, Bitcoin will never stop making dust.

What is dust and where does it come from?

Bitcoin uses an accounting structure known as the Unspent Transaction Output or UTXO. The outputs of any Bitcoin transaction are new UTXOs and the inputs are existing UTXOs which are fully consumed by that transaction. On the blockchain, BTC is always “stored” in such UTXOs. See the previous post in this series on HODL Waves to learn more about Bitcoin’s UTXO distribution over time.



This diagram shows two possible ways a wallet might construct a transaction sending 0.5 BTC. The first transaction consumes two UTXOs and so costs more in fees. The second transaction only consumes one UTXO so is cheaper but creates a very low-balance change output. Wallet software must balance these trade-offs today with imperfect knowledge of how the fee market will change in the future. This is a difficult problem.

When a wallet constructs a transaction it must decide which UTXOs to consume as inputs. This may sound simple, but it's really a difficult optimization problem.

Jameson Lopp defines three simultaneous and conflicting goals wallet software authors must pursue:

1. Support high transaction volume by keeping many UTXOs available in a wallet.
2. Preserve privacy by being non-deterministic and masking which outputs are change.
3. Minimize transaction fees, both now and later.

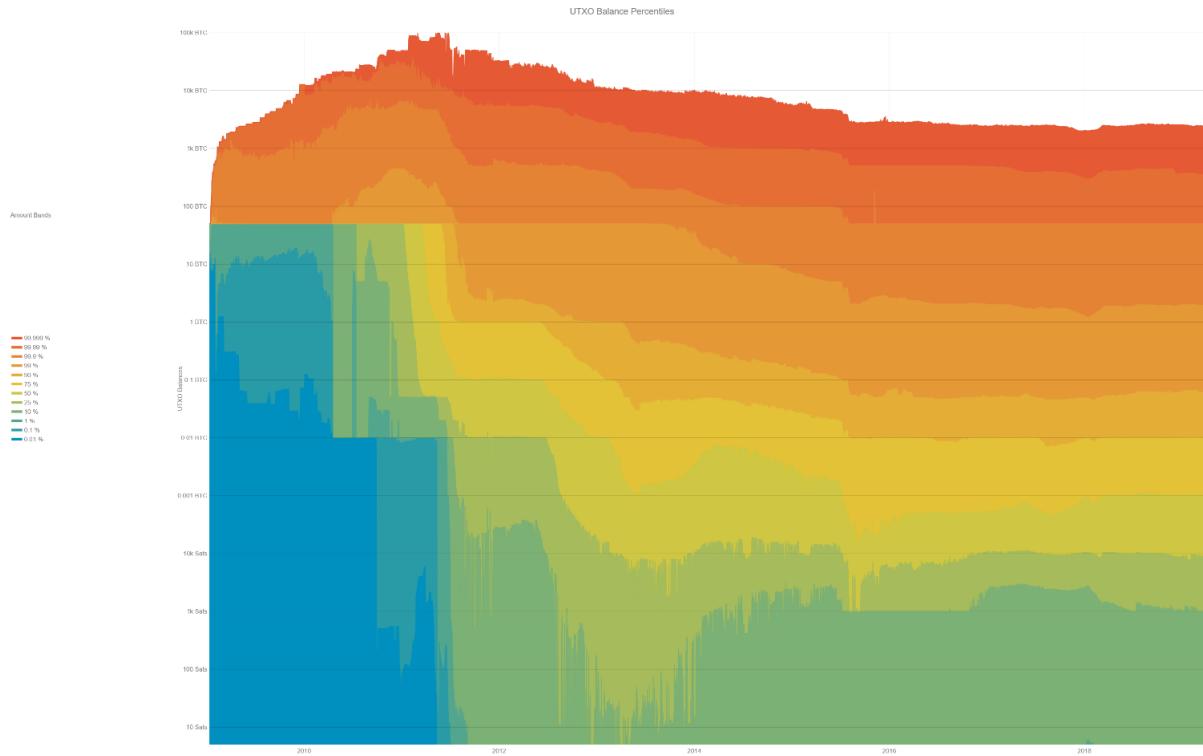
It's clear that there is no "one size fits all" solution to this problem, and in fact the three broad optimization goals outlined above tend to be in direct opposition.— Jameson Lopp

Furthermore, wallet software is often generic, meant to be shared by many different types of users. Wallet authors do not know what future transactions a given user plans on making, nor how the market for transaction fees will develop.

This means that wallets can't help but sometimes create low-balance, dusty UTXOs. UTXO management in wallets is a difficult optimization problem with no globally optimal solution for all users. This is the ultimate origin of dust.

What makes a UTXO dust?

Intuitively, UTXOs with low balances are likely to be dust. The following plot shows the distribution of UTXO balances over time:



A plot of the distribution of UTXO balances over time. Cooler colors (blues and greens) represent low-balance UTXOs and warmer colors (oranges and reds) high-balance UTXOs. The percentiles we've chosen to plot highlight the lower and upper ends of the distribution. The range of UTXO balances is enormous: there are UTXOs at the upper end of the distribution containing thousands of BTC and some at the lower end containing fewer than 100 Satoshis (11-12 orders of magnitude!). [\[Direct Link\]](#)

The plot does confirm that there are a good number of low-balance UTXOs, but can we define which of these low-balance UTXOs are dust more precisely?

Spending a UTXO in a transaction requires referring to that UTXO (by providing the ID of the transaction that created it as well as the order in which it appeared as an output in that transaction) as well as signing it with the required key(s). All of this takes a certain number of bytes to express, and miners must be compensated for bytes with transaction fees.

A transaction debits its transaction fees from its input UTXOs. This is usually not a problem as transaction fees are typically small compared to the sum of balances of all UTXOs they are consuming. But if a UTXO has a very low balance, or if transaction fees are very high, or the UTXO requires a very large number of bytes to

spend, it is possible that a resulting output UTXO may cost more to spend than it contains.

We define the **value density** of a UTXO as its balance divided by the number of bytes required to spend it.

The value density of a UTXO measures how much BTC it contains per byte required to spend it.

With this definition, classifying a UTXO as **dust** requires comparing two things:

- the lowest transaction fee currently being accepted by miners
- the value density of the UTXO

Both quantities have units of Satoshi/byte, so they can be directly compared: if the value density of a UTXO is less than the lowest transaction fee being currently accepted by miners, that UTXO is currently dust. UTXOs can drop below, and later rise above, a “dust line” over time as the (often volatile) transaction fee market changes.

How many bytes does it take to spend a UTXO?

Classifying a UTXO as dust requires knowing how many bytes are required to spend it, but this number is not really well-defined: the number of bytes required to spend a UTXO on average decreases the more UTXOs are being spent in a single transaction, because they can all share header or segwit information.

Regardless, we can at least make an arbitrary choice and ask for the number of bytes required to spend a UTXO assuming it is the single input in a transaction. The answer will depend on the type of the UTXO address. The following table summarizes this relationship:

UTXO type	Fixed fields	scriptSig. len.	scriptSig / redeemScript			Total size
			sig size	pk size	push data	
P2PK	40	1	71	-	1	113
P2PKH	40	1	71	33 – 65	2	147 – 179
P2MS	40	1 – 2	71 * m ($m \in [1, 20]$)	-	$m + 1$	$42 + 1/2 + 72 * m$
P2SH	40	1 – var	var	var	var	41 – var
P2WPKH	40	1	71	33	2	68
P2WSH	40	1	var	var	var	41 – 10041

Relationship between address type and the number of bytes required to spend a UTXO at that address. Copied from Table 3 of Pérez-Solà, Delgado-Segura, Navarro-Arribas,

Herrera-Joancomart. "Another coin bites the dust: An analysis of dust in UTXO based cryptocurrencies" (2018) [Direct Link]

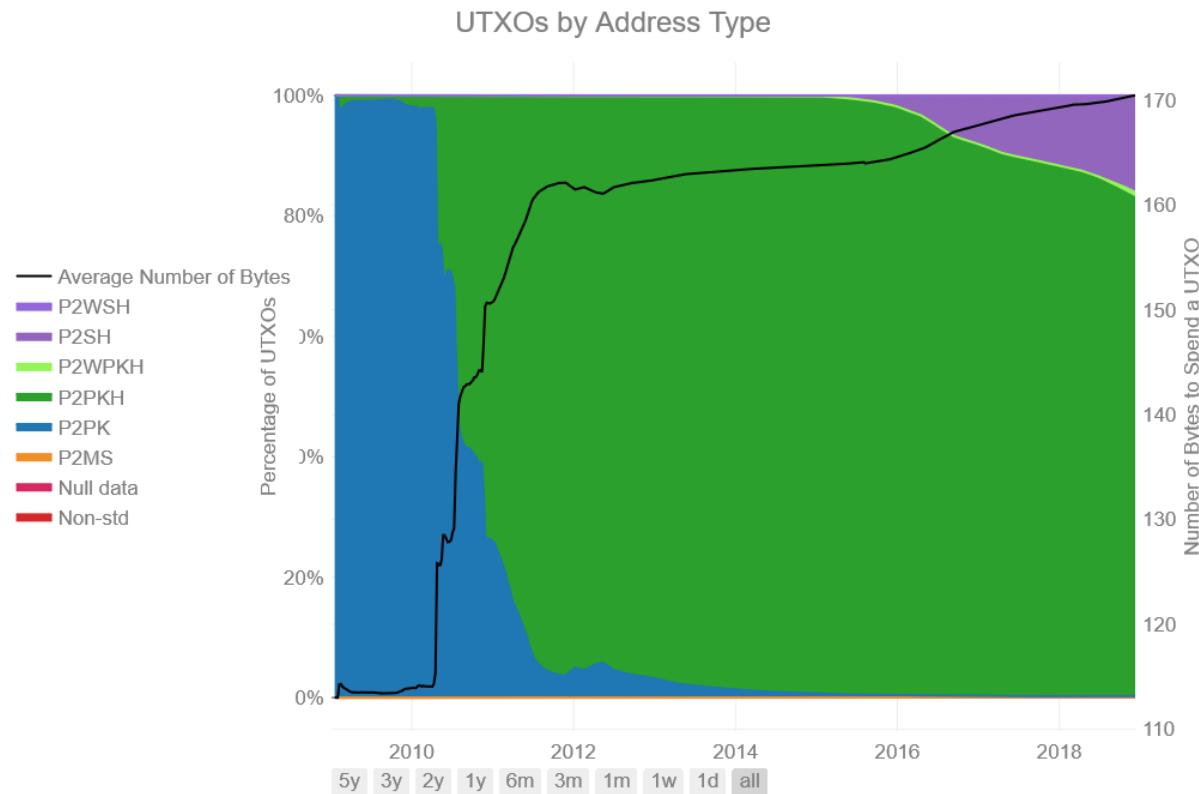
The table above has definite sizes for “simple” address types such as P2PK and P2PKH. But for P2SH addresses in particular, it’s not possible to *a priori* calculate how many bytes are required to spend a UTXO from that address. Only *a posteriori*, once the redeem script for that address has been revealed in a transaction, can it be known how many bytes it takes to spend from that address.

Nonetheless, most P2SH addresses are multisig addresses which have a predictable structure (once they are known to be multisig). And, we can extrapolate from the spends in blockchain history for many P2SH addresses:

Script Type	Estimation method	Bitcoin	Estimate of the number of bytes required to spend a UTXO from each of the given address types based on historical data. Copied from Table 6 of Pérez-Solà,
P2PKH	Block height average	[148, 180]	
P2SH	Absolute average	210.93	
Non-std	Absolute average	1.04	
P2WSH	Absolute average	251.5	

Delgado-Segura, Navarro-Arribas, Herrera-Joancomart. "Another coin bites the dust: An analysis of dust in UTXO based cryptocurrencies" (2018) [Direct Link]

Given the distribution of UTXOs among address types, we could use the estimates in the above tables to calculate the average number of bytes required to spend a UTXO at any time. The following plot summarizes this data:



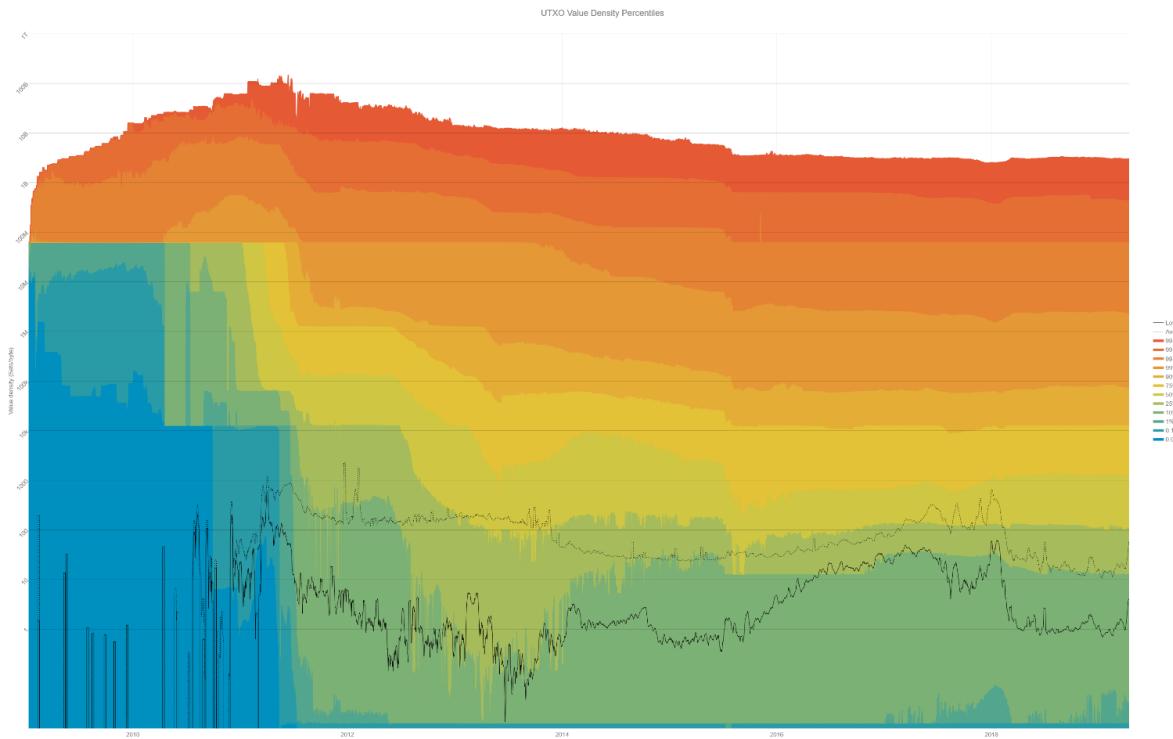
A plot of the distribution of Bitcoin's UTXO set over address types through history. The black line shows the best estimate for the number of bytes required to spend the average UTXO at that time. The dominance of addresses has shifted from P2PK to mostly P2PKH and P2SH today. [\[Direct Link\]](#)

From the plot above, we make an estimate of **172 bytes to spend the average UTXO.**

Note: By construction, this figure is an overestimate. Not only was the average number of bytes required to spend a UTXO lower than 172 bytes for most of Bitcoin's history, but smart transaction batching could lower this estimate significantly.

How much dust is there?

From the UTXO set at any block in Bitcoin's history, along with the estimate of 172 bytes to spend a UTXO, we can construct the UTXO value density distribution by dividing each UTXO's balance by the number of bytes required to spend it:



The colored bands show the value density at each percentile indicated in the legend. The dashed black line shows the average fee over time and the solid black line the lowest fee. UTXOs with value densities lower than the lowest fee cannot be spent, and those lower than the average fee are more difficult to spend. The plot assumes an average number of 172 bytes required to spend any given UTXO. [[Direct Link](#)]

This plot is very similar to the previous plot of the UTXO balance distribution—it's just rescaled by the number of bytes required to spend each UTXO (172). The units of this new distribution are Satoshi/byte, so we can directly compare it to the fee market at that block (black lines), something we couldn't do with UTXO balances alone.

What does this plot show?

There's a lot of dust!

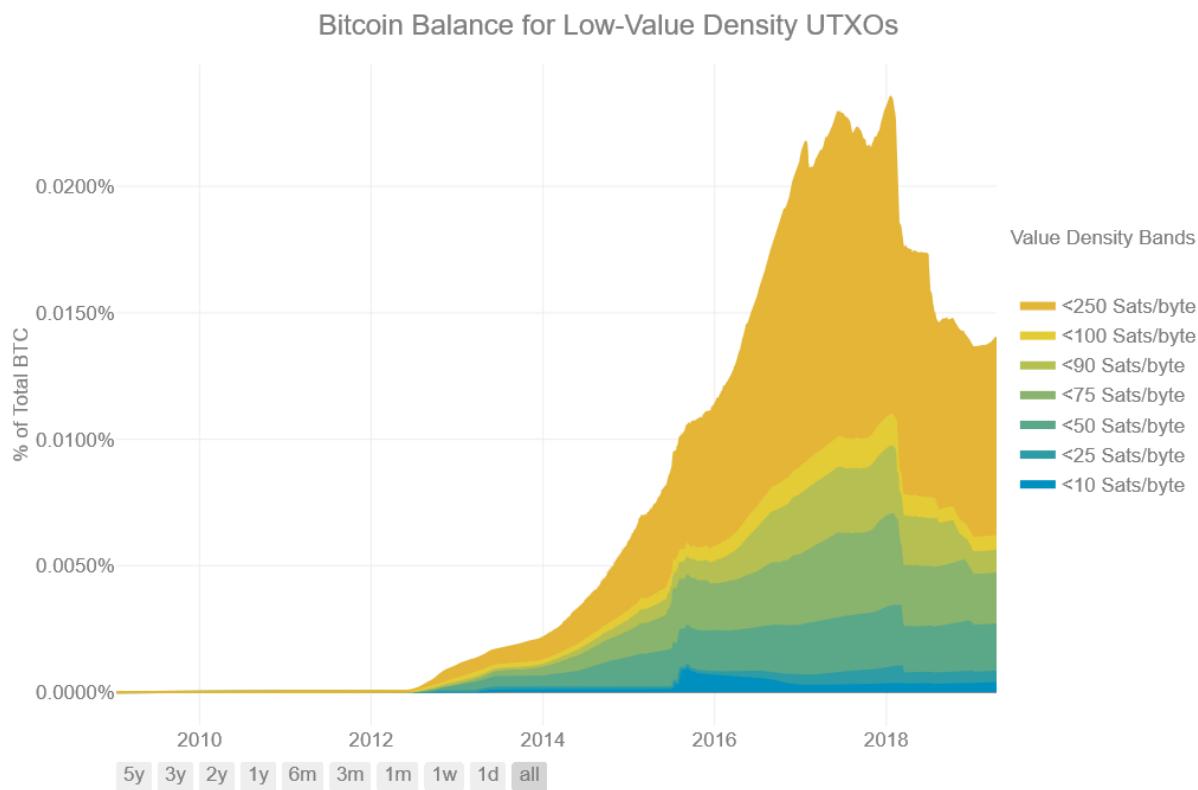
During the high-fees market of late 2017, 15–20% of all UTXOs had value densities below the lowest fee of 50–60 Satoshi/byte, making them almost impossible to spend. **40–50%** of all UTXOs had value densities below the average fee of 600–700 Satoshi/byte, making them harder to spend. This is a lot of dust!

The fee market dramatically cooled off through 2018. Today, **10–15%** of UTXOs still have value densities below the average fees of 20–30 Satoshi/byte, and 3–5% of

UTXOs have value densities below the lowest fees of 1–2 Satoshi/byte. There's much less dust, but it's still a lot.

All that dust isn't worth much!

Let's take a different perspective: a lot of the UTXOs *by count* may be dust, but how much bitcoin in total do these dusty UTXOs contain? Even though there are a lot of them, by definition they have low balances, so maybe in aggregate they don't add up to much. The plot below shows the fraction of bitcoin contained in low-value-density UTXOs:



The colored bands show the fraction of BTC held by UTXOs of the given value density. Since the bulk of BTC is contained by high-value-density UTXOs, only the bands for low-value-density UTXOs (those likely to be dust) are shown. Zoom in on the last few months to see the recent decrease in low-value-density UTXOs. The plot assumes an average of 172 bytes required to spend any given UTXO. [Direct Link]

While there are *many* UTXOs which have low value densities, the plot above shows that the aggregate BTC held in dusty UTXOs is *extremely small*. Only 0.01–0.02% of BTC by value was dust, even at peak fees. At the then-market cap of ~ \$225B, this amounted to **\$25–50M of dust**.

The average fee today is much lower than it was in late 2017. Only 0.0005% of BTC is dust at today's fees. And at today's much lower market cap of ~ \$65B, this represents **only \$300k** of dust!

The value trapped as BTC dust has shrunk from as much as \$50M in late 2017 to only \$300k today.

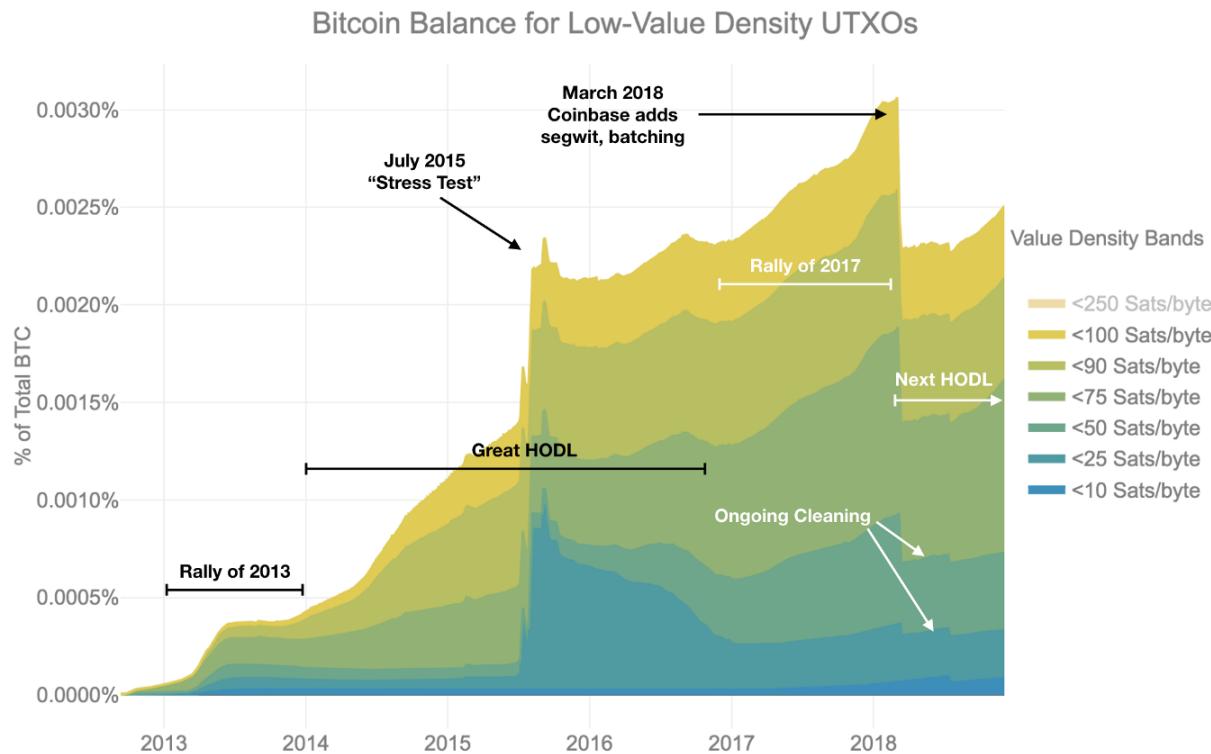
Note: These figures are over-estimates. Smart transaction batching could reduce the average number of bytes required to spend a UTXO and therefore reduce our estimates above of both the number and value of dust UTXOs.

Can we reduce dust?

Bitcoin is a leaderless system. This makes it difficult to engineer top-down approaches to eliminate existing dust and reduce future dust production. We must instead rely upon incentives for users, miners, and businesses in the space. Do such incentives exist?

Exchanges & Other Businesses

Yes, they do. While the collapsing price and fee market are chiefly responsible for the reduction in the amount of dust, in 2018 high-volume businesses such as exchanges, most notably Coinbase, instituted active dust reduction measures. The plot below of balances contained by low-value density UTXOs directly shows the impact of these active measures:



An annotated version of the plot of the fraction of BTC held by UTXOs of the given value density. The market as a whole acts to increase the amount of dust, whether slowly (HODLs) or quickly (rallies). Single actors can dramatically increase ("stress test" in 2015) or decrease (Coinbase in 2018) the amount of dust. But dust production never stops; note the recent increase and ongoing cleaning.

Businesses such as Coinbase had been creating a lot of dust and were inefficient in their usage of block space because they didn't sufficiently batch customer transactions. Due to the popularity of major exchanges such as Coinbase during the rally of 2017, this behavior affected the rest of the Bitcoin network, and many rightly complained.

When fee markets pulled back in early 2018, Coinbase had both the incentive and the ability to reduce their existing dust footprint and their future production of dust. Batching transactions saves high-volume businesses such as Coinbase fees but also reduces their dust production. Antoine Le Calvez's excellent When the Bitcoin dust settles analyzes this "UTXO consolidation" period, a **spring cleaning** of the UTXO set.

Do other constituencies in the Bitcoin ecosystem have the same combination of incentive and ability to reduce dust?

Users

Users are not directly affected by dust. They may create dust in aggregate due to inefficient wallet software they use, but few individual Bitcoin users have created much dust.

Users don't like high fees, but dust doesn't directly affect the fee market. Inefficient UTXO management which creates dust but also results in more, small transactions is a bigger cause of increasing fees. Users therefore only have a modest incentive to encourage dust reduction.

Even if they lack the incentive, do users have the *ability* to limit dust? After all, users have a lot of power in cryptocurrencies, as the UASF movement of 2017 proved. But dust is a shared problem, a tragedy of the commons, and so requires some coordinated solution. Users will need help from developers and/or exchanges and miners to clear any dust they own.

Individual users may be willing to "donate" their dust, and Bitcoin does provide mechanisms (e.g. ALL|ANYONECANPAY or NONE|ANYONECANPAY type signatures) for users to donate their dust. If wallets supported it, a socially-coordinated, **public spring cleaning** could be an interesting way to crowd-source funds for various user-chosen charities or projects benefiting the Bitcoin ecosystem.

Miners

Most miners ignore dust.

Miners in pools are just paid to hash; pool operators need to manage the UTXO set and deal with any bloat it contains, but they are also free to simply drop low value-density, dusty UTXOs from their mempools. No users are likely to spend them anyway! This would create an opportunity for scavenger-pools to pick up and attempt to mine these dust UTXOs, but this still requires users to act to spend them. Users may not notice or care.

Standalone miners or pool operators who do care about dust may choose to schedule a **fee holiday**—a time period where these miners will purposely allow zero-fee transactions which spend (only) low-value-density UTXOs, perhaps done during a spring cleaning. This will allow users to clean up their wallets while helping miners and node-operators to decrease the memory footprint of their UTXO set by a significant amount.

It's possible that proposals such as BetterHash, which distribute the ability to choose transactions, might encourage more individual miners to leave traditional mining pools (where the pool operators determine the blocks to be mined) and to construct their own blocks. They might, then, have to deal with/care more about dust.

Miners could theoretically also refuse to mine transactions which create dusty UTXOs. But would they really be willing to sacrifice fee income in the short-term to prevent creating dust in the long-term? Given that pools dominate mining and that these pools don't particularly care about dust, it seems unlikely.

Full-Node Operators

Full-node operators—those who backup the blockchain, relay, and verify transactions but don't mine—also have some power over dust creation. The `minRelayTxFee` parameter in the `bitcoind` software allows node operators to set a minimum value density below which they will ignore/drop UTXOs (and the transactions creating them). To an extent, this setting already prevents the creation of extremely low-value density UTXOs—there would probably be more dust today if this setting had never been implemented.

But few node operators tune their configuration settings to this level of detail. Developers, because they choose the default settings that come with the `bitcoind` software, may have a lot more influence over how full nodes will operate in the wild.

Developers

In many ways, developers have the most power to limit dust production.

Developers write and document wallet software. Their trade-offs (and failures) in the face of a difficult optimization problem are the root cause of dust. New strategies and best practices, as they spread from wallet to wallet, driven by the demands of users, are the best way to decrease future dust production.

Developers define default node settings, which percolate through the network of full-node operators, miners, exchanges, and other businesses. This provides a sort of herd immunity against dust, filtering out dusty transactions from malicious or inefficient wallets.

Through grassroots campaigns (just like the UASF) developers can work directly with users and miners to build the social software necessary to schedule and operate spring cleanings and fee holidays.

By building second layers such as the Lightning Network, developers can even hope to transcend the problem of dust altogether.

Dust is Inevitable

But no constituency or collaboration can hope to eliminate dust production altogether. Despite the increasing awareness of dust during 2017 and the attempts to clean it in March 2018, dust keeps being produced:

- UTXOs with value-density <50 Satoshi/byte display a sawtooth curve of constant production followed by quick pullbacks: someone is actively making dust—but at least they're cleaning up after themselves.
- There's also already 10% more UTXOs (in dollar terms) with value-density <100 Satoshi/byte—these UTXOs aren't dust today, but will turn to dust rapidly if the fee market rises again as it did in 2017.

Dust production is an inherent **inefficiency** of Bitcoin.

Does Dust Only Affect Bitcoin?

Not all blockchains use a UTXO model for transactions. Ethereum, for example, uses an account model.

- ETH deposited into an address from different transactions is commingled.
- Transaction fees are paid by the address broadcasting the transaction, not the address from which ETH is being transferred.

Both of these differences greatly reduce dust production but they don't eliminate it. Ethereum developers also worry about dust and the bloating it causes in the Ethereum blockchain.

The production of dust, defined more generically as tokens which are uneconomical to spend, seems to be a common inefficiency across blockchains.

Thermodynamics of Blockchains?

The difference between a dusty or a normal UTXO is one of utility. A Satoshi held in a dusty UTXO is less useful than the same Satoshi held in a normal UTXO. But they're otherwise identical on the blockchain.

The hashpower wagered by miners to secure the blockchain protects dusty UTXOs just as much as it protects more useful ones. This makes Satoshis held in dusty UTXOs seem even more useless, a literal waste of energy.

"Wasting energy" can be a sensitive issue for some in regards to Bitcoin. Some people already bemoan the energy used by proof-of-work to secure Bitcoin's transactions. How much more strenuous would their objections be if they knew that large amounts of what Bitcoin secures won't ever be used?

What is the energy efficiency of Bitcoin's security?

Is there a concept of an **energy efficiency** for Bitcoin? The efficiency with which it uses hashpower to protect *useful* economic assets? One can trivially define an energy efficiency for a Bitcoin miner by treating it like a space heater—but is there a more interesting, blockchain-level definition of the energy efficiency for the whole Bitcoin network? A definition which recognizes that Bitcoin's efficiency is less than it might otherwise be because of the presence of dust?

Physics & Economics

Questions about energy efficiency can be stated in terms of thermodynamics and, thus, answered using the tools of physics.

In recent decades there have been many attempts by physicists to use their tools to model economic systems. Sometimes these attempts are beautiful in their simplicity and staggering in scope of their application: billions of dollars are managed by models derived from (or similar to) the Black-Scholes equation, which calculates option prices by analogy to the diffusion of heat through a physical substance.

Other attempts to integrate these fields (“econophysics”) feel like strange, isolated chimeras, rejected by both their parent disciplines.

Are blockchains an amenable subject for the quantitative analyses and theoretical models of physicists? Consider:

- Bitcoin, while still small in market cap (and dwindling!), now has 10 years of history and is already large enough to display interesting patterns across many magnitudes of users, investment, price, volume, and value.
- Blockchains are also distributed ledgers that record their data pseudo-anonymously, but with sufficient structure to analyze large-scale behavior in precise detail (see our HODL waves post).
- Most interestingly, by using large amounts of energy, Bitcoin becomes anchored in the physical world. This provides handholds for physicists to think about the thermodynamics of blockchains.

Blockchains are an unprecedented opportunity for combining insights from economics and physics.

Blockchain as Heat Engine

The combination of these properties suggests that we may want to take the casual statement “dusty UTXOs are a waste of energy” more seriously—indeed, more *literally*: UTXOs are a “waste” of energy because they aren’t doing any useful “work” for anyone. This lowers the efficiency we seek to measure.

Physicists defined a simple framework for understanding how useful heat, work, and waste (entropy) are related to efficiency in mechanical engines: the classical theory of thermodynamics.

$$\Delta Q = W + \Delta U - T\Delta S$$

Thermodynamic equations like this one relate the input energy and work done by an engine to changes in its internal energy and the amount of entropy it produces. This particular equation is merely suggestive; it's not clear how to even define some of these terms for blockchains.

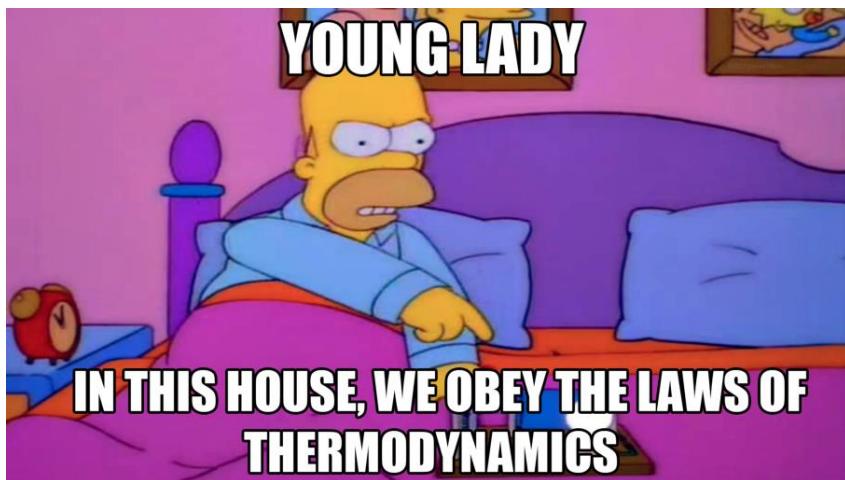
No classical engine is perfect; the extraction of useful work is always accompanied by an increase in entropy, usually manifested as waste heat in the system: a Joule of energy distributed among the molecules of air and fuel in the reaction chamber is more useful than the same Joule of energy present as random vibrations among molecules in the hot exhaust of the engine. An engine's efficiency is the degree to which an engine avoids producing waste heat in favor of useful mechanical work.

Dusty UTXOs aren't useful, but they are being secured anyway, just as waste heat in the exhaust of the engine isn't useful but produced anyway. And just as engineers have designed clever systems to avoid the production of waste heat and to shed it quickly, blockchain engineers are developing smarter wallet software, and blockchain companies are "cooling off" their own dust in an effort to increase the efficiency of the chain (in particular, cooling UTXOs is done in order of their "grain-size"—businesses clean higher-value density dust before lower-value density, as shown by [Antoine Le Calvez](#) in [When the Bitcoin dust settles](#)).

Making the analogy between dust and waste heat more precise is challenging. The same thermodynamic laws governing engines apply to any system—including a proof-of-work based blockchain. The difficulty is in applying their definitions. What is "work" in the context a bitcoin transaction? How does one measure a blockchain's "internal energy"? Is Bitcoin in equilibrium? **Treating the system as just a bunch of computers making physical waste heat is true, but uninteresting and overly reductive. Is there a level of abstraction at which the domain data of Bitcoin (transactions, UTXOs, price, volume, fees, &c.) can be thought of as a thermodynamic system?**

If we had a better theory about the *thermodynamics of proof-of-work blockchains*, we might be able to answer such questions and define "energy efficiency" for Bitcoin along with a methodology for calculating it from real-world data on energy usage, transaction volume, UTXO creation, price data, fee markets, etc.

A thermodynamic theory of blockchains would be an advance in both economics and physics. Answering the question, “Where does the energy miners input into hashing Bitcoin go?” in a way that helps us understand the economics of Bitcoin using the language of thermodynamics could be a very powerful new framework for understanding the world.



Left: [\[Source\]](#)

This post is the third in a series using data science to tell stories about Bitcoin. It analyzes how much “dust”—difficult to spend UTXOs—exists in Bitcoin’s blockchain.

You might also enjoy

- [Part 1](#): In which we describe market cycles with HODL waves.
- [Part 2](#): In which we estimate how much Bitcoin is lost.

The Lightning Network

Evolving Bitcoin into a layered system

By [Jordan Clifford](#)

Posted December 19, 2018



photo credit: [John Fowler](#)

In this post, we'll explore the Lightning Network (LN): what it is, how it works, what makes it special, what tradeoffs it makes and some of the weaknesses it has. At a high level, the Lightning Network utilizes smart contract functionality within Bitcoin allowing users to temporarily keep the state of the books locally, rather than having each update happen on the global blockchain.

The ideas within the Lightning Network are not new. Satoshi himself envisioned using [payment channels](#) to batch transactions off chain before writing a final settlement transaction to the chain. In 2014, Peter Todd, a famous Bitcoin developer and blockchain consultant, [discussed](#) how payment channels could be tied together in a hub-and-spoke model.

The Lightning Network builds on this prior art, and was formally introduced in a February 2015 [white paper](#)—a collaboration of blockchain researchers [Joseph Poon](#) and [Tadge Dryja](#). The vision of the Lightning Network is a mighty one. The goal is to create an overlay network on the Bitcoin protocol allowing arbitrary parties to route payments to each other without writing to the blockchain.

Background

Bitcoin was created to be a peer-to-peer cash system. One tenet dear to the Bitcoin community is the ideal that anyone on the planet is able to validate the state of the chain. Many within Bitcoin feel that to fulfill its promise of no trusted third parties, verifying the current state of the ledger must be achievable with modest bandwidth and typical consumer grade hardware. These beliefs have halted momentum

towards increasing the block size, leaving developers to pursue alternative strategies for scaling the system.

The Lightning Network was pitched as a viable alternative to increasing the block size via a hard fork increase of the block size, which Bitcoin's developers felt too controversial and difficult to coordinate. However, in order to have a fully functional Lightning Network, a malleability fix was a necessary prerequisite. Transaction malleability means that transactions can be altered before they are included in a block, creating a near-identical transaction, but with a different transaction id. A malleability fix prevents transactions from being altered.

A change called Segregated Witness was introduced in late 2015 that served as a malleability fix and included other benefits. The developer community liked that it was a soft fork rather than a hard fork, since soft forks are easier to coordinate as clients can update at their own leisure. The promise of the Lightning Network is undoubtedly one of the deciding factors in this change getting adopted in August of 2017.

Building Blocks

One of the best aspects of the Lightning Network is that it works using only existing functionality of Bitcoin. In fact, from the perspective of the Bitcoin network, LN transactions appear as ordinary transactions. Bitcoin doesn't need to know which transactions are part of the Lightning Network.

Transactions

Bitcoin operates on a model called the unspent transaction output (UTXO) model. A UTXO belongs to anyone who can meet the criteria assigned to that UTXO. The typical criteria is codified as an address, and is satisfied by creating a signature with a specific private key that created the address.

A transaction in Bitcoin results in the movement of bitcoin from one or more UTXO inputs into newly created UTXO outputs.

Possession of a private key is the most common spending criteria for a UTXO, but many other criteria are available as well such as the following:

MultiSig

A multisig UTXO requires signatures from multiple keys, ensuring that multiple parties agree to the transaction. The Lightning Network makes heavy use of multisig addresses. Parties choosing to connect to each other do by depositing into a multisig address that holds funds that are spendable only upon consent of both parties.

Hash Lock

It is possible to add rather interesting spending criteria to a UTXO. One such criteria built into Bitcoin is the ability to require a solution to a cryptographic puzzle be submitted when spending. The bitcoin is locked until the puzzle is solved. A hash lock is exactly such a lock. Hash locked bitcoin require the recipient to publish data that results in a specific hash.

A hash function takes an arbitrary amount of data and condenses it down into a fixed length string. A tiny change in the original data makes the hash unrecognizably different. The fact that a hash function is incredibly difficult to reverse is what makes Bitcoin secure.

The data that results in a specified hash is called a pre-image. The pre-image is chosen by the intended recipient, and they provide the hash to the sender. We'll see later that it's exactly this hash lock that guarantees funds are not intercepted when being sent over the Lightning Network.

Time Lock

A time lock is a useful building block for smart contracts. As it sounds, a time lock prevents bitcoin from being spent before a certain time. The time can be absolute (specified as a block height), or relative to the publishing of the transaction.

As we'll see these delays are very important for allowing parties the needed time to keep each other honest. Without time locks, it would be possible for a party to publish an out of date closing transaction and instantly cash out more than they are entitled to.

Payment Channels

Payment channels were conceived by Satoshi Nakamoto. They are a clever way of allowing users to keep a running tally between themselves, without broadcasting each update to the world. Fundamentally, a payment channel requires two transactions, a funding transaction and a closing transaction.

A funding transaction sets up the channel by depositing bitcoin into a multisig address. From there, the parties can update the balance as often as they wish. They exchange enough information when transacting so that each has a copy of the closing transaction. They won't typically publish the closing transaction. Only once they are done transacting with each other, will they feel compelled to close the channel with a closing transaction.

Note that payment channels only really make sense if you expect to make multiple transactions in the interim.

One way Payment Channels

The simple case for a payment channel is when all payments happen in one direction. If Alice expects to be doing a lot of business with Bob, then it can make sense for Alice to open a one-way payment channel to Bob. Alice funds the channel herself. The money goes into a multisig address requiring both Alice and Bob's consent to spend it. As she wants to spend money with Bob, she signs a closing transaction updating the balance. When Bob is ready to close the channel, he signs his half of the closing transaction and broadcasts it.

What makes this efficient is that Bob typically does not close the channel until he doesn't expect any more business coming from Alice. Alice can make many payments for the price of two transactions being written to the chain.

In this simplified model, Alice cannot close the channel at all. In practice, there is a timeout for the channel, allowing Alice to claim her money back if Bob hasn't closed the channel within the specified window of time.

Bidirectional Payment Channels

One way payment channels can only get us so far if we want to make a massively interconnected web allowing payments between arbitrary parties. The one-way payment channels worked because the recipient can be relied on to only close the channel with the closing transaction that pays him the most. Bidirectional payment channels are quite a bit more complicated to get right.

With bidirectional channels, when the channel is funded, both parties get a copy of a commitment transaction which can close the channel. The commitment transaction has special properties which makes the setup work. For one, the commitment transactions are not the same. Alice's commitment transaction has Alice's bitcoin locked up for 1000 blocks, but Bob's bitcoin are immediately spendable. Meanwhile in Bob's commitment transaction, he has his bitcoin locked up for 1000 blocks, while Alice's can be spent immediately.

The reason for the asymmetry is to allow room for disputes. When Alice and Bob update the state of the channel with a payment in either direction, they are making an agreement to revoke old commitment transactions. In order to do so, they reveal to each other enough information to allow each to steal the counterparty's bitcoin if the counterparty were to publish an old commitment transaction.

So, the party publishing the commitment transaction has to wait 1000 blocks to spend their bitcoin. However, if the commitment transaction is stale, the other party can take all of the bitcoin. This backdoor is installed via a key that changes with each transaction called the revocation key. When a commitment transaction is revoked, the revocation key becomes known to the other party. If a stale transaction is

published, the counterparty can withdraw the entire contents of the channel, via a penalty transaction. The possibility of a penalty transaction is key to keeping Lightning Network trustless.

Linking Payment Channels

Payment channels are only so useful if you have to open up a payment channel with every counterparty you ever plan to transact with. The Lightning Network really shines when opening channels with just a few counterparts allows you to make payments to nearly everyone on the Lightning Network.

Imagine that Alice has a payment channel to Bob, but she wants to pay Charlie. If Bob has a payment channel with Charlie, the Lightning Network gives us the tools for Alice to pay Charlie without any on-chain transactions.

The key to allowing payments that run through multiple hops is the hash lock. The ultimate recipient of a payment generates some private data, which becomes the pre-image. They hash that data and give it to the original sender. Each party in the chain of payment creates a new commitment transaction that is hash locked with the same hash. The updated closing transaction is conditional on the pre-image being revealed.

The pre-image will only be revealed by the recipient once they have received the requisite funds. Once it is revealed, all of the intermediary payments become unlocked as well since the data is now public. It is through this series of hash locks that payments can be sent trustlessly across multiple hops without fear of interception. Bob can only collect his payment from Alice if he also pays Charlie, otherwise Charlie will not reveal the pre-image.

Tradeoffs and Open Problems

The Lightning Network is very anticipated, but not without some drawbacks and open problems.

Scales transactions not users

The Lightning Network undeniably allows more transactions per second for people within the Lightning Network. Transactions can happen at blazing speed and because the intermediate state is held locally, not globally, it scales very well.

However, it should be noted that for each user entering the Lightning Network, it requires at least one transaction up front, and another down the line. More likely it will require multiple transactions since it's recommended that users open multiple channels. Therefore the Lightning Network scales up the number of transactions a

particular group can do very well, but enlarging the group is going to require more space for on-chain transactions.

Not great for some use cases

The Lightning network requires extra overhead that a normal transaction does not. If someone wants to receive a portion of their paycheck in Bitcoin and hold for an extended period of time, they may not benefit from the Lightning Network, and would be better off just receiving a standard bitcoin transaction.

The Lighting Network requires monitoring the blockchain to rebut any transactions to ensure that an old one is not used. This can be outsourced, but it still adds a bit of complexity.

Routing

In order for a payment to work over the Lightning Network, a route between the payor and payee must be found. This is really a two stage problem. First the network topology (an outline of the connections each user has) should be such that it's likely a route exists. Second, when it comes time to send a payment, the route must be identified.

One way we know that we can solve the routing problem is with a hub-and-spoke model, but this has been heavily criticized within the crypto community. The hub-and-spoke model has a small number of power users, typically companies that everyone connects to. Routes are easy to find since the hubs are very well connected, but it creates powerful intermediaries—something crypto was designed to avoid. Such a design would potentially compromise privacy and engender possible censorship.

The ideal Lightning Network is a peer-to-peer mesh network. Each user would be connected to a handful of other users, and through the "[Six Degrees of Kevin Bacon](#)" theory, it's postulated that a route can be found between arbitrary parties.

The truth is that this is still very much an active area of research. Leading the charge, BitFury, a mining hardware manufacturer, has put forth a [paper](#) outlining an algorithm called Flare.

Balancing the channels

Once a route is found between two parties, if most transactions are happening in one direction, that route may not be good for very long. The sender will deplete their balance on the outgoing channel, so it's important to keep balance in the channels by finding different routes or finding a way to push money back to the outbound channel via another route. This remains an area of open research.

Where are we?

Currently, the Lightning Network is live in beta mode, meaning it's not mature software and bugs are expected. Reflective of its still experimental nature, the Lightning Network as of 12/18/2018 has ~ 2000 active nodes each with an average of 14 channels open. The average channel capacity is approximately \$120.

Adoption so far has been minimal, given the early stages of the network. Only a few test cases have emerged so far such as [Bitrefill](#) which allows you to buy gift cards and pay bills, Blockstream's [Lightning store](#) and the now infamous graffiti wall, [Satoshi's Place](#).

Who's behind this?

The Lightning Network is built on a series of interoperability standards called the [Basis of Lightning Technology](#) (BOLTs). Three teams are building clients that all are capable of working together: [Lightning Labs](#), [Blockstream](#), and [ACINQ](#).

Lightning Labs is the de facto leader of the Lightning Network. The company was co-founded by [Elizabeth Stark](#) and [Olaoluwa Osuntokun](#) to bring this concept to a reality. Lightning Labs has built the reference client for the Lightning Network called Lightning Network Daemon (lnd) and they also maintain the network standards documents (BOLTs) repository. The lnd is written in the Go programming language.

Blockstream is involved in much of the cutting edge Bitcoin development and the Lightning Network is no exception. Blockstream's Rusty Russell has contributed heavily to the Lightning specification documents and also leads Blockstream's cLightning client development. Blockstream has positioned cLightning as the go-to client for enterprise deployments. The client is written in C and is very performant.

ACINQ is a startup based in Paris, France that is carving out its own niche within the Lightning ecosystem. Their client, [eclair](#) (French for Lightning), is written in Scala so it can run on nearly any platform. They want to build user friendly interfaces and have released an Android Lightning Network client for mobile use.

Two other clients previously under development, [Blockchain's Thunder](#) and [MIT-DCI's lit](#) are now inactive. They are not currently being updated to the latest network standards.

What's next?

The Lightning Network is promising technology, yet still in its infancy. Whether it is able to fulfill on the hype will depend on how successful bitcoin is at continuing to grab the lionshare of the demand for crypto and how well the competition is able to scale. It will also depend on how quickly the user experience can be polished. This is

a story that will unfold over the coming years, and will certainly teach us plenty of lessons in how to scale up payments.

Thank you to caleb tebbe, Justin Camarena, Linda Xie, Cyrus Younessi, and Jordan Palmer for reviewing this post.

Disclaimer: Jordan Clifford is a Managing Director of Scalar Capital Management, LLC, an investment manager focused on cryptographic and blockchain related assets. Scalar Capital holds a position in Bitcoin.

Thanks to Linda Xie, Cyrus Younessi, Jordan Palmer, and caleb tebbe.

Philosophical Teachings of Bitcoin

What I've Learned From Bitcoin: Part I

By Gigi

Posted December 21, 2018

This is part 1 of a 3 part series

- Part 1 Philosophical Teachings of Bitcoin
- Part 2 Economic Teachings of Bitcoin
- Part 3 Technological Teachings of Bitcoin



Some questions have easy answers. "What have you learned from Bitcoin?" isn't one of them. After trying to answer this question in a short tweet, and failing miserably, I realized that the amount of things I've learned is far too numerous to answer quickly, if at all. I also realized that any set of answers to this question will be different for everyone—a reflection of the very personal journey through the wonderful world of crypto. Hence, the subtitle of this series is *What I've Learned From Bitcoin*, with which I want to acknowledge the inherent personal bias of answering a question like this.

I tried to group the teachings of Bitcoin by topics, resulting in three parts:

- I: Philosophical Teachings of Bitcoin

- II:Economic Teachings of Bitcoin
- III:Technological Teachings of Bitcoin

As hinted above, attempting to answer this question fully is a fool's errand, thus my answers will always be incomplete. I would like to lessen this shortcoming by inviting you, dear reader, to share your own answers to this question:

Bitcoin is indeed a game disguised. It is akin to a trapdoor, a gateway to a different world. A world much stranger than I would have ever imagined it to be. A world which takes your assumptions and shatters them into a thousand tiny pieces, again and again. Stick around for long enough, and Bitcoin will completely change your worldview.

"After this, there is no turning back. You take the blue pill—the story ends, you wake up in your bed and believe whatever you want to believe. You take the red pill—you stay in Wonderland, and I show you how deep the rabbit hole goes."

— Morpheus ***



Lesson 1: Immutability and change

Bitcoin is inherently hard to describe. It is a *new thing*, and any attempt to draw a comparison to previous concepts—be it by calling it digital gold or the internet of money—is bound to fall short of the whole. Whatever your favorite analogy might be, two aspects of Bitcoin are absolutely essential: decentralization and immutability.

One way to think about Bitcoin is as an automated social contract. The software is just one piece of the puzzle, and hoping to change Bitcoin by changing the software is an exercise in futility. One would have to convince the rest of the network to adopt the changes, which is more a psychological effort than a software engineering one.

The following might sound absurd at first, like so many other things in this space, but I believe that it is profoundly true nonetheless: You won't change Bitcoin, but Bitcoin will change you.

"Bitcoin will change us more than we will change it." —Marty Bent

It took me a long time to realize the profundity of this. Since Bitcoin is just software and all of it is open-source, you can simply change things at will, right? Wrong. Very wrong. Unsurprisingly, Bitcoin's creator knew this all too well.

The nature of Bitcoin is such that once version 0.1 was released, the core design was set in stone for the rest of its lifetime. —Satoshi Nakamoto

Many people have attempted to change Bitcoin's nature. So far all of them have failed. While there is an endless sea of forks and altcoins, the Bitcoin network still does its thing, just as it did when the first node went online. The altcoins won't matter in the long run. The forks will eventually starve to death. Bitcoin is what matters. As long as our fundamental understanding of mathematics and/or physics doesn't change, the Bitcoin honeybadger will continue to not care.

"Bitcoin is the first example of a new form of life. It lives and breathes on the internet. It lives because it can pay people to keep it alive. [...] It can't be changed. It can't be argued with. It can't be tampered with. It can't be corrupted. It can't be stopped. [...] If nuclear war destroyed half of our planet, it would continue to live, uncorrupted." —Ralph Merkle

The heartbeat of the Bitcoin network will outlast all of ours.

Realizing the above changed me way more than the past blocks of the Bitcoin blockchain ever will. It changed my time preference, my understanding of economics, my political views, and so much more. Hell, it is even changing people's diets. If all of this sounds crazy to you, you're in good company. All of this is crazy, and yet it is happening.

Bitcoin taught me that it won't change. I will.

Lesson 2: The scarcity of scarcity

In general, the advance of technology seems to make things more abundant. More and more people are able to enjoy what previously have been luxurious goods. Soon, we will all live like kings. Most of us already do. As Peter Diamandis wrote in Abundance: "Technology is a resource-liberating mechanism. It can make the once scarce the now abundant."

Bitcoin, an advanced technology in itself, breaks this trend and creates a new commodity which is truly scarce. Some even argue that it is one of the rarest things in the universe. The supply can't be inflated, no matter how much effort one chooses to expend towards creating more.

"Only two things are genuinely scarce: time and bitcoin." —Saifedean Ammous

Paradoxically, it does so by a mechanism of copying. Transactions are broadcast, blocks are propagated, the distributed ledger is—well, you guessed it—distributed. All of these are just fancy words for copying. Heck, Bitcoin even copies itself onto as many computers as it can, by incentivizing individual people to run full nodes and mine new blocks.

All of this duplication wonderfully works together in a concerted effort to produce scarcity.

In a time of abundance, Bitcoin taught me what real scarcity is.

Lesson 3: An immaculate conception

Everyone loves a good origin story. The origin story of Bitcoin is a fascinating one, and the details of it are more important than one might think at first. Who is Satoshi Nakamoto? Was he one person or a group of people? Was he a she? Time-traveling alien, or advanced AI? Outlandish theories aside, we will probably never know. And this is important.

Satoshi chose to be anonymous. He planted the seed of Bitcoin. He stuck around for long enough to make sure the network won't die in its infancy. And then he vanished.

What might look like a weird anonymity stunt is actually crucial for a truly decentralized system. No centralized control. No centralized authority. No inventor. No-one to prosecute, torture, blackmail, or extort. An immaculate conception of technology.

"One of the greatest things that Satoshi did was disappear." —Jimmy Song

Since the birth of Bitcoin, thousands of other cryptocurrencies were created. None of these clones share its origin story. If you want to supersede Bitcoin, you will have to transcend its origin story. In a war of ideas, narratives dictate survival.

"Gold was first fashioned into jewelry and used for barter over 7,000 years ago. Gold's captivating gleam led to it being considered a gift from the gods." —Gold: The Extraordinary Metal

Like gold in ancient times, Bitcoin might be considered a gift from the gods. Unlike gold, Bitcoins origins are all too human. And this time, we know who the gods of development and maintenance are: people all over the world, anonymous or not.

Bitcoin taught me that narratives are important.

Lesson 4: The problem of identity

Nic Carter, in an homage to Thomas Nagel's treatment of the same question in regards to a bat, wrote an excellent piece which discusses the following question: What is it like to be a bitcoin? He brilliantly shows that open, public blockchains in general, and Bitcoin in particular, suffer from the same conundrum as the Ship of Theseus: which Bitcoin is the real Bitcoin?

"Consider just how little persistence Bitcoin's components have. The entire codebase has been reworked, altered, and expanded such that it barely resembles its original version. [...] The registry of who owns what, the ledger itself, is virtually the only persistent trait of the network [...] To be considered truly leaderless, you must surrender the easy solution of having an entity that can designate one chain as the legitimate one." —Nic Carter

It seems like the advancement of technology keeps forcing us to take these philosophical questions seriously. Sooner or later, self-driving cars will be faced with real-world versions of the trolley problem, forcing them to make ethical decisions about whose lives do matter and whose do not.

Cryptocurrencies, especially since the first contentious hard-fork, force us to think about and agree upon the metaphysics of identity. Interestingly, the two biggest examples we have so far have lead to two different answers. On August 1, 2017, Bitcoin split into two camps. The market decided that the unaltered chain is the original Bitcoin. One year earlier, on October 25, 2016, Ethereum split into two camps. The market decided that the *altered* chain is the original Ethereum.

If properly decentralized, the questions posed by the *Ship of Theseus* will have to be answered in perpetuity for as long as these networks of value-transfer exist.

Bitcoin taught me that decentralization contradicts identity.

Lesson 5: Replication and locality

Quantum mechanics aside, locality is a non-issue in the physical world. The question "*Where is X?*" can be answered in a meaningful way, no matter if X is a person or an object. In the digital world, the question of *where* is already a tricky one, but not impossible to answer. Where are your emails, really? A bad answer would be "the cloud", which is just someone else's computer. Still, if you wanted to track down every storage device which has your emails on it you could, in theory, locate them.

With bitcoin, the question of "where" is *really* tricky. Where, exactly, are your bitcoins?

"I opened my eyes, looked around, and asked the inevitable, the traditional, the lamentably hackneyed postoperative question: 'Where am I?' —Daniel Dennett

The problem is twofold: First, the distributed ledger is distributed by full replication, meaning the ledger is everywhere. Second, there are no bitcoins. Not only physically, but *technically*.

Bitcoin keeps track of a set of unspent transaction outputs, without ever having to refer to an entity which represents a bitcoin. The existence of a bitcoin is inferred by looking at the set of unspent transaction outputs and calling every entry with a 100 million base units a bitcoin.

"Where is it, at this moment, in transit? [...] First, there are no bitcoins. There just aren't. They don't exist. There are ledger entries in a ledger that's shared [...] They don't exist in any physical location. The ledger exists in every physical location, essentially. Geography doesn't make sense here—it is not going to help you figuring out your policy here." —Peter Van Valkenburgh

So, what do you actually own when you say "*I have a bitcoin*" if there are no bitcoins? Well, remember all these strange words which you were forced to write down by the wallet you used? Turns out these magic words are what you own: a magic spell which can be used to add some entries to the public ledger—the keys to "move" some bitcoins. This is why, for all intents and purposes, your private keys *are* your bitcoins. If you think I'm making all of this up feel free to send me your private keys.

Bitcoin taught me that locality is a tricky business.

Lesson 6: The power of free speech

Bitcoin is an idea. An idea which, in its current form, is the manifestation of a machinery purely powered by text. Every aspect of Bitcoin is text: The whitepaper is text. The software which is run by its nodes is text. The ledger is text. Transactions are text. Public and private keys are text. Every aspect of Bitcoin is text, and thus equivalent to speech.

"Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances." — First Amendment to the United States Constitution

Although the final battle of the Crypto Wars has not been fought yet, it will be very difficult to criminalize an idea, let alone an idea which is based on the exchange of text messages. Every time a government tries to outlaw text or speech, we slip down a path of absurdity which inevitably leads to abominations like illegal numbers and illegal primes.

As long as there is a part of the world where speech is free as in *freedom*, Bitcoin is unstoppable.

"There is no point in any Bitcoin transaction that Bitcoin ceases to be *text*. *It is all text*, all the time. [...] Bitcoin is **text**. Bitcoin is **speech**. It cannot be regulated in a free country like the USA with guaranteed inalienable rights and a First Amendment that explicitly excludes the act of publishing from government oversight." —Beautyon

Bitcoin taught me that in a free society, free speech and free software are unstoppable.

Lesson 7: The limits of knowledge

Getting into Bitcoin is a humbling experience. I thought that I knew things. I thought that I was educated. I thought that I knew my computer science, at the very least. I studied it for years, so I have to know everything about digital signatures, hashes, encryption, operational security, and networks, right?

Wrong.

Learning all the fundamentals which make Bitcoin work is hard. Understanding all of them deeply is borderline impossible.

"No one has found the bottom of the Bitcoin rabbit hole." —Jameson Lopp

My list of books to read keeps expanding way quicker than I could possibly read them. The list of papers and articles to read is virtually endless. There are more podcasts on all of these topics than I could ever listen to. It truly is humbling. Further, Bitcoin is evolving and it's almost impossible to stay up-to-date with the accelerating rate of innovation. The dust of the first layer hasn't even settled yet, and people have already built the second layer and are working on the third.

Bitcoin taught me that I know very little about almost anything. It taught me that this rabbit hole is bottomless.

Conclusion

Bitcoin is a child of the internet. Even though it requires computers to function efficiently, computer science is not sufficient to understand it. The implications of this new technology are far-reaching. Bitcoin is not only borderless but also boundaryless in respect to academic disciplines.

In this first part of the *Teachings of Bitcoin* I tried to outline some of the philosophical implications of this fascinating machinery. In part two I will try to discuss what Bitcoin taught me about economics. Part three will conclude this series to show what I, a technologist, have learned from the tech perspective by stumbling into Bitcoin.

As mentioned above, I think that any answer to the question “*What have you learned from Bitcoin?*” will always be incomplete. The systems are too dynamic, the space moving too fast, and the topics too numerous. Politics, game theory, monetary history, network theory, finance, cryptography, information theory, censorship, law and regulation, human organization, psychology—all these and more are areas of expertise which might help to grasp what Bitcoin is.

What have you learned from Bitcoin?

Further Reading

- [*The Bitcoin Standard: The Decentralized Alternative to Central Banking*](#) by Saifedean Ammous
- [*Abundance: The Future Is Better Than You Think*](#) by Peter Diamandis
- [*The Mind's I*](#) by Daniel Dennett and Douglas Hofstadter
- [*Money, blockchains, and social scalability*](#) by Nick Szabo
- [*Bitcoin's Existential Crisis*](#), originally published as *What is it like to be a Bitcoin?* by Nic Carter
- [*Unpacking Bitcoin's Social Contract: A framework for skeptics*](#) by Hasu
- [*Why America Can't Regulate Bitcoin*](#) by Beautyon
- [*Why Bitcoin is different*](#) by Jimmy Song
- Peter Van Valkenburg on [*Preserving the Freedom to Innovate with Public Blockchains*](#) hosted by Peter McCormack

Acknowledgments

- Thanks to [Arjun Balaji](#) for [the tweet](#) which motivated me to write this.
- Thanks to [Marty Bent](#) for providing endless food for thought and entertainment. If you are not subscribed to [Marty's Bent](#) and [Tales From The Crypt](#), you are missing out.
- Thanks to [Michael Goldstein](#) and [Pierre Rochard](#) for curating and providing the greatest Bitcoin literature via the [Nakamoto Institute](#) and the [Noded Podcast](#) which influenced my philosophical views on Bitcoin substantially.
- Thanks to [Peter McCormack](#) for his [honest tweets](#) and the [What Bitcoin Did](#) podcast, which keeps providing great insights from many areas of the space.
- Thanks to Jannik for providing feedback to early drafts of this article.
- And finally, thanks to all the bitcoin maximalists, shitcoin minimalists, shills, bots, and shitposters which reside in the beautiful garden that is crypto twitter.

Translations

- Spanish translation by [Camilo Jorajuria de León @CamiloJdL](#)
-

Bitcoin's Incentive Scheme and the Rational Individual

By Hugo Nguyen

December 24, 2018

This is Part 4 of a 5 part series

- Part 1 - The Anatomy of Proof-of-Work
- Part 2 - Bitcoin, Chance and Randomness
- Part 3 - How Cryptography Redefines Private Property
- Part 4 - Bitcoin's Incentive Scheme and the Rational Individual
- Part 5 - Bitcoin: Two Parts Math, One Part Biology

Unlike Proof-of-Work and Public-Key Cryptography, the third component of Bitcoin is not based on math, but human behavior. Specifically, Bitcoin relies on a system of financial incentives and people chasing these incentives to sustain itself.



That sounds a bit scary, and a sharp shift from the strong mathematical foundation that underlies most modern technologies, such as the computer or artificial intelligence. If we have learned anything from history, it is that humans are not always predictable. We are, after all, biological creatures made up of "wet" matter. We're not like "dry", cold-hearted machines who can calculate things accurately or consistently. We change our mind in a heartbeat. Not only that, we constantly bicker, and hardly seem to be able to agree on anything.

So **how can we create a technology out of fickle human behavior?** Bitcoin's 10-year track record is evidence that perhaps we can, and this aspect of Bitcoin is as innovative as the novel uses of Proof-of-Work and Public-Key Cryptography, which we explored in-depth in the first 3 parts of the series.

Bitcoin's incentive scheme relies on the assumption that people are *rational* actors. If people are rational, they would be incentivized to participate in mining, buying and

holding Bitcoin. The concept of rationality is incredibly important, but often taken for granted, so it's worth a background discussion.

Economic Rationality

In economics, the definition of rationality, or the *economically-rational individual*, has been a topic of great debate, and economists still disagree on the precise definition. At the heart of economic rationality however is the central premise that individuals act to maximize their expected utility. That is, when presented with several choices, individuals will choose the one that they think will make them the happiest, i.e., maximizing net benefit, which is equal to total benefits minus total costs. This is known as the Expected Utility Theory.

Gabriel Cramer and Daniel Bernoulli gave birth to the idea in the 18th century, and it gained in importance as time went by. Nowadays, Expected Utility Theory dominates the field of economics and is widely used in many economic models and real-life policies.

Towards the later half of the 20th century however, doubts started to creep in: do people actually behave like economically-rational individuals, as described by the Expected Utility Theory?

When the choices and consequences are clear and measurable, we have little problem in making optimal decisions. But when the choices are complex, consequences less clear, less measurable, we can be wildly off the mark. And real-world situations are typically of the latter type. So perhaps humans are rational, but due to limited information and our own cognitive limitations, we can only be rational up to a certain point.

Put another way, humans are only rational when the math involved is relatively simple. This is the idea of "bounded rationality", which Herbert Simon introduced in 1950s.

Going further, Daniel Kahneman and Amos Tversky, observing that irrational behavior is actually quite common and non-random, created what they termed the Prospect Theory in their seminal paper in 1979. Prospect Theory describes several systemic biases—such as loss aversion—in human behavior, which often cause us to act irrationally.

Prospect Theory became the foundation of the new field of Behavioral Economics. It also started a movement towards a better way of doing economics: theories that are based less on abstract, normative ideas, and more on hard evidence and data.

Rational Behavior: Biological Roots

"We are survival machines—robot vehicles blindly programmed to preserve the selfish molecules known as genes." "Prediction in a complex world is a chancy business. Every decision that a survival machine takes is a gamble, and **it is the business of genes to program brains in advance so that on average they take decisions that pay off**. The currency used in the casino of evolution is survival, strictly gene survival, but for many purposes individual survival is a reasonable approximation."—Richard Dawkins [1]

Rationality might also have roots in biology, especially if you view survival of the fittest as competition at the gene level and not at the individual level [2]. This is also known as the Selfish Gene Theory, developed by John Maynard Smith, W.D. Hamilton and Richard Dawkins, among others. The Selfish Gene Theory postulates that DNA is the main means of information transfer between generations and over time, populations will move towards evolutionarily stable strategy.

Because the world has very limited amount of resources and because each of us is wired biologically to survive and pass on our genes, we are bound to compete for these resources. That means that all else being equal:

- When the opportunity to extract gains (material or non-material) presents itself, our default mode of behavior is to take it to maximize our chance of survival, in the face of future uncertainty.
- When two or more such opportunities arise, we will take the one that gives us more gains, provided that the gains can be accurately measured. Again, this is so that we maximize our chance of survival, in the face of future uncertainty.

This is similar to Expected Utility Theory, only rephrased from the evolutionary standpoint.

In reality, measurement of gains are subjective and only transferable between individuals under a common Unit-of-Measurement (UoM), such as prices in dollar or gold. In the case of Prisoners' Dilemma for example, the UoM is the number of years in prison. Difficulty arises when there is no consistent UoM or UoMs are not easily convertible, e.g., how much money is worth staying one year in prison?

So rationality, even if coded at the gene level, is likely very rough heuristics. Genes, after all, can't make worldly information suddenly more available, or reduce the complex math inherent in the natural world. But genes can ensure a basic high-winning-percentage strategy: to program us to take resources in a resource-constrained world. You might end up taking more than you need, but it is better to err on the side of your action being *maybe* unnecessary, than being *for sure* sorry the next day.

Bitcoin's Incentive Scheme

Above we have established that human behavior, although fickle and suffers from systemic biases, likely exhibits bounded rationality, coded at the gene level. The simpler the problem and the simpler the math involved, the more likely we will make the optimal, rational decision.

As it occurs, Bitcoin's incentive scheme mostly falls into this category. What is Bitcoin's incentive scheme?

(a) **Fixed supply:** There can be no more than 21 million bitcoins ever.

(b) **Mining subsidy:** Bitcoins are created each time a miner discovers a block. The number of bitcoins generated per block is set to decrease geometrically, with a 50% reduction every 210,000 blocks, or approximately four years. As of this writing (Dec 2018), the current subsidy is 12.5 bitcoins per block.

(c) **Transaction fees:** Users include transaction fees in their transactions as payment to miners for processing those transactions. Transaction fees follow the market forces of supply and demand. When blocks are full, fees are high. Vice versa, when blocks are empty, fees are at their lowest.

Let's briefly go through each one and see how rationality plays a role in making these incentives work.

(a) A fixed supply is Bitcoin's primary financial incentive. If successful, Bitcoin would be the rarest asset ever existed—much rarer than even gold and diamond. All else being equal, if people are rational, they should prefer the rarest asset to store value in, given a number of available assets.

(b) Mining subsidy is a temporary incentive, but it is essential to the initiation of Bitcoin. Bitcoin, as with most networks, had a chicken-and-egg problem: why should the first few people participate in an infant network when there were barely anyone else? Relying purely on non-profit-minded volunteers to support the network would be unsustainable. Bitcoin solved this problem by giving early adopters higher amounts of rewards, in the form of subsidy. If people were rational, and estimated Bitcoin to have *any* chance of success, then the subsidy should serve as a strong enough incentive to overcome the initial risks and uncertainty associated with Bitcoin mining. The subsidy bought Bitcoin time until it is strong enough to protect itself from external attacks. This was also the fairest way to distribute bitcoins: by giving them to people who most strongly believed in and contributed to the project when no one else did. However, mining subsidy is irrelevant in the long run, past the bootstrapping stage.

(c) Transaction fees are Bitcoin's true second main incentive. As stated, in the long run Bitcoin has to remove mining subsidy altogether in order to not violate the

scarcity incentive from (a). As Satoshi put it: "In a few decades when the reward gets too small, the transaction fee will become the main compensation for nodes."

If transaction fees are high enough, and people are rational, there should be a healthy mining industry to keep the network secure. Worth noting that due to transaction fees being a highly variable factor—which is a stark contrast to the predictability of a fixed supply and fixed inflation schedule—the math involved in calculating opportunity costs of pursuing transaction fees is more complex. Bitcoin's transition to a fee-driven model is untested, and it remains to be seen whether the transition would happen smoothly.

So we see how Bitcoin's sustainability greatly depends on rational human behavior at the core. This is a crucial point and an aspect where Bitcoin is inferior to gold, the previous standard of sound money. If people choose to stop using gold as money (perhaps irrationally), gold is fine. It would still exist in nature, and could make a comeback as money centuries later. If people choose to stop using or mining Bitcoin (perhaps irrationally), it will need to be bootstrapped later, or might fail to be bootstrapped ever again.

In return for this inferiority, Bitcoin is superior to gold in almost all other departments desirable for a monetary asset, e.g., transferability and portability.

Side Note: Development Incentive

Since Bitcoin exists as software and requires active development and maintenance [3], a few words are warranted on the issue of development incentive. Since this issue is more about resource allocation than the creation of digital scarce money itself, feel free to skip this section. Development incentive in general is orthogonal to Bitcoin's incentive scheme as described above.

Unlike miners, developers do not have a direct financial incentive in the protection and development of Bitcoin. Instead, Bitcoin software development relies on a voluntary open-source-software system—where developers who are most philosophically-aligned with the cypherpunk ethos of Bitcoin are motivated to work on it on their own free time. This might seem inefficient, and perhaps due to the success of Bitcoin's incentive scheme so far, several altcoins have been trying to address this problem by adding development incentive to their protocols.

However, in-protocol development incentive is highly challenging. The reason is that it is very different to Bitcoin's original incentive scheme, which has some very special properties:

- The common goal can be **mathematically-defined**: miners get paid for a hash that is smaller than or equal to the current difficulty target.

- The common goal is **computationally-verifiable**: miners' work towards the goal is verifiable by anyone, cheaply; and miners only get rewarded after the fact.

This makes Bitcoin's incentive scheme *automatable*. That is, it doesn't need any human intervention to work, and can exist safely as fixed rules within the protocol. In general, in-protocol incentives make sense if the goals can be mathematically-defined and computationally-verifiable.

Development goals, however, are often highly fuzzy [4], neither mathematically-defined nor computationally-verifiable. For example, a typical development goal is to scale Bitcoin to handle twice the traffic without degrading overall network security or Bitcoin's essential attributes. However, opinions differ wildly on what "network security" or Bitcoin's "essential attributes" mean. These goals, even if somehow met, are hard to be verified or verified cheaply. Ultimately what that means is that these goals require subjective human inputs. Thus, they are poor candidates to be built into the protocol, adding overhead without being necessarily beneficial. Development incentive is better off being handled off-chain.

In summary, Bitcoin is unlike any other technologies ever created in that human behavior is one of its core moving parts. It is the first of its kind.

Bitcoin's reliance on human behavior implicitly assumes that humans are rational actors. This rationality assumption might break down in certain situations, such as when information is limited, or when the opportunity costs calculations become too complex. Or within a community of Buddhist monks who were trained from birth to reject material gains. Or imagine a world where resources are infinitely abundant: it's likely that the beings there will develop behavior not wired to compete or maximize utility [5].

Despite that, there is strong evidence that we humans do possess some degree of rationality, or at least a bounded version of rationality. It is this bounded rationality that Bitcoin's survival hinges on. Bitcoin needs rational actors to bootstrap its network. Bitcoin needs rational actors to buy into its promise of sound money, HODL at all costs, and consequently raise its price. Bitcoin needs rational actors to keep participating in mining and sustain the network for the next 100-1000 years. Can we, and future generations, stay rational at all times and forever? Or would we be foolish and prematurely abandon this idea, no matter how sound it is?

*This is part 4 of the Bitcoin Fundamentals series. Check out the full series here: [part 1](#), [part 2](#), [part 3](#), [part 4](#), and [part 5](#).

Acknowledgements

Special thanks to [Murad Mahmudov](#), [Nic Carter](#) and [Steve Lee](#) for their extremely valuable feedback.

[1]: [The Selfish Gene](#), by Richard Dawkins.

[2]: "Some research suggests there is a genetic basis for greed. It is possible people who have a shorter version of the ruthlessness gene (*AVPR1a*) may behave more selfishly; [Ruthlessness gene discovered](#)." ([Wikipedia](#)). Also see [related work](#) on the burgeoning field of Genoeconomics.

[3]: Recently a consensus-critical bug, [CVE-2018-17144](#), has been discovered then quickly fixed in Bitcoin. If it was exploited, some Bitcoin nodes could have been tricked into accepting a block that inflates the supply beyond 21 million bitcoins. This event highlights the difficult nature of software development, despite the quality of development team (read my analysis of that bug [here](#)). There is also a good chance that the Bitcoin protocol will get ossified at some point in the future, which lessens the need for active development, if not completely removes it (i.e.: critical bugs might still need to get fixed).

[4]: The fuzzy nature of software requirements and difficulty in writing precise "specs" are problems well-known within the software industry.

[5]: Note that in this last example one can argue that this behavior is not really irrational in that context. However we are using "rationality" loosely here to mean utility maximization, not necessarily about being based on logic or reason.

Thanks to [Nic Carter](#).

Bitcoin is a Decentralized Organism (Mycelium) – Part 1/3

By **Brandon Quittem**

Posted December 11, 2018

This is post 1 of a 3 part series

- [Bitcoin is a Decentralized Organism \(Mycelium\) – Part 1 / 3](#)
- [Bitcoin is a Social Creature \(Mushroom\) – Part 2/3](#)
- Post 3 will be listed here when available

Below: Original Artwork by Emmaline Bailey



Forward

First, I need to give credit to Dan Held for publishing his 4-part series [comparing bitcoin's origin to planting a tree](#). While I loved his series, I believe a more robust

analogy is comparing bitcoin to fungi. If you're new to this topic, strap in—it is my honor to initiate you into the fascinating world of fungi.

Polymathic responsibility: Just as Satoshi combined separate disciplines to stitch together a franken-technology we call bitcoin... It is my belief that each of us has the responsibility to explore our unique cross sections of knowledge. Here's my exploration of fungi and bitcoin—the parallels are astounding.

Introduction

Bitcoin appears superficially simple upon first glance, however truly understanding the system is a daunting task.

"Intellectual traps" exist along the way, tricking observers into making hasty assumptions. I liken the pursuit of understanding bitcoin to a mountain climber

continually reaching “false peaks” that momentarily fool the climber into thinking they’ve reached the actual summit.

As soon as you think you have bitcoin figured out, you discover how little you actually know (false peak).

Competing narratives make it even more challenging... Magic internet money, speculative mania, fintech revolution, bitcoin boils the oceans, rat poison squared, libertarian idealism, digital gold, apex predator of monetary media, gordian knot of interlocking incentives, etc.

To make matters more complicated, bitcoin is a living system constantly changing based on environmental stimuli. True understanding is a moving target unlikely to ever be hit.

Attempting to answer the question “what is bitcoin,” I found exploring parallels to the natural world to be particularly illuminating.

In particular, some of bitcoin’s best characteristics are simply reflections of successful evolutionary strategies found in nature, specifically in the fungi kingdom.

Fungi are predominantly made up of “mycelium”—an underground decentralized intelligence network described by Paul Stamets as “earth’s natural internet.”



Image credit: John Upton

“I believe that mycelium is the neurological network of nature. Interlacing mosaics of mycelium infuse habitats with information-sharing membranes. These membranes are aware, react to change, and

collectively have the long-term health of the host environment in mind. The mycelium stays in constant molecular communication with its environment, devising diverse enzymatic and chemical responses to complex challenges.”

— Paul Stamets, Mycelium Running: How Mushrooms Can Help Save the World

In this essay I’m going to explore the similarities between fungi and bitcoin in 3 parts, each representing a different stage in the life cycle of common fungi.

- Part 1: Bitcoin as a decentralized network architecture (Mycelium)—this one
- Part 2: Bitcoin as a social phenomenon (Mushrooms)

- Part 3: Bitcoin as a catalyst for human evolution (Reproduction/Sporulation) – coming soon!

Introduction to Fungi

My favorite TED Talk: 6 Ways Mushrooms Can Save the World (Paul Stamets)

Fungi are in their own separate kingdom just like plants and animals. There are more fungi species than plants and animals combined.

Animals are more closely related to fungi than we are to plants. Both fungi and animals inhale oxygen and exhale carbon dioxide. Plants produce their own food through photosynthesis (autotrophic) while animals and fungi must find their own food (heterotrophic). Animals evolved to have internal stomachs/brains whereas fungi pursued external stomachs/brains.

Fungi Fact #1: humans share over 50% of their DNA with fungi. Scientists proposed a new super kingdom called Opisthokonta combining Fungi and Animals.

Fungi can take many forms. Most organize in an underground “root structure” called mycelium that's found nearly everywhere on this planet.

When conditions are right, fungi produce mushrooms which then release spores (seeds) that attempt to colonize life in a nearby location. Mushrooms are simply the reproductive organ. Mushrooms are to the mycelium what apples are to a tree.

Fungi are paramount to life on earth:

- The largest organism on our planet is a fungal network
- Fungi are the best chemists on our planet, much of our medicine comes from fungi
- Trees cannot survive without underground fungal allies
- Fungi have been around for 1.3b years surviving all 5 great extinction events
- Fungi are capable of saving the bees

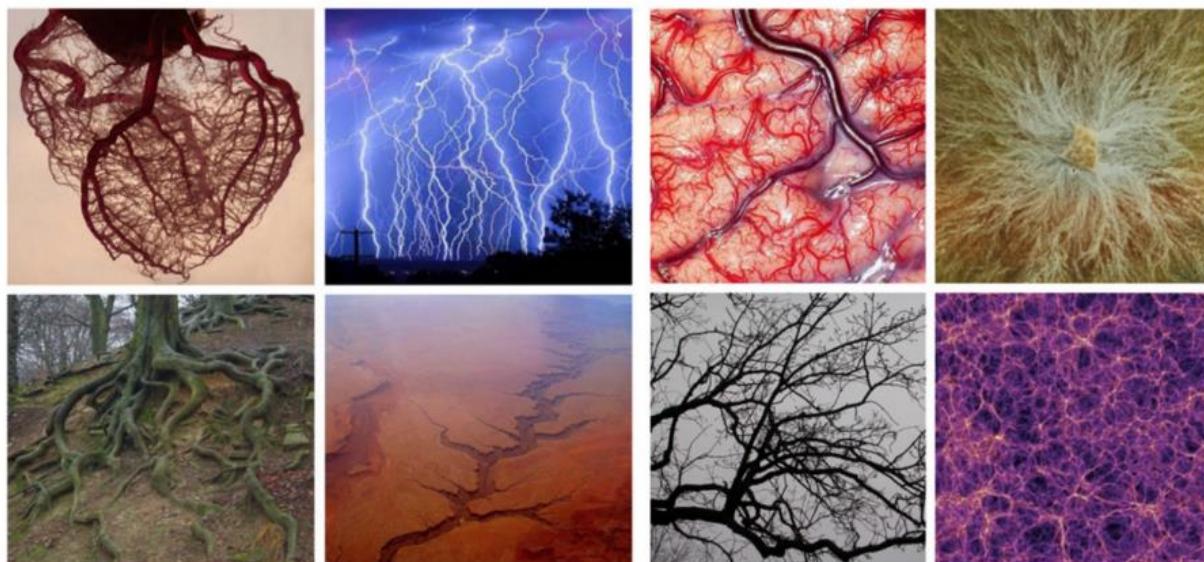
Fungi are Decentralized Intelligence Networks

Fungal networks don't have a centralized “brain.” Instead, they are a one-cell walled “root system” called Mycelium. This underground stomach and distributed intelligence network is capable of sending information bi-directionally over long distances and even across species lines. These fungal networks constantly evolve based on feedback from their environment.

At any one point, a fungal network contains millions of end points each searching for food, defending their territory, or inventing new molecules to subvert their

competition (other fungi, bacteria, etc). These networks form a decentralized consensus on how to use resources, when to reproduce, and what strategy best defends the organism.

This mirrors the decentralized consensus (social contract) formed in bitcoin. Nodes determine what software they wish to run and enforce the consensus rules they support accordingly. Miners determine which transactions to include in blocks. Exchanges, wallets, and merchants each steward large groups of users. Each participant in bitcoin voluntarily chooses how they wish to participate and the aggregate consensus represents the network.



From left: the human heart, lightning, the human brain, mycelium, roots from a tree, an aerial view of The Grand Canyon, branches from a tree, and the cosmic web of The Universe. [#evolveandascend](http://www.evolveandascend.com)

Decentralized Networks are Older Than Humanity

Decentralized networks have existed long before humans were around. In fact, fungi have been successfully implementing such systems for 1.3 billion years making them the most successful kingdom on our planet.

Besides fungi, there are several examples of distributed network archetypes found throughout nature (mycelium, dark matter, neurons, the internet, etc). Clearly this strategy works otherwise nature wouldn't insist on replicating it.

When seen in the context of this long history of the decentralized network archetype, the advent of decentralized digital money seems less novel and more inevitable.

The decentralized network archetype is Lindy.

During a Billion Years of Evolution, Fungi Have Become Masters of Survival.

Fungi are uniquely adaptive and continue surviving mass extinction events.

65 million years ago a giant asteroid hit our planet killing most life (including the dinosaurs) on our planet. The impact created a cloud of smoke so thick that it blocked sunlight from reaching the earth's surface for many years. Without sunlight, plants died off and with them most animals. Fungi however do not rely on sunlight to survive, they can adapt quickly, and can find their own food.

After each extinction event, fungi "inherit the earth" and slowly rebuild until conditions stabilize and life can continue again.

Bitcoin will become the most successful monetary specie because its decentralized, adapts (relatively) quickly, finds it's own food (unmet demand), and doesn't need government support. In the event of a mass monetary extinction event, bitcoin will "inherit the earth."

Japanese Government vs the Humble Slime Mold

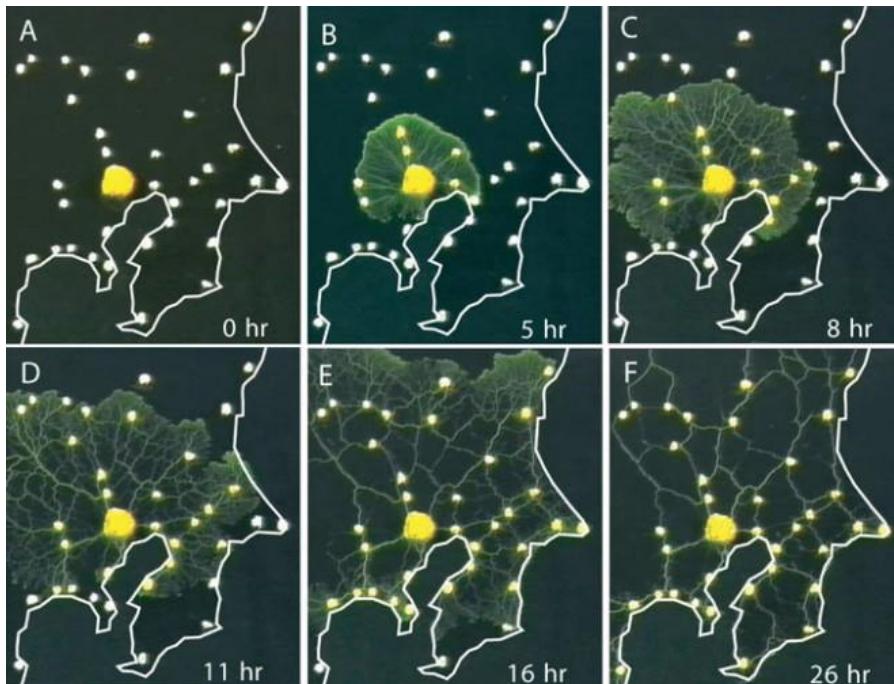
Whether it's central banks trying to steer the economy or hierarchical corporations trying to maximize value in the information age... Central planning has many flaws.

When making decisions in the "information economy," decentralized or flat organizations are more effective. They resist corruption, minimize bureaucracy, and push decision making to the extremities where individuals (nodes) have the most up to date information about the problem at hand.

Let's take a look at the Tokyo subway system to illustrate the power of decentralized networks.

Scientists conducted an experiment where an ancient fungus (slime mold) was incentivized to recreate the Tokyo subway system. Each subway stop (node) was marked with the slime molds favorite food (oat flakes).

After a short while, the slime mold grew to connect all the nodes/stops in a more efficient design than the centrally planned committee of engineers hired by the Japanese government.



Slime Mold designing Tokyo Subway System

From the Abstract:

Transport networks are ubiquitous in both social and biological systems. Robust network performance involves a complex trade-off involving cost, transport efficiency, and fault tolerance. Biological networks have been honed by many cycles of evolutionary

selection pressure and are likely to yield reasonable solutions to such combinatorial optimization problems. Furthermore, **they develop without centralized control and may represent a readily scalable solution for growing networks in general**. We show that the slime mold *Physarum polycephalum* forms networks with comparable efficiency, fault tolerance, and cost to those of real-world infrastructure networks—in this case, the Tokyo rail system. The core mechanisms needed for adaptive network formation can be captured in a biologically inspired mathematical model that may be useful to guide network construction in other domains.

When you think of the costs and complexities involved in such an infrastructure project, it's quite sobering to realize a slime mold can design a better network in a single day.

Satoshi understood the power of the slime mold.

Bitcoin is a non-sovereign monetary good that pushes complexity and decision making to the edge just like fungi. Over time, this free market decentralization allows bitcoin to out-compete various legacy financial systems who have little skin in the game, suffer from the innovator's dilemma, become more fragile over time, and often drown in bureaucracy (or worse).

Life Without a Centralized Point of Failure

Mycelium has no “central point of control.” Any individual part can be removed but the system as a whole survives.

Bitcoin functions the same way: as any one developer, node, miner, exchange, or user may be vulnerable yet not crucial for its survival. No one to jail, no one to shut down, no essential hardware to seize. Anytime one attacks bitcoin/mycelium but doesn't successfully kill it, the system gets stronger.

"If you come at the king, you best not miss" — Omar Little (The Wire)

Nation states and central banks face a paradoxical challenge. If they attempt to destroy their competition, they'll highlight the very need for bitcoin in the first place. And yet, the longer they wait, the stronger bitcoin becomes.

Hardened from hostility

Both mycelium and bitcoin endure in the most competitive ecosystems on our planet and must constantly adapt in order to survive. They have skin in the game and become hardened from hostility.

Fungi are in a 24/7 competitive environment, constantly fighting little underground battles against various bacteria, microbes, and competing fungi.

If one mycelial "node" senses a predator/prey, it sends information to the "mushroom scientists" who then create a new enzyme to target the predator/prey. The fungal network distributes this new enzyme where needed.

Over time, the fungi develops a chemical library that acts both as a robust immune system and improves its ability as a predator—enabling greater ecological success. It's no wonder fungi can survive anywhere and continue to maintain dominance on our planet. Fungi are antifragile.

Fungi fact #2: As humans, we benefit from medicinal compounds created by fungi. Most famously: Penicillin, which came from an accidental discovery by Alexander Fleming. Penicillin has been used to combat bacterial epidemics that historically have decimated human populations. Since the discovery of Penicillin our population has tripled.

Bitcoin responds to its environment in a similar manner. As bugs/threats/opportunities are found in the system, information travels to the "bitcoin scientists" (developers) who create an "enzyme" (software patch) and this update propagates through the system. This enables greater ecology success for bitcoin too. Bitcoin is antifragile.

Both fungi and bitcoin harden their defenses over time and learn to consume new food sources. This has a compounding effect increasing antifragility as well as life expectancy over time.

In one extreme case, let's take a look at the largest organism on our planet, the Honey Mushroom (*Armillaria* sp). Found in the Blue Mountains in Eastern Oregon, this single organism is over 2.4 miles (3.8 km) across. It's estimated to be between 1,900 and 8,650 years old and is currently consuming an entire forest.

Dealing with Competition

Fungal networks steal competitive advantages from their neighbors in the form of genetic information just like bitcoin absorbs competitive advantages displayed by altcoins.

There is a (misguided) belief in which people assume that altcoins will implement cool new features that will eventually outcompete bitcoin.

The opposing camp believes that bitcoin will eventually absorb all the best features after they've been tested in the market which makes alternative currencies unable to compete over the long term. I stand in this camp.

Let's take a look at how fungi approach their competition...

First we need to understand some basic genetics. Genes are typically passed down from parent to offspring in what's known as "Vertical Gene Transfer."

Interestingly, fungi perform "Horizontal Gene transfer"—effectively slurping up genetic information from different species competing in the same ecosystem.

Fungi "take what works" from other species that compete in the same ecosystem. This phenomenon can be observed by examining "dung loving" who are more closely related to each other than their genetic ancestors.

This process of horizontal gene transfer demonstrated by fungi foreshadows the future state where bitcoin integrates any proven ideas produced by alt coins at large.

For example: Combining the Lightning Joule Browser extension with a node (launch your own, use Casa, or otherwise) enables micro-transactions through your browser. This effectively eliminates the need for tokens like BAT.

You could even make the argument that bitcoin has been performing horizontal gene transfer since Satoshi first combined technologies used in previous attempts at electronic cash systems such as Hash Cash, E-gold, etc.

Arbitrage, Incentives, and Finding Their Place in Ecology

Fungi perform two ecological roles on this planet: they recycle all matter into base elements & act as our planet's immune system.

"Mycelia are the grand disassemblers of nature" — Paul Stamets

Fungi spend their days quietly decomposing organic matter. They transform rocks, branches, leaf litter, dead animals, and oil spills into their base elements (carbon, nitrogen, oxygen, etc). Then fungi trade these valuable elements with nearby organisms.

Fungi fact #3: Our forests would be buried in hundreds of feet of leaves and branches if fungi didn't decompose them and redistribute the nutrients.

In other words, fungi unlock stranded resources. A tree cannot re-use its own leaves or branches as the carbon/nitrogen/phosphorus are locked in an unusable form. Fungi exploit arbitrage opportunities in their ecosystem.

Bitcoin, Through its PoW Mechanism, Unlocks Stranded Resources in the Form of Energy.

Before we tackle bitcoin, let's explore a fascinating historical example: How aluminum was used to "export stranded renewable energy" from a country like Iceland.

Iceland produces renewable geothermal energy, often in remote places. This leads to an excess supply that cannot reach the demand (energy doesn't travel well over long distances).

Iceland took advantage of their excess energy by producing aluminum, which is a very energy intensive process. Iceland effectively turns excess energy into a durable store of value (Aluminum) which can be exported.

Bitcoin does the same thing. Instead of stranded energy "dying on the vine," producers can mine bitcoin (or just sell excess energy to miners). This, too, enables excess energy production to be turned into a durable store of value. The second order effect is that bitcoin is effectively subsidizing renewable energy projects.

To explore this concept in depth, check out Dan Held's Article: [PoW is Efficient](#).

Fungi Fact #4: Fungi eating rocks is the main reason we have topsoil. Topsoil enables us to grow food. It took fungi over 1b years to produce just the 18 inches of topsoil that we have today.

Fungi (and Bitcoin) Are Ecological Immune Systems

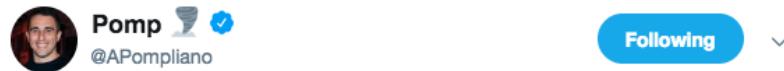
Fungi are the immune systems for both the ecosystems in which they live and the planet at large.

Fungi produce medicinal compounds and protect their ecosystems through complex symbiotic relationships. Fungi broker resources underground (via mycelium) between species to ensure the health of the entire ecosystem.

[How trees secretly talk to each other in the forest] What do trees talk about? In the Douglas fir forests of Canada, see how trees "talk" to each other...(<https://video.nationalgeographic.com/video/decoder/00000165-61d1-d3b2-a17d-egf9571f0000>)

In crude terms, the fungi mine minerals underground for trees in exchange for sugars (food) that the tree produces through photosynthesis. Trees get increased protection from invaders and crucial minerals which they cannot find on their own. Ever wonder why the baby oak tree can survive on a forest floor where it receives no sunlight?

Each organism participating in this shared incentive system improves the evolutionary fitness of the forest. I believe forests are living super-organisms consisting of a variety of different species.



Bitcoin performs a similar ecological role

Recent tweet from Pomp

The market sends signals for bitcoin to create features that satisfy unmet demands or improve security as new threats emerge.

Bitcoin is the internet's response to the fraud and corruption of the legacy financial system.

Just a matter of time before the real disruption begins.

11:50 AM - 29 Nov 2018

453 Retweets 1,981 Likes



- Block space demand increases above capacity, Lightning Network is born.
- China cracks down on exchanges, [LocalBitcoins.com](#) flourishes.
- As Venezuela, Turkey, and Argentina hyper-inflate their currency, bitcoin steps in as a non-sovereign SoV.
- [Blockstream launches Satellites](#) able to broadcast bitcoin transactions to mitigate catastrophic events.

You could even make the case that bitcoin acts as humanity's immune system — helping fight off cancerous governments, rent seeking businesses, central bank seigniorage, debasement of the monetary supply, and even one of humanity's tragic faults: greed.

Positive feedback loop

Bitcoin also benefits from the aligned incentives between users, full nodes, miners, exchanges, and merchants. As bitcoin better adapts to its environment, it better meets the demands of its growing constituents, which in turn recruits more network participants. This positive feedback loop promotes sustained growth of the network.

Like the honey mushroom consuming entire forests in Oregon, bitcoin is getting bigger and stronger over time.

Conclusion

Did you enjoy this? [Check out Part 2 where I examine bitcoin as a social phenomenon.](#)

Bitcoin is hard to pin down. Is it technology? A get rich quick scheme? New age religion? Payment rails? Or is it primarily a social system (super-organism) made of individually replaceable cells that share aligned incentives? Join me as we explore these questions through the lens of Fungi in [Part 2](#).

Follow me here on [medium](#) and [twitter](#) to be notified when future articles are released.

Fungi fact #5: I wrote most of this essay while consuming medicinal mushrooms used for cognitive enhancement (Lions Mane, Chaga, and Cordyceps).

Thanks for reading, Brandon

Acknowledgments

- Thanks to [Dan Held](#), [Nic Carter](#), [Murad Mahmudov](#), [Vijay Boypati](#), [Pierre Rochard](#), [Hasu](#), and many more for challenging my understanding of bitcoin.
 - Thanks to [Paul Stamets](#) for pushing the boundaries of Mycology and inspiring me along the way.
 - Thanks to my friends who convinced me I wasn't crazy to compare mycelium and bitcoin in the first place. And for the edits: Rob Fox, [Dan Liebeskind](#), Justin Evidon, Anne Rapp, and many more.
 - Special thanks again to Dan Held whose [Planting Bitcoin](#) series motivated me to finally get these ideas written down and for providing notes on earlier versions of this essay.
-

Bitcoin is a Social Creature (Mushroom)—Part 2/3

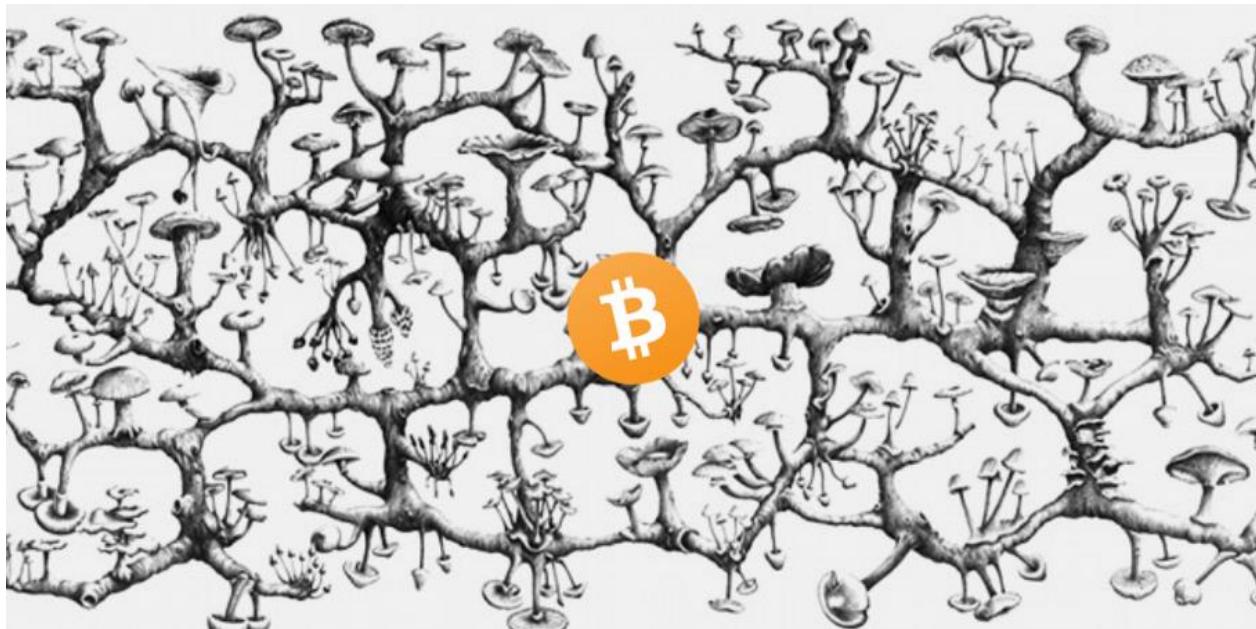
By Brandon Quittem

Posted December 28, 2018

This is post 1 of a 3 part series

- Bitcoin is a Decentralized Organism (Mycelium)—Part 1 / 3
- Bitcoin is a Social Creature (Mushroom)—Part 2/3
- Post 3 will be listed here when available

Exploring Hype Cycles, Ethnomycology, and the Cult of Satoshi



Original Artwork by Richard Giblett

Introduction

In my last article, "Bitcoin is a Decentralized Organism" we explored bitcoin's decentralized architecture through the lens of mycelium. We covered the decentralized network archetype, antifragility, PoW, arbitrage, bitcoin's role in it's ecology, and the merits of decentralization.

However, our fungi story is not yet complete. The next stage in the fungal life cycle is to reproduce and this all happens inside the mushroom. After reaching maturity,

mushrooms release little mushroom seeds called spores capable of colonizing new territory.

Although the fungi kingdom is quite alien compared to life in the animal kingdom, humans have had a relationship with mushrooms for a long time. Historically, mushrooms have represented mystery, fear, opportunity, impermanence, and to some a cult-like reverence.

In this article, we're going to explore bitcoin as a social phenomenon through the lens of the mysterious mushroom.

Disclaimer: If you're new to the fascinating world of fungi, I recommend starting with part 1.

Short on time? Here's a condensed version:

<https://twitter.com/bquitem/status/1072864756296486913>

Bitcoin is a Social System Ratified by Code

Bitcoin is made up of individual constituents each with their own perspectives, motivations, and abilities. Collectively they form consensus on the rules of the bitcoin game. The code simply ratifies this social consensus.

From Hasu's seminal piece Unpacking Bitcoin's Social Contract:

"The Bitcoin protocol automates the contract that is agreed upon on the social layer, while the social layer determines the rules of Bitcoin, based on the consensus of its users. They are symbiotic: Neither would be sufficient without the other."

Humans are messy, emotional, predictably irrational beings. Bitcoin, being comprised of a network of humans, is no different.

Section #1: Human Psychology, Hype Cycles, and the Mushroom Method

Fungi exist primarily in their "mycelium form" which you can think of as an underground root system connecting trees and plants. Humans wouldn't even know mycelium exists as it stays quiet underground for the majority of its life.

However, when fungi sense that conditions are favorable (temperature, humidity, etc), it sends up a mushroom above ground. These mushrooms are the sexual organs of fungi—essentially phallic spore (seed) delivery systems.

Before mushrooms break the ground, fungi concentrate energy into a tiny mass of cells underground called "pinheads" which persist until the perfect moment. Then,

seemingly out of nowhere, mushrooms explode out of the ground doubling in size each day until reaching maturity.

Fungi Fact #1: Some fungi can produce mushrooms with enough force to break through asphalt.

After the mushroom is fully mature it crescendos with a release of millions of spores (mushroom "seeds") before quickly decomposing back into the ground.

The mushroom only lives for a few triumphant days and most spores perish before infancy, however a small percentage of the spores will travel nearby and form new fungal colonies. These new colonies might stay underground for several years before the reproductive cycle continues again.

Fungi Fact #2: Spores are lighter than air which makes travel easy. Theoretically spores could catch an updraft and leave earth's orbit. Luckily, they're on a short list of biological matter capable of surviving the cold vacuum and radiation of space. Panspermia anyone? Save your tinfoil hats for part 3 ;)

Mushroom Timelapse porn

Bitcoin's Hype Cycles Parallel Fungal Reproduction

To the casual observer, most of bitcoin's life is boring—months go by with relatively little action. Then when conditions are just right, bitcoin explodes into life, growing massively in size, and hijacking the consciousness of observers. Price goes to the "moon," media is flooded with hyperbole, and "DMs from normies" flood in.

Then almost as soon as it crescendos, bitcoin fades away, dying back into obscurity as casual participants write it off as a fad, hype, or a failed experiment. Like the mushroom spores, most new users exit the ecosystem. However a small percentage form new colonies in bitcoin land. These bear market survivors become new "hodlers of last resort."

Unsurprisingly, the bear market narrative is driven by surface level activity (price).

Bitcoin Detractors Mistake the Hype Cycle (Mushroom) for the Big Picture (Mycelial Network)

Amnesiac pundits proudly pile on proclaiming bitcoin has perished (for the 335th time). Fiat maximalists take victory laps on twitter by posting 12 month charts.

"You're missing the mycelium for the mushroom!" h/t Nic Carter

Roubini celebrates by hosting his 3rd bear market barbecue. Detractors gather to roast the proverbial (bitcoin) mushroom while patting each other on the back.

However to be fair, bitcoin is complicated. Many “crypto people” still think bitcoin is myspace and Ripplecoin is the “standard.” Unsurprisingly most journalists don't grasp what's going on. Imagine being assigned the “bitcoin beat” as a well intentioned, run-of-the-mill journalist.

While the mushroom has died (recent hype cycle), the mycelium (bitcoin) is thriving underground.

Like a mushroom past its prime, bitcoin exuberance decays and the price plummets. This bear market will shake out weak hands, hedge funds will fail, ICOs will give back investor money or worse, projects will fail, and some charlatans will be exposed.

However hodlers, new and old, collectively go underground and quietly make bitcoin better: building, learning, and forming alliances.

Bitcoin has improved dramatically in 2018:

- Lightning Network is picking up momentum
- SegWit adoption grows to around 40% improving transaction throughout
- New developers being groomed by Jimmy Song & Justin Moon
- The Block sets the standard for journalism in the space
- Casa, Pierre, Nodl, and others make running full nodes easier
- Nomics producing cleaner data than CMC
- Foundations laid for inevitable financialization (Fidelity, Bakkt, etc)
- Schnorr signatures are being built out (tech specs / whitepaper / TL;DR)
- Trace Mayer promotes “Proof of Keys” to minimize risk of rehypothecation + stress test ecosystem + remind new users about self sovereignty
- Blockstream enables bitcoin transactions via satellite. Things get interesting when combined with mesh networks.
- New metrics for measuring health of cryptocurrencies emerge such as Realized Cap, Economic Throughput, Economic Density (\$/bytes), and MVRV.

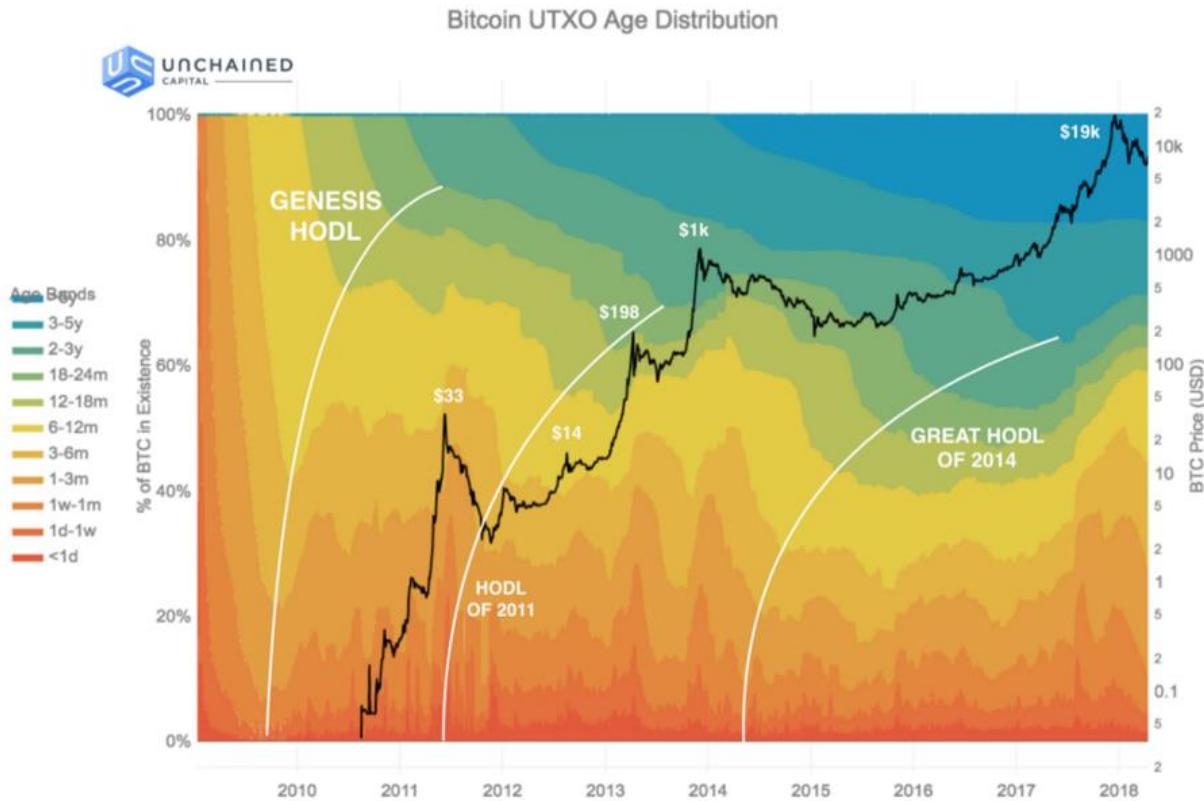
Saifedean Ammous (@saifedean) Following
Correction: Roubini hasn't been mocking Bitcoin since it was \$600. He's been mocking it since it was \$58. Imagine how short your attention span must be, & how strong your self-delusion, to gloat with vindication during every dip from \$58 to \$7,000.

Nouriel Roubini (@Nouriel)
In good company with Gold. @Convertbond: While everyone was focused on Gold and Silver, #BITCOIN dropped another 40%, traded below \$58

1:21 PM · Apr 16, 2013

- Passed the peak of miner centralization (bye bye Bitmain)
- Coinshares report says 77% of bitcoin's energy consumption is from renewable sources
- New scribblers stand on the shoulders of giants attempting to describe bitcoin in novel ways.

As time goes on, narratives evolve as bitcoin continues to reveal herself (himself? itself?) to curious onlookers.



(Hodl Waves by Dhruv Bansal at Unchained Capital)

Eventually the market bottoms. Hodlers cling together like a Band of Brothers creating a strong foundation capable of sustaining future growth.

"Hodlers are the revolutionaries" — Dan Held

As hodlers hoard more bitcoin, the "float" (supply actively being traded) is increasingly constrained. With a decreasing available supply, each new user puts more upward pressure on the price. As price rises, media shines a spotlight, new users are pulled in, and before long we're back in another hype cycle.

Section #2: Mycophobia, Maria Sabina, and the Cult of Satoshi

Sometimes people say crypto can be a bit "culty." This is both true and a net positive. Before we get into bitcoin's religious tendencies, let's learn from our history with mushrooms.

The modern western world has been inflicted with "mycophobia"—the irrational fear of fungi. People fear what they do not understand, and let's face it: most people think mushrooms are "vegetables."

Mushrooms are strange. They represent the life-and-death cycle of impermanence that humans subconsciously fear. *Facing our own mortality is no fun, better to just avoid it.*

However, it hasn't always been this way. In fact, humans have had a relationship with mushrooms for a long time. From food, to medicine, to superstitions and religious artifacts. Mushrooms can save your life, kill you, feed you, and even alter your consciousness.

Anthropological evidence suggests that humans who partnered with fungi had an evolutionary advantage. As more people understand fungi (and bitcoin), they'll soon realize how important they just might be.

Humans Who Partner with Fungi have an Evolutionary Advantage

Ancient man relied on mushrooms to survive in the Alps of northern Italy. Ötzi, the Ice Man, who died nearly 5,300 years ago, was discovered carrying two mushrooms (Amadou and Birch Polypore) tethered on a leather strap. One of the mushrooms was used to start fires and the other was discovered to be medicinally active against the parasite discovered in his gut.

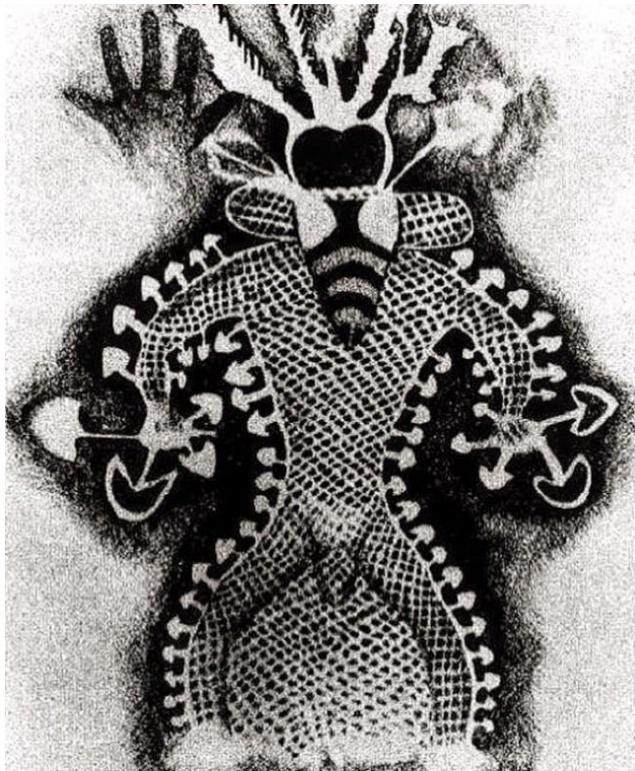


(source)

As far back as 19,000 years ago, a particularly high status woman dubbed the "red lady" consumed mushrooms as evidenced by the spores recovered from her teeth. Whether this mushrooms was for food, religious purposes, or otherwise is unknown.

One of our oldest examples of cave paintings was discovered in northern Algeria, estimated to be over 6,000 years

old. This painting depicted "bee man" who has mushrooms in his hands and growing out of his body.

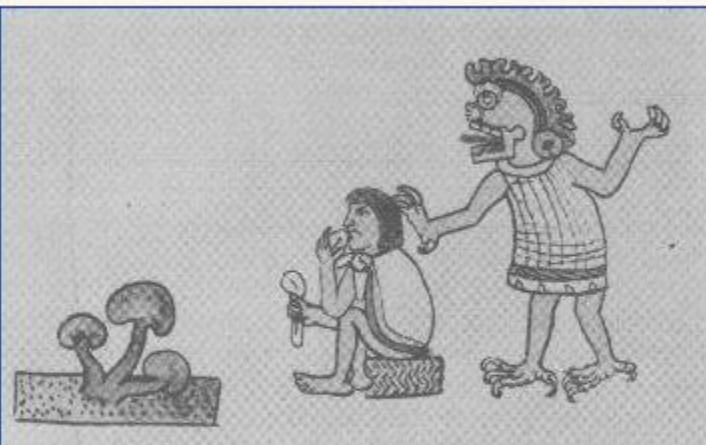


Cave painting: "Bee man" covered in mushrooms. Circa 4,000 BC

In Siberia, the Koryak people revered the "Fly Agaric" mushroom (*Amanita Muscaria*) which is the iconic "red and white" mushroom famously portrayed in Super Mario Brothers and Alice in Wonderland. The Koryak loved this mushroom so much they would drink the urine of humans and reindeer who recently consumed the mushroom. Apparently you can recycle urine in this way up to 5x while achieving desired effects. How they discovered this phenomenon is another question all together...

Get your tinfoil hat, the Fly Agaric may have inspired our Christmas traditions.

The Mazatec Culture from present day Mexico revered the mushroom as sacred. Discovered relatively recently by Gordon Wasson which he detailed in a famous article in a 1955 edition of Life Magazine. Many tourists have since visited this region in Mexico seeking to learn from the famous Mushroom Shaman, Maria Sabina, and her kin.



MEXICAN drawing of 16th Century shows three mushrooms, a man eating them and a god behind him, who is speaking through the mushroom.



MUSHROOM stone" form the highlands of Guatemala dates back to 300-600 A.D.

Mushroom artifacts from Central America

Clearly the mushroom has captured the attention of our ancestors.

Bitcoin Conjures up a Similar Quasi-Religious Fervor

Described brilliantly by Yuval Noah Harari, Homo Sapiens are uniquely capable of cooperating flexibly in large numbers. This enables us to collectively agree on abstract concepts such as nations, gods, and money.

Just as humans formed religious cults around the mushroom, one way to describe bitcoin is a neo-money religious movement.

The mystery of Satoshi created a strong foundation enabling emergent religious tendencies.

Bitcoin was created through immaculate conception by a mythical character (Satoshi) who later sacrificed himself for the greater good.

The Cult of Satoshi inspires some fanatics to dedicate their lives to promoting the "good word." Not all bitcoiners fall into the same religious sect. Some scholars cling to the ancient religious text (whitepaper) while others interpret Satoshi's vision through his early forum posts.

Disagreements about priorities evidenced by the scaling debates have lead to hard forks and fractured "congregations." Not unlike Martin Luther fracturing the catholic church by pinning the "Ninety-five Theses" on the church door in 1517.

Roger Ver was known as "Bitcoin Jesus" from his early days spreading the good word by gifting satoshis to fiat afflicted restaurateurs.

Messianic figures like Faketoshi (Craig Wright) spring up claiming to be the real Satoshi Nakamoto. Faketoshi, the fundamentalist, brands his sacrament as "Satoshi's Vision," the one true bitcoin as laid out in the "bible" (whitepaper).

"The functional details are not covered in the paper, but the sourcecode is coming soon."—Satoshi Nakamoto

Nevermind how incomplete or how many errors are found in the whitepaper, Faketoshi claims his fork of a fork is the real "Satoshi's Vision." Even if Faketoshi's fork WAS closest to Satoshi's original vision (it wasn't), does it even matter?

The answer is no. The essence of bitcoin is intimately tied to the ever evolving social consensus surrounding the protocol.

Each Rival Sect is a Competing Social Contract

Bitcoin's social contract coalesces around a few simple rules. These agreed upon rules (a Schelling point) are then ratified in the bitcoin protocol automating social consensus.

(Source: Hasu's *Bitcoin as a Social Contract*)



Let's use the "great scaling debate" as an example. One group (BCH) believed we should focus on "cheap payments" at the expense of "decentralization," while the other (BTC) believed we need to prioritize "decentralization" on the base layer and scale payments off chain.

As a competing religious sect in a free market, the BCash gang was free to fork the bitcoin code and test their hypothesis. One year later, it's clear that the social consensus surrounding bitcoin doesn't agree with the BCH approach as the market doesn't value BCH or any other fork spawn.

Detractors of bitcoin might then say "forking bitcoin code inflates supply."

However, that's like saying when Zimbabwe prints more money it devalues the US Dollar. [h/t Murad]

In the case of the failed BCash fork(s), they copied the code (bitcoin protocol) but failed to mobilize the people (social layer) resulting in an asset with relatively

minimal value. A prime example of bitcoin resisting corruption from bad actors by requiring social consensus in order to change the network.

In other words, bitcoin replaces social assumptions with mathematical assumptions. We will dive deeper into the consequences this has on our social scalability in part 3 (coming soon).

Religious Fanatic Behavior is an Indicator of Future Success?

We're witnessing a new scarce commodity being monetized in real time. No living person has witnessed such a phenomenon.

In order to actually pull this off, the collective consciousness of the planet will need to change. Convincing people that money isn't green paper and it doesn't need to come from our government will take time.

In order to overcome the inevitable adversity required to create a new global reserve currency, it just might require some "religious zeal." As each new disciple converts to the cult of Satoshi, the chances of hyperbitcoinization increase.

That being said, there are risks of over-politicizing bitcoin . [h/t Hasu]

Some factions of the community portray bitcoin as a club for Austrian Economists who only eat meat that they personally shot with one of their many guns. While those things are well and fine, they are not prerequisites for being a bitcoiner. Let's not entangle the two at the cost of repelling prospective bitcoiners.

Now, be sure to convince all your friends and family to read the New Testament (The Bitcoin Standard) at least twice before heading out on your next FUD Crushing Crusade.

Good Cults Have Incentives to Evangelize

Money is the ultimate network effect—its value is determined by the number of people you can interact with.

In bitcoin, not only does it capture its user's imagination in a religious sense, but there are also financial incentives to recruit new members into the congregation. With each new user that buys bitcoin, the value of bitcoin directionally increases, benefiting previous hodlers. Then that new user is incentivized to convert their friends. Who then convert their friends. And the cycle continues.

As price increases, so do the incentives to improve security as evidenced by the difficulty adjustment—one of Satoshi's most brilliant contributions.

Price increases → mining becomes more profitable → more miners contribute hash power → better security makes bitcoin more valuable.

The Fungus Is Spreading

If the bear market blues make you frown, just look underground. There are countless developments (some listed above) to be optimistic about.

nic [proof of reserves] carter
@nic_carter

Replies to @NeerajKA

Broke: digital gold
Woke: digital slime mold

8:52 AM - 12 Dec 2018

The bitcoin fungus is quietly spreading underground.

With each passing day bitcoin is eating more fiat, becoming more robust, more decentralized, and more Lindy.

Even the darkest night will end and the sun will rise.

Conclusion

Did you enjoy part 2? Part 3 is coming out soon where we will explore bitcoin as a catalyst for human evolution. Here's [Part 1](#) in case you missed it.

Part 3 Teaser: Bitcoin is an inevitable consequence of nature trending towards higher orders of complexity. Bitcoin as a trust minimized communication layer will infiltrate all corners of our globe. This immutable foundation enables us to build a more socially scalable society—a requirement if we're going to coordinate on a global level to achieve new heights of human achievement. Political and environmental coordination, tracking externalities, and even becoming a multi planet species.

Follow me here on [medium](#) and [twitter](#) to be notified when part 3 is released.

Thanks for reading, Brandon

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

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

Acknowledgments

- Thanks to Dan Held, Nic Carter, and Rob Fox for reviewing earlier drafts.
- Thanks to Hasu, Murad Mahmudov, Vijay Boypati, Mart Bent, Pierre Rochard, Jameson Lopp, and many more for challenging my understanding of bitcoin.
- Thanks to Paul Stamets for pushing the boundaries of Mycology and inspiring me along the way. (the bitcoin community welcomes you)

Thanks to Dan Held.

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