CY18 Q4 October

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

Contents

Goals and Scope

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

History

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

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

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

Money Crypto vs. Tech Crypto

By Erik Torenberg

Posted in October, 2018

Crypto has a bit of a narrative problem.

When talking about Why Crypto Matters and where The Big Opportunity is, people often begin from different assumptions and starting points, and, more importantly, have a different end game in mind, which leads to confusion: investors are unclear what thesis they're applying to the market, newcomers struggle to follow along, and maximalists spend endless energy trying to convince one group to think like the other, without fully appreciating where they differ (or align!) on first principles.

Let me try to simplify by painting a (very broad) picture of the two main belief systems in the space:

One belief system maintains that the point of cryptocurrency is to redefine how money works by (re-)introducing Sound Money. Let's call this narrative "Money Crypto".

Another belief system holds that the real point is to redefine how the internet works by introducing Web 3.0. Let's call this narrative "Tech Crypto".

Others call these respective narratives "Bitcoin Maximalism" and "Ethereum Maximalism", but it's broader and more expansive than that.

While there's overlap between these belief systems, to be sure, they have different aims, different approaches, and different philosophical underpinnings – which leads to some of the confusion.

Money Crypto

Money Crypto believes that the goal of all this is the introduction of Sound Money – money with an iron-clad monetary policy that cannot be changed by governments, central-banks, or other entities.

With Sound Money, governments will be forced to behave responsibly because they are no longer able to borrow from tomorrow (via debt/inflation) to finance wars or fund short term political objectives at the expense of long term wealth.

Money Crypto believes that censorship resistant store of wealth is paramount. This may seem strange to us living in the U.S., where we trust our banks and governments (for now!), but much of the world doesn't have that luxury: People suffer from corrupt

governments, currency controls preventing people from covering capital, and currency inflation due to government instability.

Money Crypto believes, naturally, that Bitcoin is superior because it is an un-inflatable, disinflationary, censorship-resistant, fixed-supply asset that can't be shut down by any government and operates without any trusted-third parties.

The Bitcoin/Bitcoin Cash almost-civil-war over block size doesn't scare Money Crypto. On the contrary, it gives them more confidence: If it was so hard to change something as small as the block size, it will be nearly impossible to imagine changing something as monumental as money supply

Money Crypto believes that, of all currently existing cryptocurrencies, Bitcoin has the best chance of being sound money. It has the "immaculate conception" effect: an anonymous, uninvolved founder and no central entity; It's got the first-mover advantage; It has the greatest lindy effect; It has the highest market cap; Most liquidity; Most credible monetary policy and scarcity; Best censorship resistance; Best brand; Best durability; Best network effects, etc, etc, etc.

Money Crypto believes that we should treat cryptocurrencies as money – and not as the next app store or the next software platform that captures all of the VC dollars.

Money Crypto believes that the internet is a faulty analogy for studying the nature of money, and that we can instead learn more about the future of cryptocurrency from studying economic history and how monies have emerged over time.

What can we learn exactly? That whenever people control money, they create more of it — insidiously diluting existing money holders in the process.

Money Crypto believes that Ethereum is novel and interesting, but the value it creates (let alone captures!) will be orders of magnitudes smaller than the next money (Bitcoin). All the apps / dApps being built on top of Ethereum will create some value — but it won't make ETH, the token, a better money. Yes, Ethereum has many more developers, but Money Crypto believes 1 protocol developer is worth 10,000 app developers.

Money Crypto explicitly rejects the Utility Hypothesis, maintaining that digital money will be SOV first, not MOE first.

Value capture is insanely hard in decentralized realm, the logic goes. Indeed: If decentralized applications succeed at removing middlemen and rent seeking behavior — they won't create revenues, they will destroy them.

Money Crypto is specifically "Bitcoin, not blockchain". Nearly all Blockchain use cases are not merely unnecessary — they also make the application slower and more expensive.

Indeed: Satoshi used blockchain structure in an extremely specific and deliberate sacrifice of a massive amount of speed & cost in order for us to achieve sovereign level censorship resistance, trustlessness, and greater social scalability.

To summarize: Money Crypto believes The Future of Crypto isn't software — it's money.

Crypto isn't equity. It's not a website. It's not a company. And It's not social media network.

It's money.

Tech Crypto

Tech Crypto, on the other hand, believes we should study the history of the internet – rather than the history of money – to help us understand how cryptocurrencies will evolve, and how they will usher in the next epoch of the internet, web3.

The narrative goes something like this: Although the internet started as a decentralized and open system, it quickly became centralized and concentrated among 5 players — Google, Amazon, Apple, Facebook, and Microsoft — addicted users, controlled their attention, monetized through advertising, acquired those that compete, and shamelessly copied those who somehow survived.

Far from fulfilling its original vision of decentralizing control, web 2.0 has in fact created power centers that are orders of magnitude larger than anything that preceded the internet. Although the marginal cost of moving packets around on the internet is 0 – and despite the amazing economic gains and consumer surplus that web 2.0 has produced – the social costs have been significant: grotesque inequality, end of privacy, fake news, monopolies, filter bubbles, a threat to democracy, and more.

Tech Crypto believes that the internet will only have increasingly more of a say in how power and wealth is distributed, and fixing the incentives (via cryptonetworks) is one of the most important things we can do, along with enabling consumers to own and control their own data.

Had the token model for network development existed during web 2.0, things could have played out differently:

Tokens provide a way not only to define a protocol, but to bootstrap the operating expenses required to host it as a service.

Tokens power the economic incentives to enable distributed computation – compute, storage, bandwidth – at scale in a decentralized way.

Tech Crypto views tokens as the most salient innovation in human-coordination mechanisms since the invention joint stock corporation centuries ago. Before the joint stock company corporation, businesses had natural limitations. People owned the businesses in their entirety and passed them down to their offspring. There was no liquidity in equity, and therefore businesses could not raise capital.

The advent of joint stock corporations, and more recently publicly traded corporations, has produced incredible businesses that wouldn't have been possible otherwise. We've seen, however, the faults of those same systems:

The joint-stock equity industry model is inefficient at accounting for actual value creation behind online networks, as in, it only rewards employees – not users, contractors, or developers. Value of a share of stock is a function of profits. And profits reflect companies' ability to monetize data — not the actual worth of the service. When a company reaches a certain size their incentives become misaligned with their users and developers building on top of them.

Tokens also do something else which may enable the disruption of hitherto unbeatable network-effect businesses: they – in theory – incentivize orders of magnitude more people to contribute to the network. This includes all stakeholders — users, developers, contractors, speculators — not just employees. Instead of accruing value by ownership, like equity, network participants accrue value by improving underlying protocol, either by mining, validating, building on top of, or by using the service.

How do you create the next Facebook? Give millions of people upside in its success, the theory goes, instead of just a few hundred.

And it's not just tokens. Every aspect of blockchain infrastructure becomes a building block for the next developer looking to build something on top of it. This leads to compounding innovation, since every application leads to more possible applications. Just look at standards like ERC721 or 0x turning into memes, leading to more companies starting, which then become building blocks for creating more innovations on top of them.

In contrast, Web 2.0 naturally led to silos and consolidation. Tokens are the fuel that both incentivizes protocol maintenance and development, as well as guarantees enforcement of trust and openness.

Tech Crypto says the blockchain, using the crypto networks described above, will disintermediate all middlemen: Not just all of payments ($500B) but all banks, all social networks, marketplace operators, etc.

Tech Crypto, as you probably guessed, is more bullish on Ethereum. They see BTC as digital gold and Ethereum (or some other smart contract platforms) as the world's computer, and are eager to build millions of dApps on it.

Tech Crypto says In order for money to be money it needs to be used as money.

Tech Crypto compares blockchain to the early web - people said the web wouldn't scale either. That it was unnecessary. That it was a toy.

Tech Crypto says that software tends to rewrite the rutles of things it runs into – "software is eating the world" – and crypto is no different.

Tech Crypto says don't bet against developers.

Which Narrative is Right?

Tech Crypto and Money Crypto in some ways couldn't be more different – from their beliefs to their vibes. To quote Murad Mahmudov: "Tech Crypto is more gentle, touchy feely social justice-y positive vibe-y hippies. Money crypto is more carnivorous borderline annoying intense uncompromising right wing meat eaters."

And yet. It's too early to tell whether either or both of them are right - nor are they mutually exclusive. It's possible that both are right about the eventual of outcome but merely disagree about the order of operations. There are a lot of people in Tech Crypto who are sympathetic to the Money Crypto narrative: They believe that working to swing the pendulum back towards decentralization is vital, and that tokenization is a powerful mechanism to do so, but also that it's entirely possible that we haven't figured out token design yet and that it could be a money token like BTC that we all eventually use (or that there is some much more invisible token swapping thing or that it will be securitized equity style tokens that do it or something else.)

There are also factions that just wildly disagree. Some of Money Crypto believes that Tech Crypto applications will not accrue value, and that the near religious belief in tokens will dissipate when the ICO bubble pops. Some of Tech Crypto believes that the money problems are overstated (Quoting "Why Decentralization Matters ": "For example, it is sometimes said that the reason cryptonetwork advocates favor decentralization is to resist government censorship, or because of libertarian political views. These are not the main reasons decentralization is important".)

Ultimately, Money Crypto approaches this tech from a largely Austrian economics perspective, looking at at how monetary media have evolved over history and then trying to replicate those same characteristics in digital form (Saifedean Ammous' The Bitcoin Standard is the manifesto here). Tech crypto, on the other hand, thinks that those historical examples only go so far, because having money wrapped in software creates entirely new paradigms, opens up the design space, and potentially even

means that this time around, money will take a much different path than it has historically.

Some of these factions not only disagree, but also think the other as detrimental. Parts of Money Crypto believe that tech crypto is detrimental as it obfuscates the "real value" of crypto – Sound Money – and that ICOs distract developers from working on Bitcoin. There are parts of Tech Crypto that believe that the Money Crypto narrative – and the often aggressive and hostile nature – is turning people away from using or building on top of cryptocurrencies. 1 It's sort of like the great Slate Star Codex post about group infighting. Take Vegans and Paleo fans, for example. Rationally, you would want both the vegan and paleo people to work on getting people off, say, McDonald's because either diet is clearly an improvement.

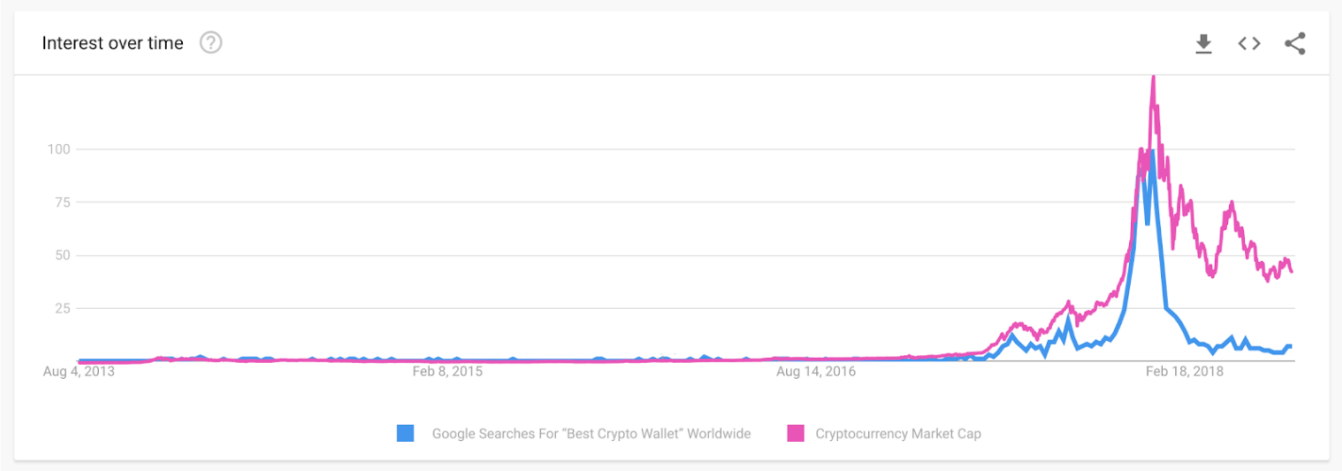
But, in practice, the human dynamics are such that they will not stop fighting with each other precisely because their viewpoints are so similar.

Sound familiar?

Similarly, I'd argue, any animosity between Money Crypto & Tech Crypto is better directed towards their common enemies (central banks, corrupt governments, tech monopolies, etc). I'd go further and say that both belief systems can benefit from each other's rise.

Without Money Crypto people helping make crypto a good form of currency, Tech Crypto can't accomplish its goal of letting people get paid for hosting/mining/participating because they need their currencies to be worth something for them to be compelling incentives.

And without Tech Crypto builders, Money Crypto people are climbing up a hill because having a new ecosystem around digital currencies will give them credibility and value. (See the graph below - when crypto value gets higher, more people get wallets. More people having wallets means more people can use dApps).



To be sure, these concepts – Money Crypto & Tech Crypto – could be classified any number of ways, but for the sake of clarity, we've excluded other, more granular factions. For example, there are many people who want to redefine how money works but via some mechanism other than Bitcoin – privacy coins, stable coins, etc. Similarly, there are many people who, beyond the internet, want to "decentralize all the things" from supply chains to automotive, from media to data – in both tech and governance. An upgraded web is part of this, but not the only part.

What's important to realize here is that not only can these narratives both exist, we may find that they ultimately leverage and further the other's chance of success.

Thanks to Mike Maples, Kyle Samani, Tony Sheng, Trent McConaghy, Nathaniel Whittemore, Taylor Pearlson, Dani Grant, Kevin Pan, Myles Snyder, Denis Nazarov, Arjun Balaji, Soona Amhaz, and Murad Mahmudov for their meaningful contributions to this piece.

Bitcoin Market-Value-to-Realized-Value (MVRV) Ratio

Introducing realized cap to BTC market cycle analysis

By Murad Mahmudov and David Puell

Posted October 1, 2018

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

Nic Carter from Castle Island Ventures (in a co-effort with Antoine Le Calvez from Blockchain.info) has recently presented his newly-termed concept of *realized cap* at Riga Baltic Honeybadger 2018 conference, inspired by some previous ideas of Pierre Rochard. Nic was kind enough to share some of his findings and data with us after the conference, and we wanted to delve into some analysis of the information available to us. For the purposes of this article, let's define a couple of terms:

Market value

Otherwise known as total market capitalization, it applies to Bitcoin if you were to multiply the latest available BTCUSD trading price on exchanges by the number of bitcoins mined thus far (currently standing at 17,299,787 BTC as of Oct. 1, 2018).

Realized value

Instead of counting all of the mined coins at equal, current price, the UTXOs are aggregated and assigned a price based on the BTCUSD market price at the time when said UTXOs last moved.

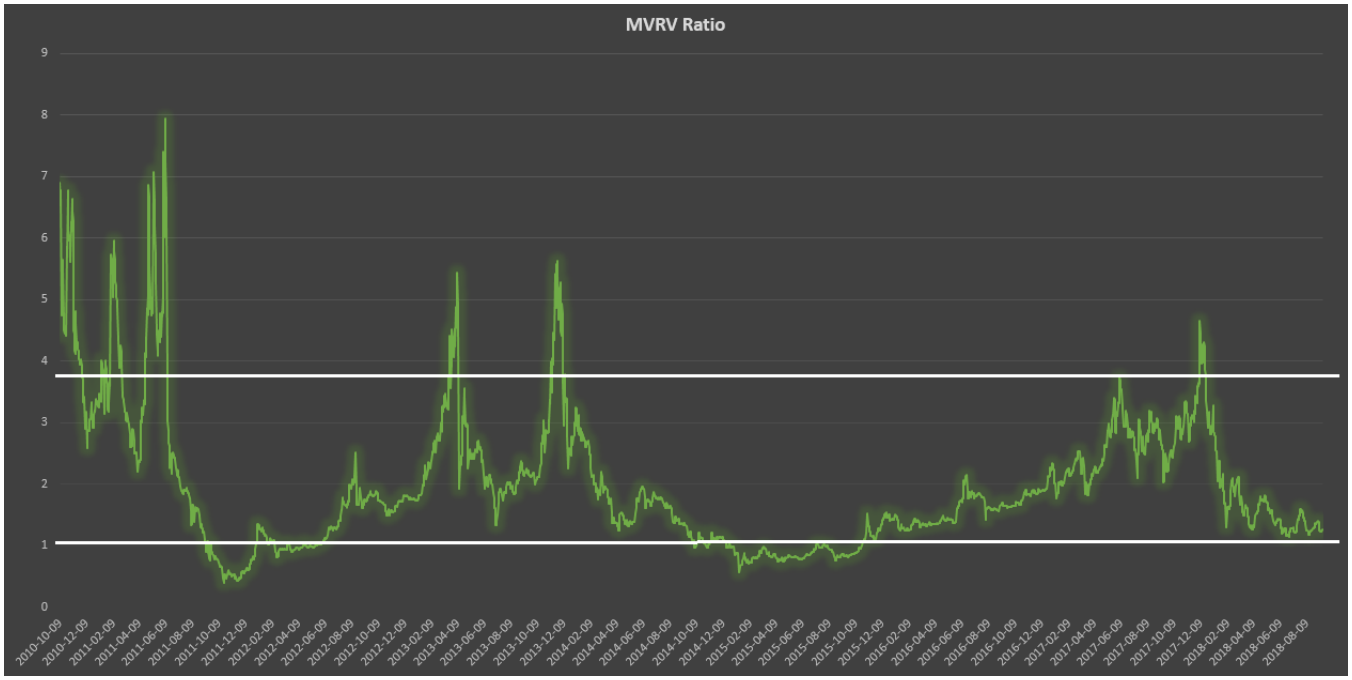
The Logic Behind Realized Value

Realized cap's effectiveness intuitively seems to adjust for two aspects of BTC's nature: (1) lost coins, and (2) coins used for hodling, establishing the collective psychological sum of entries when users began seeing Bitcoin's value and long-term potential. Realized cap seems to suggest the final layer of people's cumulative cost basis and, in recent history, the ultimate line of "center of mass" where 2017 strong buyers remain unrattled by short-term uncertainty.

One way of looking at realized value is that it helps us eliminate some of the lost, unused, unclaimed coins from our total value calculations. Another way is seeing it as an indicator of the sum of levels where groups of long-term, legit, buyer-hodlers entered into their Bitcoin positions, with local and immediate emotions and manias stripped out.

MVRV Ratio

MVRV is calculated by simply dividing market value by realized value on a daily basis (in this case from Oct. 9, 2010 to Sept. 14, 2018). This formula provides the following oscillator:



From this calculation, two historical thresholds emerge: 3.7, which denotes overvaluation, and 1, which denotes undervaluation. It is also interesting to see how MVRV evokes both the Mayer Multiple and Dmitry Kalichkin's NVT signal without the need for a moving average.

Market Dichotomy?

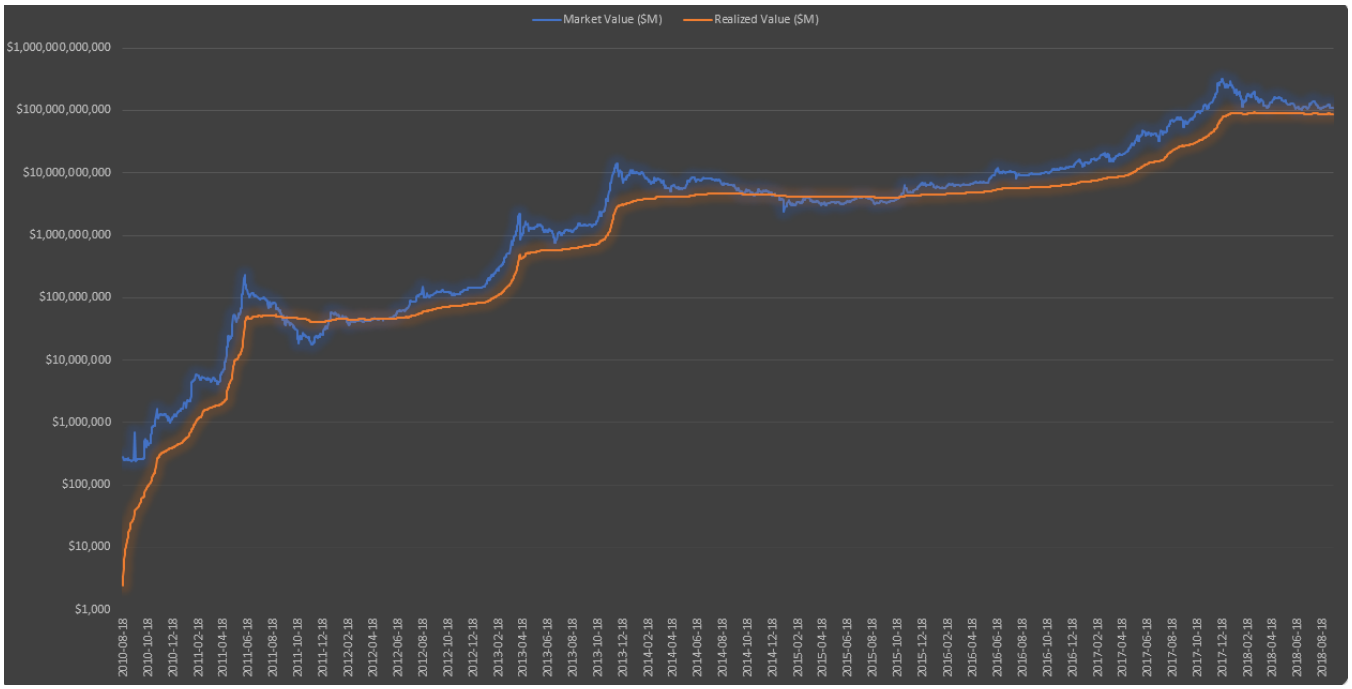
A theoretical framework for this ratio would echo a dichotomy that can be best expressed in the following:

1. Speculators vs. hodlers.
2. High time preference vs. low time preference (as argued by Saifedean Ammous in chapter 5 of *The Bitcoin Standard*).
3. Irrational exuberance vs. uncertainty acclimation (as argued by Jimmy Song in "The Antifragility of Bitcoin" presentation).

We believe that both market concepts and participants are crucial for Bitcoin's game theory and price action, since the booms seem to expand the network via an exuberant viral gossip mechanism that broadcasts the existence of Bitcoin to the world population; while the busts, in the long-run, seem to reward individuals who chose to delay short-term financial gratification in the search for sound money. This very dichotomy, in our opinion, also explains the relevance and effectiveness of MVRV ratio. Network value, to go back to Willy Woo's terminology, is to us *both* market value and realized value.

Similar to Woo's NVT principle, MVRV appears to track the interaction between the market actors that best describe the aforementioned dichotomy. It suggests the at times major divergence between price discovery at exchanges and the "sounder," more steady rise of unmoved coins—either lost or used for hodling.

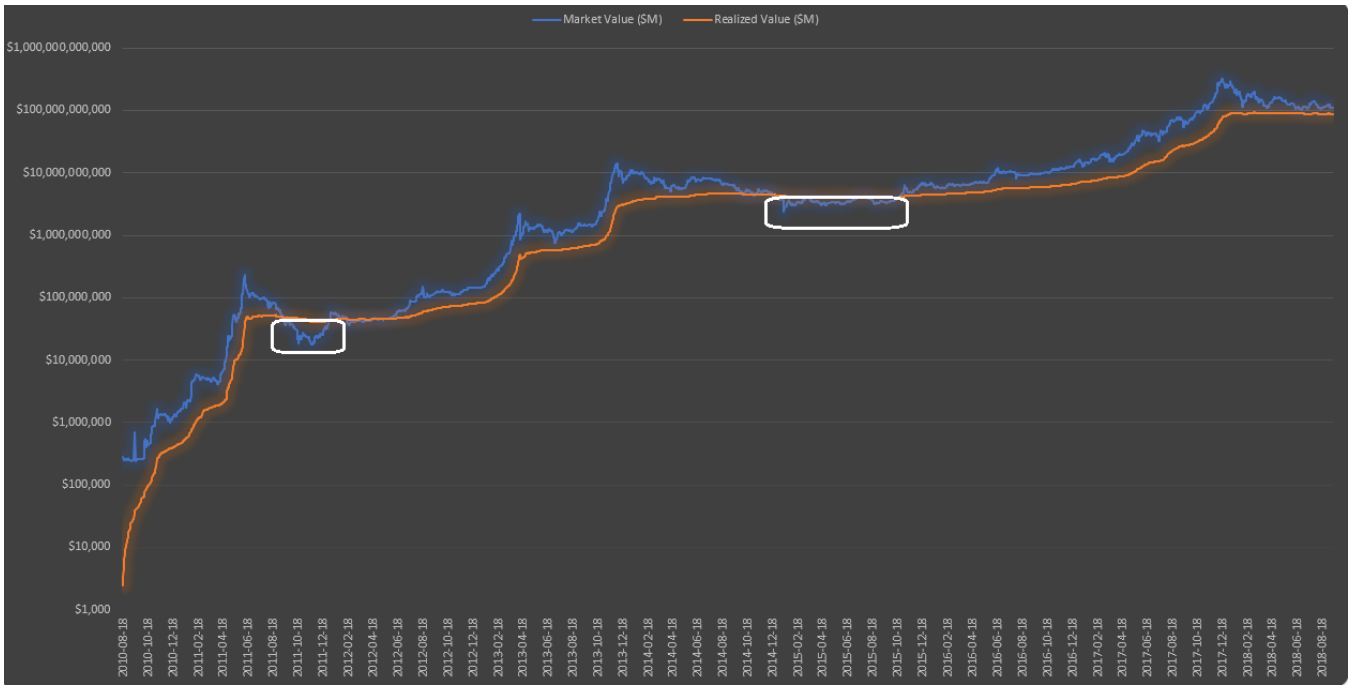
It is of particular interest whenever market value goes below a 1:1 ratio to realized value. We suggest that these periods account for both undervaluation and the capitulation-despondency stages of market psychology. Just as the upper levels of MVRV suggest the climax of euphoria, overshooting it's "fair" value at the peaks, price action as discovered at exchanges tends to undershoot beyond BTC's "real" value at the bottoms. Looking back at the past two Bitcoin bear cycles, we can say without a doubt that both occasions proved to be the most opportune periods to accumulate bitcoins.



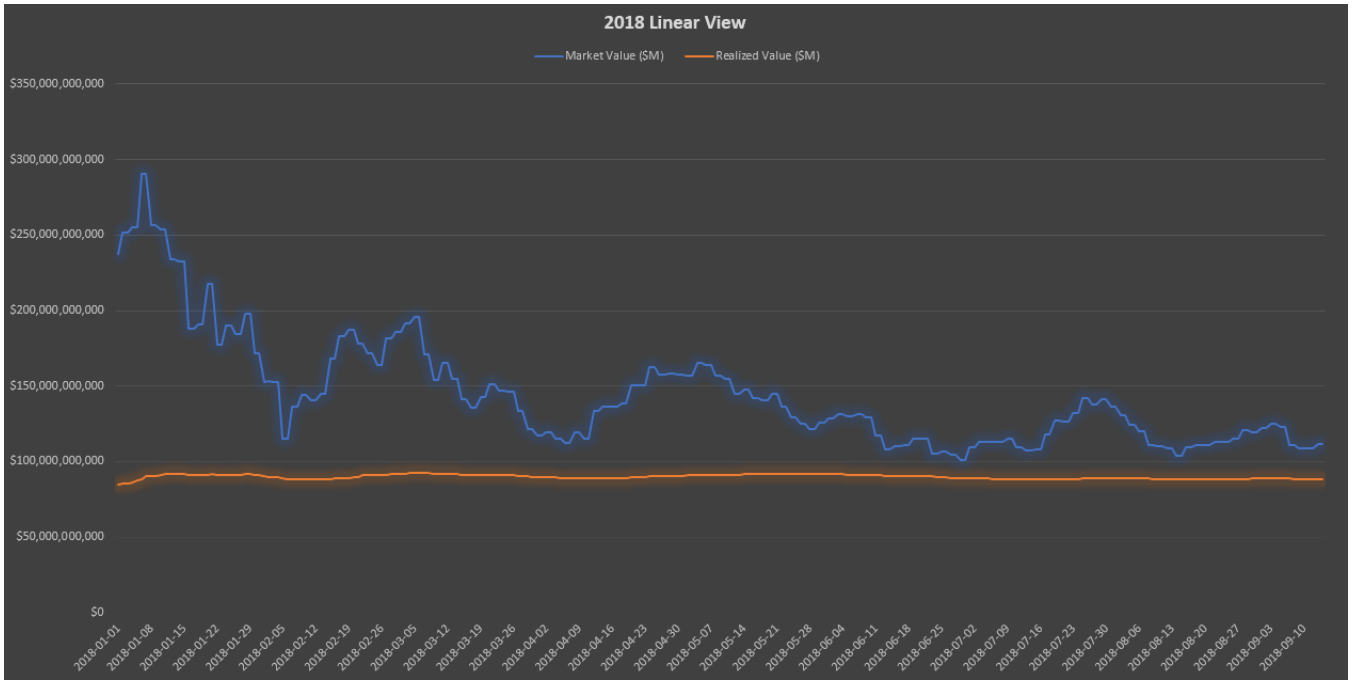
When plotted over the long run on a log chart, the realized value line of Bitcoin (orange above) is more similar to a stepwise function, with near-vertical moves upwards during peak months of bull market, then a prolonged period of horizontal flatness. That being said, each flatness level could be roughly interpreted as Bitcoin's newfound stable fair value threshold. The traditional market cap, however, is more sharply pronounced by the emotion of the crowds, namely excessive euphoria when market value sharply diverges upwards away from realized value, and, conversely, excessive fear when market value drops below realized value for a multi-month period.

Current Environment

Simply put, we expect market value to descend below realized value on a mid-term basis, which in turn would establish a structural gap between them, to be filled after an accumulation period of potentially as long as several months. The following chart displays the historical periods when accumulation in Bitcoin took place (which would be represented by MVRV ratio's descent below 1).



A zoomed-in linear version of the current environment gives us a clearer view of how market value remains overextended above realized value.



Some Caveats

As with any fundamental or technical indicator, we recommend using this particular tool with prudence. Some observations:

1. *Thresholds:* Going forward, as market cap decreases in volatility, we believe that the upper threshold of MVRV might not prove as reliable—as market cap overextends less and less above realized cap as time progresses. However, we expect the lower threshold to remain useful to detect Bitcoin's undervaluation in multi-month periods ripe for accumulation. This is to say that the saving power and the speculative power of Bitcoin will become, increasingly more and more, very closely intertwined.
2. *Precision:* MVRV ratio only provides a long-term perspective of BTC market cycles—specifically, to apply Wyckoffian terminology, distribution and accumulation phases.
3. _Technical methodology:_The use of MVRV as a momentum oscillator where the breakage of a trendline implies capitulation (similar to NVT signal or the Mayer Multiple) still comes into question. Thus, more conservatively, we provide two recommendations: (a) to analyze this indicator as a companion to other fundamental and technical tools; and (b) mostly use its thresholds for multi-yearly analysis; a diagnostics tool of Bitcoin's "hodling" health.
4. *Realized cap:* It is important as well to remember that realized cap may drop given a black-swan shock event where strong hands lose confidence in BTC. For this reason we recommend assessing market value and realized value both as a ratio and separately.

Acknowledgements

We would like to thank the following people, whose work and help was essential for this analysis:

1. Nic Carter and Antoine Le Calvez, for inventing the realized cap and providing us with invaluable data.
2. Pierre Rochard, whose initial idea was the starting point for the invention of realized cap.
3. Willy Woo and Dmitry Kalichkin, whose work on NVT and NVM has been deeply influential.
4. Saifedean Ammous and Jimmy Song, for providing crucial ideas in developing a theoretical framework for MVRV.

Sources and Data

1. Daily market value and realized value data provided by Nic Carter (Castle Island Ventures) and Antoine Le Calvez (Blockchain.info).
2. Ammous, Saifedean. *The Bitcoin Standard*. Hoboken: Wiley, 2018.
3. Song, Jimmy. "The Antifragility of Bitcoin." *Off-Chain with Jimmy Song* YouTubeChannel:https://www.youtube.com/watch?v=LYjUOFc0OMo

Bitcoin's Distribution was Fair

By Dan Held

Posted Oct 4, 2018

Foreword

As Bitcoin rises in popularity, and continues to challenge mainstream thought, there will be concerns around certain parameters of its existence. One of those is that the distribution of Bitcoin wasn't "fair," particularly in the earlier stages of network development. I'll dive into the timeline surrounding Bitcoin's launch, and provide a thorough debunking of unfair early distribution claims.

TL;DR—Satoshi set out to design the fairest system possible.

To enjoy this article in its fullest, I recommend playing this song then continue reading. If you like this music, please follow my playlist on Spotify.

Distribution

Premining is the mining or creation of a number of crypto coins before the cryptocurrency is launched to the public. Premining sometimes has a negative connotation due to the ability of private developers to privately mine and allocate a number coins to themselves before releasing the open source code of the currency to the public. This could lead to a feeling of lack of transparency in the digital currency offered to the public.

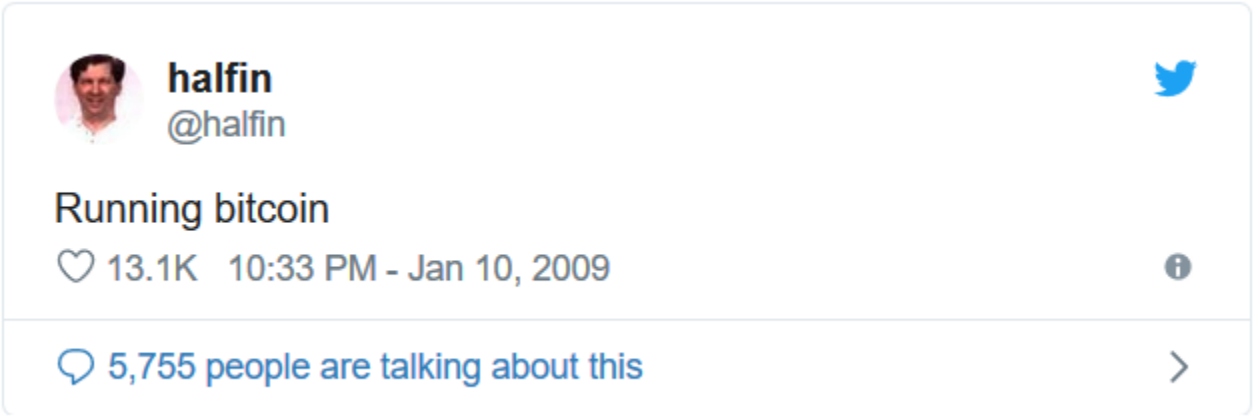
Satoshi didn't premine. Satoshi gave everyone a two month heads up before mining the Genesis block, reaching out to the only other people who would possibly be interested in experimenting with a sovereign digital currency at the time, the cypherpunks (via public e-mail list). The whitepaper was published on October 31, 2008, then Bitcoin 0.1 software was released on January 9, 2009.

The Genesis Block alone was minted earlier January 3, 2009. It was unlike all other blocks (no previous block to reference) and required custom code to mine it. Satoshi included a message in the Genesis Block as a "proof of no premine."

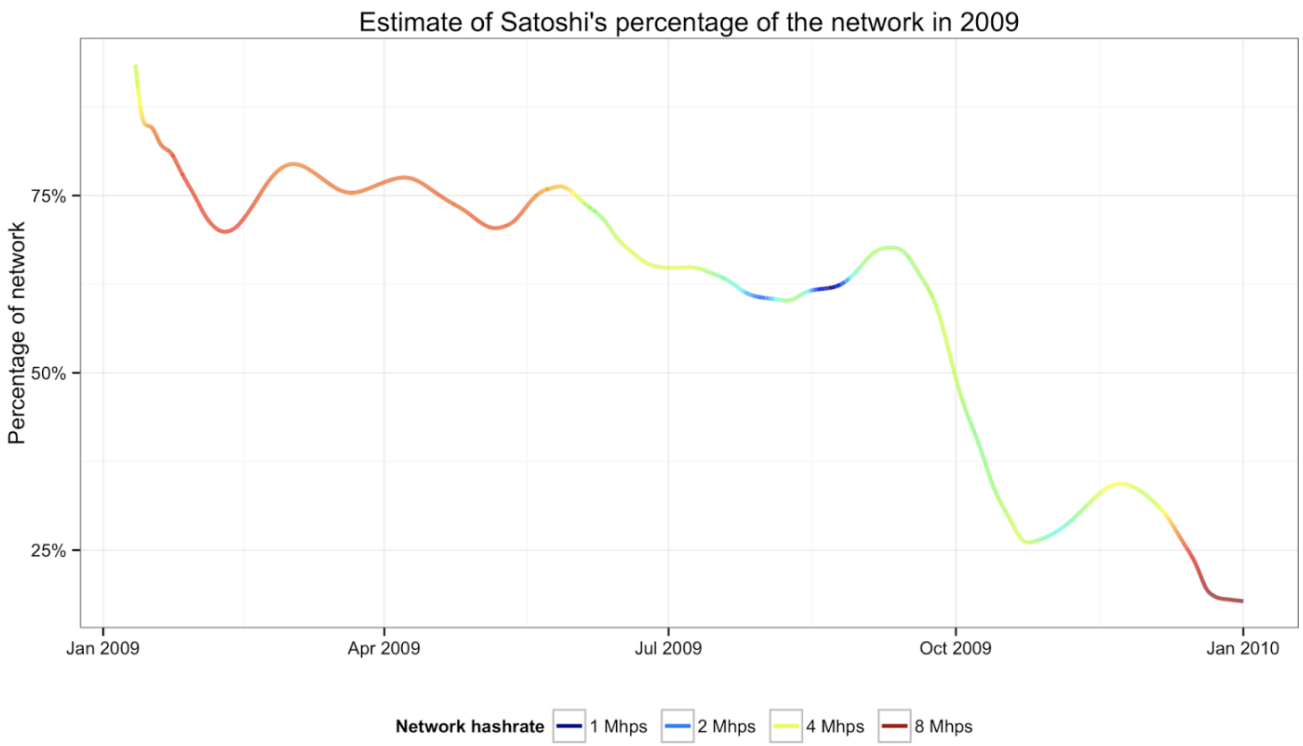
"The Times 03/Jan/2009 Chancellor on brink of second bailout for banks"-Genesis Block

Timestamps for subsequent blocks indicate that Nakamoto did not try to mine all the early blocks solely for himself. Before Satoshi's invention, the concept of pre-mining didn't exist. To be this prescient demonstrated incredible maturity.

The code to mine bitcoin was available on the day Satoshi began mining (other than the special purpose Genesis Block). It even had a 1-click miner in there so it was incredibly easy. Once the code was released, several individuals started mining—we know for a fact that Hal Finney was mining one day after the initial launch. Satoshi definitely wasn't mining alone in the early days, granted the number participating was slim.



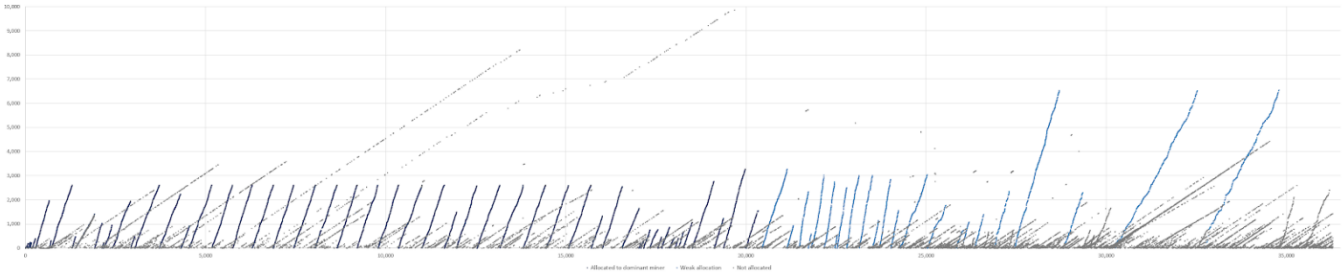
For the first year of Bitcoin's existence, Satoshi and other miners couldn't muster enough hashrate to mine more than 144 blocks/day and trigger an upwards difficulty adjustment. Satoshi mined because the network required a miner, he turned them off when there was a stable network that didn't need his mining power. He reduced his % of the hashrate in a slow and steady manner. The Satoshi fingerprinted mining carefully balanced the hashrate of the cluster, with the goal of historically viewable well-meaning intentions. Satoshi initially followed a plan of reducing the hashrate by 1.7 Mhps every five months, but a month after the second such drop abandoned this method in favour of a continuously decreasing hashrate.



http://organofcorti.blogspot.com/2014/08/167-satoshis-hashrate.html

How much did Satoshi mine? Other than a few coins (some still circulating), it's not empirically knowable how many he owned, but we can assign a high probability that he was the miner who minted close to ~ 700,000. BitMEX reviewed the original estimate made by Sergio Demian Lerner where he discovered that Satoshi's miner had a "fingerprint" (the increase in the ExtraNonce value in the block can potentially be used to link different blocks to the same miner). BitMEX built on his analysis and concluded that although the evidence is far less robust than many assume, there is reasonable evidence that a single dominant miner in 2009 could have generated around 700,000 bitcoin.

"Although there is strong evidence of a dominant miner in 2009, we think the evidence is far less robust than many have assumed. Although a picture is worth a thousand words, sometimes pictures can be a little misleading. Even if one is convinced, the evidence only supports the claim that the dominant miner may have generated significantly less than a million bitcoin in our view. Perhaps 600,000 to 700,000 bitcoin is a better estimate."—BitMEX

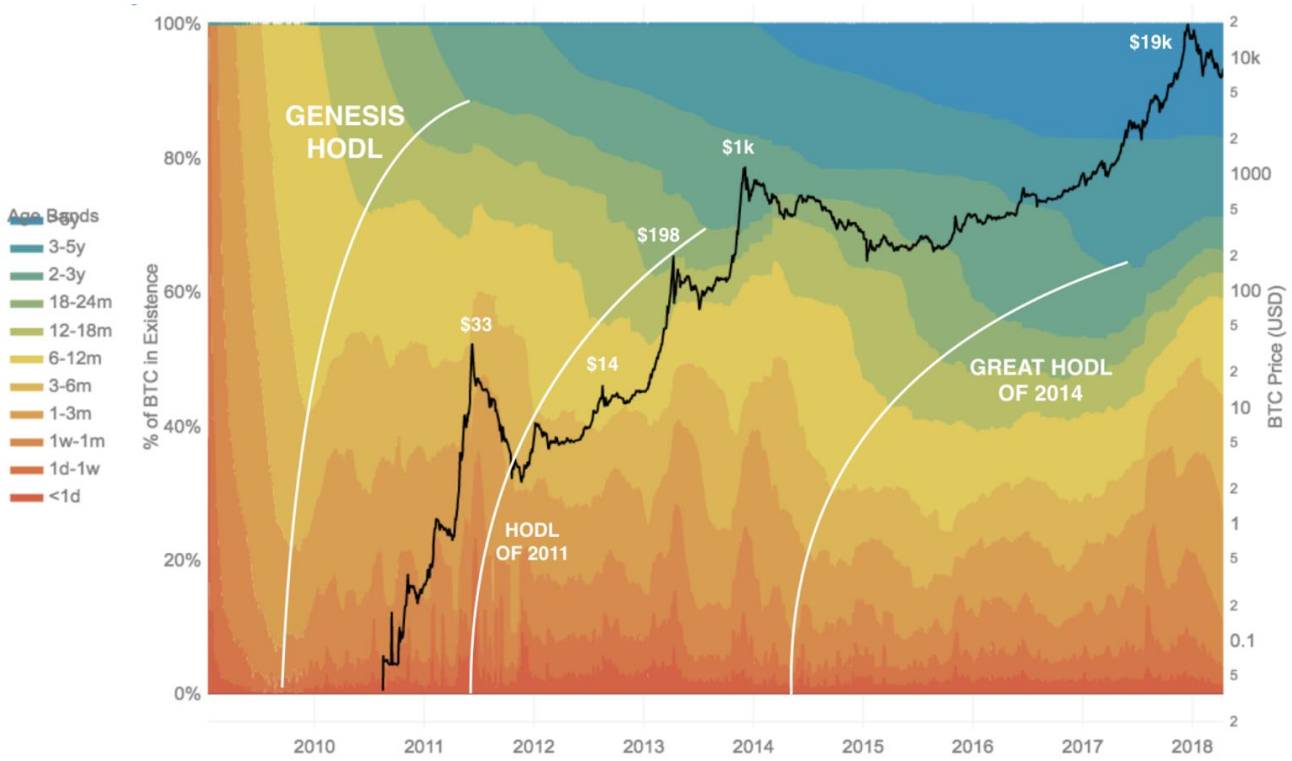


Bitcoin blocks mined in 2009 — Allocation to the dominant miner — ExtraNonce value (y-axis) vs block height (axis)

Bitcoin's market cap was ~ $0 for nearly a year and a half. Miners were wasting money on hardware and electricity to mine, with no guarantee that the Bitcoins they received would ever have value. In fact, "faucets" were set up to freely distribute Bitcoins in order to "seed" adoption (ex the 10k btc faucet set up by Gavin and other Bitcoiners who donated funds). The first recorded exchange of Bitcoin for "real world" value occurred on May 22, 2010, now known as Bitcoin Pizza Day, where Laszlo Hanyecz agreed to pay 10,000 Bitcoins for two delivered Papa John's pizzas. He went on to do this trade 2 more times, maximizing the dispersion of his Bitcoins.

"It might make sense just to get some in case it catches on. If enough people think the same way, that becomes a self fulfilling prophecy."—Satoshi Nakamoto

The early pioneers were the ones crazy enough to take the financial, temporal and social risks to participate in the Bitcoin project, keeping it alive and acting as arbiters of the system in its early days. Nearly all lost or sold all of their Bitcoins as evidenced by this analysis done by Dhruv Bansal



With each of those boom/bust cycles we've seen Bitcoin redistributed from old hodlers to new hodlers via selling, decreasing the Gini Coefficient. In 2017 alone, we saw 15% of all BTC move out of old hodler hands.

The theoretical total number of bitcoins, slightly less than 21 million, should not be confused with the total spendable supply. The total spendable supply is always lower than the theoretical total supply, and is subject to accidental loss, willful destruction, and technical peculiarities.

"Ten years ago cryptographers and HCI experts created the ultimate experiment to see how well human beings could hold onto long-lived secret keys. We structured the experiment so participants would lose hundreds or thousands of dollars if they failed. The results of that experiment have not been pretty."—Some Cryptographer on Twitter

There are many stories of people losing BTC in large amounts—especially in the early days—when BTC wasn't worth much and was easily forgotten on an old hard-drive, USB memory stick, even a scrap of paper. Coins which remain unspent for >5 years have a high likelihood to be lost forever. Despite the richness of blockchain data, it's extremely difficult to measure how much cryptocurrency is truly lost, as lost coins leave no trace in the blockchain. The problem is that so much BTC which is not lost looks exactly the same on the blockchain.

"The study of lost bitcoin is geology masquerading as data science."—Dhruv Bansal

Unchained Capital did a great analysis of lost coins, and found that bitcoin loss occurred over two distinct "cryptogeologic" eras: Systemic (earlier miners, and Incremental loss: (coins lost by individual users gradually over time). Their estimate: 2.78–3.79M BTC lost which aligns with another more sophisticated analysis done by Chainalysis.

"Lost coins only make everyone else's coins worth slightly more. Think of it as a donation to everyone."—Satoshi Nakamoto

From private key management mistakes, to scams and exchange hacks, to resisting selling temptation, early HODLers SURVIVED. In compensation for that risk, they absolutely deserve the value appreciation.

Some argue Bitcoin's distribution is analogous to a Ponzi scheme, but it's nothing like one. The definition of a Ponzi Scheme: "a fraudulent investing scam promising high rates of return with little risk to investors. The Ponzi scheme generates returns for older investors by acquiring new investors." It isn't one for the following reasons:

Transparency

Absolutely nothing about Bitcoin is a secret. It's open source, anyone can review the code, anyone can contribute to the code, anyone can run the software voluntarily and participate in the network, and anyone can use the network without permission. The entire history of all Bitcoin transactions is visible to anyone in the world too. It's the total opposite of a fraudulent investing scam, which is shrouded in vague promises of high returns with capital inflows and outflows that are kept in a secret ledger.

Returns

The Bitcoin whitepaper never mentions an investment or promising high returns. In a Ponzi scheme, the value for early investors rely solely on new entrants coming in with fresh capital, and their earnings/dividends come directly from this capital. With Bitcoin, the opposite is true. Most early Bitcoiners lost or sold their Bitcoin. Bitcoiners are human, they make human mistakes and have human needs (buying a house).

"Bitcoins have no dividend or potential future dividend, therefore not like a stock. More like a collectible or commodity."—Satoshi Nakamoto

Usage

The market's determination of what one Bitcoin is worth has nothing to do with greater fools getting in the system, but an after effect of its true value proposition, one that it already had even when it was worth nothing.

Conclusion

Satoshi was a person like any other, not some infallible being. This was the fairest distribution he could have come up with given what he was building/timing/audience. It's intellectually dishonest to compare Satoshi's early mining of Bitcoin at a loss, with premining of an ICO with a positive market value (or expected positive market value).

"Bitcoin benefited from an extremely rare set of circumstances. Because it launched in a world where digital cash had no established value, they circulated freely. That can't be recaptured today since everyone expects coins to have value. Not only was it fair, but it was historically unique in its fairness. The immaculate conception."Nic Carter

Satoshi wanted to signal to everyone that Bitcoin wasn't a scam. The conservative deescalation of his mining contributions, his departure from the community, never spending any of his coins, nor using his influence for any purpose, shows that he wanted the world to make up their own mind about his project and judge it on its own terms.

Unlike every other founder in history, Satoshi never cashed out.

Blockchain Is a Semantic Wasteland

Why haven't we abandoned it?

By Nic Carter

Posted October 5, 2018

Credit: Bigmouse108/iStock/Getty Images Plus

"Blockchain" this, "blockchain" that. It's a concept so momentous that it has even managed to shed its article. Proponents don't speak of "the" blockchain or "a" blockchain. Instead, they reverently preach Blockchain: the solution to all enterprise needs (in particular, supply chain management). The brute, unassailable, self-evident concept has disrupted not only the rules of commerce but those of grammar. Question it and you'll be exposed as a hopeless rube and a Luddite. Use it sincerely and you'll be lumped in with the hype men and techno-utopians.

It's impossible to avoid. Ads for IBM blare promises about revolutionizing tomato-tracking with blockchain. The U.K. finance minister recently asserted that blockchain may be a solution to Britain's Brexit woes. At a recent conference held by Ripple, former U.S. President Bill Clinton said of blockchain, "the permutations and possibilities are staggeringly great."

The word "blockchain" is satire-resistant. It's such an obvious target that it's no longer funny, and blockchain proponents are almost totally immune to ridicule. Nothing can check their indefatigable enthusiasm: There are press releases to be written, conferences to attend, and corporate R&D dollars to waste. Blockchain represents both the glittering future and the dismal present—almost all touted use cases are obvious nonsense.

The ICO mania of 2015–2017 that is now unwinding was premised, in large part, on the ability of blockchains to disrupt markets. In simpler terms, the idea was to Uber-ize every conceivable service and replace the intermediary with a magic database detailing who is doing favors for whom. Some of those pitches invoked trillion-dollar (yes, trillion with a T) total addressable markets.

Today's soulless corporate blockchains and opportunistic, ICO-based blockchains have both endured scorn and ridicule. Yet the term persists, an empty semantic husk, kept alive by a thousand press releases, conveying as little meaning as possible. The term is used to refer simultaneously to projects, structures, and databases that have virtually nothing in common. As a consequence, attempts to define it are usually hopeless failures.

Here, I'll try to explain the origin of "blockchain" and what we should do about it.

Where did "blockchain" come from, anyway?

Most histories of the term "blockchain" will mention that Satoshi Nakamoto created the first one. Except, that's not accurate. Nakamoto never referred to bitcoin as a blockchain, calling it instead a "chain of hash-based proof-of-work," a "chain of blocks," and even a "timechain" (in an early comment within the original codebase). Imagine: We were so close to living in a world of **"**enterprise timechains" and "strawberries-on-the-timechain."

Nakamoto was careful to emphasize that the chain was a set of proofs of work, each linked to the hash of its parent. (See for yourself!) The proof of work is absolutely essential to the concept. It is proof that anyone proposing a block has, well, worked for it. It enables the system to achieve Sybil resistance and to come to convergence (the longest chain—under the same ruleset—is the correct history, by definition) without any single arbitrator.

This data structure, with its inclusion of hashes of previous blocks, ensures that the past is preserved and the database is consistent. Replicating the database to every node in the network ensures that it can't be shut down or altered unilaterally.

The reason "blockchain" is such seductive marketing… is the subtle implication that the data structure alone—absent proof of work or open validation—could convey the same benefits as bitcoin.

The entire system was built with an adversarial context in mind. Hostile governments had shut down all previous attempts at e-cash. They certainly would have shut down bitcoin if they could have. Thus, it was built for a purpose. To clarify: Nakamoto may have created the first *popular, widely used* linked-list structure—not the first of its kind—but the innovation was in merging that linked list with the computational hardness of adding new entries to the chain.

Does this sound like what any of the enterprise blockchains are trying to accomplish? Of course not. There is no shadowy organization dedicated to forging strawberry provenance records that might seek to interfere with IBM's supply-chain blockchain. Thus, IBM's blockchain does not need to be built to the same standard as bitcoin. The kinds of records preserved on enterprise blockchains do not need the kinds of protections that Nakamoto consensus ensures. They do not need or want open validator sets. Some trusted organization could just vouch for the database, or a consortium of interested parties could share records between them.

For more on the failures of private blockchains, I recommend this post from a reformed private blockchain consultant.

Why is the term so popular?

From what I can tell, people witnessed the success of bitcoin—which relies in part on an ersatz, expensive database—and wanted to generalize it to other uses. Even early bitcoin developer Hal Finney mused about disaggregating the data structure from the monetary system.

It also might be possible to refactor and restructure Bitcoin to separate out the key new idea, a decentralized, global, irreversible transaction database. Such a functionality might be useful for other purposes. Once it exists, using it to record monetary transfers would be a sort of side effet and might be harder to shut down. — Hal Finney in his January 24, 2009 *Cryptography Mailing list*

However, to the best of our knowledge, these systems only really work if the reward is internal—that is, if well-behaved validation is rewarded with the "native" token. If bitcoin miners were paid in U.S. dollars, they wouldn't necessarily have any incentive to mine on top of the longest chain. The value of their hardware depends on the continuing existence and flourishing of the chain they're building on top of. But

private, permissioned, or enterprise blockchains do not have native currencies nor do they issue monetary units to validators, as the validator set is permissioned and thus has Sybil resistance and good behavior built in by design.

“Blockchain” is such seductive marketing, I believe, because the data structure alone—absent proof of work or open validation—could convey the same benefits as bitcoin without the token or costly anti-Sybil protection.

Patri Friedman put it well in a tweet:

Bitcoin is a monolith that colors the way investors and corporate R&D offices think about similar projects. Would Ripple have been as popular without bitcoin having been invented? What about Corda and Hyperledger? Litecoin? ICOs generally? Ethereum? It is hard to even imagine the alternate history, but I suspect the answer is no in all cases. Bitcoin is a juggernaut that carried with it a set of assumptions that were ported over to projects with a passing resemblance, rightly or wrongly.

Consequently, I would be suspicious of anyone who routinely uses “blockchain,” especially if they are trying to sell you something. Overuse of the term, especially in a general context and without qualifiers, most likely reveals one of three things about a person:

- They are well-meaning but forced by convention to use subpar linguistic tools.
- They are a bit muddled and trying to mask their ignorance with technobabble.
- They are trying to posture as an expert in an industry which realistically has no experts.

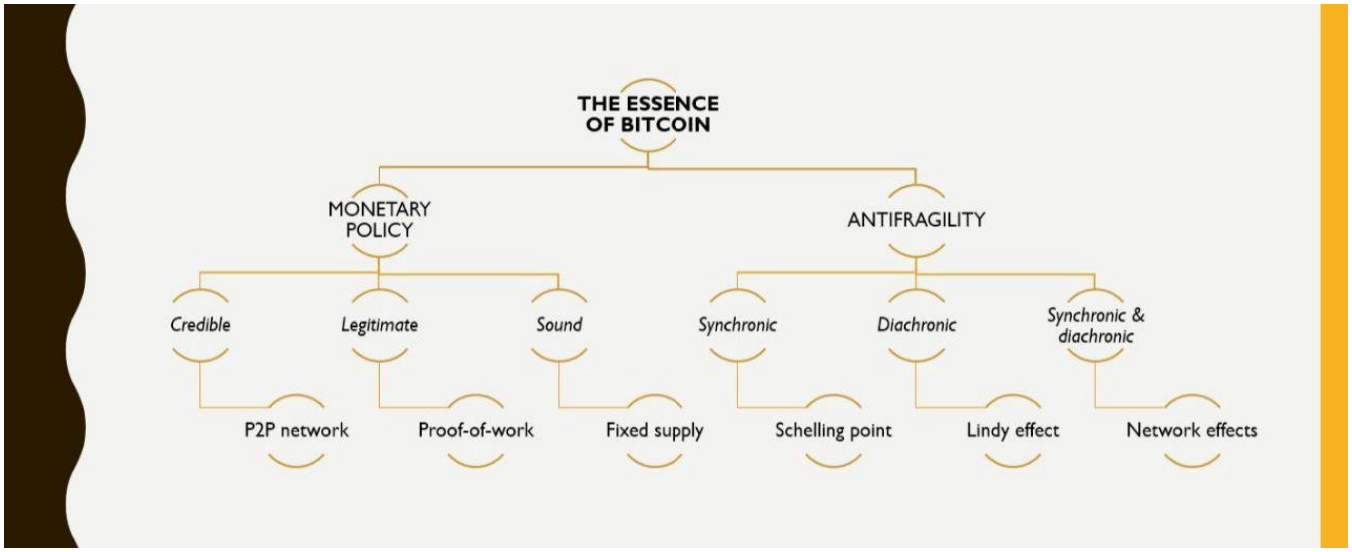
I firmly believe the misuse of the term traces back to a desire to create (or market) systems that are intended to be bitcoin-like without the unsavory bits. That, however, misses the point: Bitcoin's blockchain is just a part of it, not its essence.

Bitcoin and its blockchain

Referring to bitcoin as a blockchain is like referring to a car as a transmission. A transmission is a key element of the system, but it doesn't represent it in totality. Blockchain is a metonymy—a part used to refer to the whole. There's nothing wrong with that, intrinsically. The conceptual tangle comes when one decides that the blockchain is bitcoin's essence and is owed credit for its success.

Bitcoin relies on a linked list, indeed. But it also relies on a peer-to-peer (P2P) network, an open source and leaderless project, a replicated database, a self-supporting incentive system, a heaviest chain consensus rule, and a proof-of-work scheme that gives block proposals unforgeable costliness. (Unforgeable costliness in simple terms: It's impossible to fake a block submission; you would have to have allocated a good chunk of computing power, or energy, to the task. It is therefore hard to create new bitcoins but easy for anyone to verify that you worked hard at it.)

These inputs combine nicely to create a system that has certain qualities: provable scarcity, an ability to be audited, tamper-resistance, fair-ish distribution, almost perfect supply inelasticity (rising the price does not—cannot—cause production to accelerate), free participation (no one can stop you from broadcasting a bitcoin transaction), and so on. These qualities make bitcoin a unique relative to, say, Paypal or Visa. They are its differentiators. Without the P2P nature, the open-source collaboration, the voluntarist developers, and, crucially, the proof of work block proposal method, bitcoin would not exist. The below chart, created by David Puell based on ideas from Pierre Rochard, is an attempt to capture bitcoin's essence. Notice that the chain of blocks, while necessary to make the system work, is not sufficient on its own. Bitcoin relies on more.



David Puell's laudable attempt to characterize bitcoin's essence in one chart.

I can't tell you exactly what the essence of bitcoin is, but to limit it to a chain of blocks is reductionist in the extreme. The soul of bitcoin is not the blockchain. But if you pull the blockchain out of bitcoin, you get something rather empty.

Why rail against "blockchain"?

I believe better conceptual frameworks will lead to better outcomes. Author George Orwell believed that the words we use directly affect the way we see the world. He even intimated that scrubbing words from popular usage could eliminate their referents, the very concepts they sought to represent:

The purpose of Newspeak was not only to provide a medium of expression for the world-view and mental habits proper to the devotees of IngSoc, but to make all other modes of thought impossible. It was intended that when Newspeak had been adopted once and for all and Oldspeak forgotten, a heretical thought—that is, a thought diverging from the principles of IngSoc—should be literally unthinkable, at least so far as thought is dependent on words.

Eliminate the word "freedom" from popular use and you'll eliminate the desire for freedom entirely, so the theory goes. Additionally, Orwell strongly felt that sloppy language was indicative of muddled thought and used as a way to sneak indefensible assertions past an unwitting reader.

My point here is that in elevating the linked list to the exalted status of "blockchain," we overrate it. In insinuating that bitcoin is just a blockchain or simply the origin of the more interesting underlying technology, we do bitcoin a disservice. By constructing the blockchain artifice in popular consciousness, we enable sloppiness of thought and do away with rigor. "Blockchain" dilutes the importance of a tremendously important and valuable innovation—a trust-minimized monetary

system—and abases it by putting it to work to generate efficiencies, real or imagined, in enterprise supply chain management.

The path forward requires honesty

To the permissioned or enterprise blockchainers: Be honest about what you're building. If you're building a database controlled by a consortium of pre-permissioned entities, don't claim or imply it will have similar reliability characteristics to systems designed to live in far more adversarial environments. Imagine how you would market your system had bitcoin not been invented.

Let public blockchains be. You aren't competing with them. Your systems have totally different goals. If you do want to persist with the blockchain moniker, I encourage you to very carefully define what you mean by "blockchain," and be sure to distinguish your system from open, public blockchains. Lastly, for god's sake, give "blockchain" back its article (refer to "a" or "the" blockchain, please).

To the computer scientists: Stop mocking nontechnical people for using "blockchain." You're missing the point. They aren't really referring to the data structure, so it's beside the point to say, "Just use MySQL." "Blockchain," for better or for worse (definitely for worse) has become a term of art that is typically used to refer to the whole system—economic and social—rather than just the data structure.

To regulators: Please do not try to define "blockchain" or create blockchain regulation. You will fail, not due to your lack of astuteness but because the term "blockchain" is so semantically dispersed as to be undefinable. Definitions need to be specific and useful and also general enough to encompass all of the members of the set. However, these tensions tear "blockchain" apart. It is used too generally to be useful.

@prestonjbyrne Florida proposed my favorite definition of "blockchain", which may or may not be pretty much everything or nothing. —-
@zackvoell](https://twitter.com/zackvoell/)

Instead, disaggregate. Recognize that legislation covering cryptocurrency probably cannot cover security tokens, "utility tokens," and permissioned blockchains too. Private or enterprise blockchains aren't just "bitcoin in a suit"—they're totally different. The two really have nothing in common.

To everyone else: Please join me in spurning the use of "blockchain" at every opportunity. Let's try and devise new terms that are specific enough to be useful and do justice to their referents. I currently use "public blockchain" to describe permissionless, open networks like bitcoin and Ethereum, but I would love to use a different term that doesn't rely on the b-word. If you do insist on using it, I like Peter Todd's definition best: "A blockchain is a chain of blocks."

Using it in a minimalist, direct way removes some of its conceptual weight. This eliminates its ability to implicitly promise amazing consistency, reliability, and uptime. The more honest your definition of "blockchain," the less it lends itself to exciting press releases. The blockchain, in Todd's definition, is really just a way to arrange data. And that is supremely unsatisfying given how it's used today.

If you want to read more about disaggregating these systems, I recommend *Distributed Ledger Technology Systems: A Conceptual Framework*, published by an interdisciplinary set of practitioners and academics under the aegis of the Cambridge Centre for Alternative Finance.

I believe that in five or 10 years, we will look back at the popularity of "blockchain" and be slightly embarrassed.

Canny readers will notice that I co-founded a firm that invests in blockchain startups. This is true. I am humiliated. But our use of the term is a matter of practical reality. The term has proliferated widely enough to become a Schelling point—an easy meeting place where technologists and allocators can communicate. Out of convenience, and so that we are understood, we use the term. But we'd love to abandon it. It encompasses many distinct concepts, some of which we love and some of which we hold in contempt.

I believe that in five or 10 years, we will look back at the popularity of "blockchain" and be slightly embarrassed. The term will seem as archaic as "surfing the world wide

web" or using the "information superhighway." Consider this an open solicitation for replacements to the term. Let's move on.

Powered by Lightning; Programmable Money—Part 1

A quick primer on the Lightning Network and how it is making money programmable.

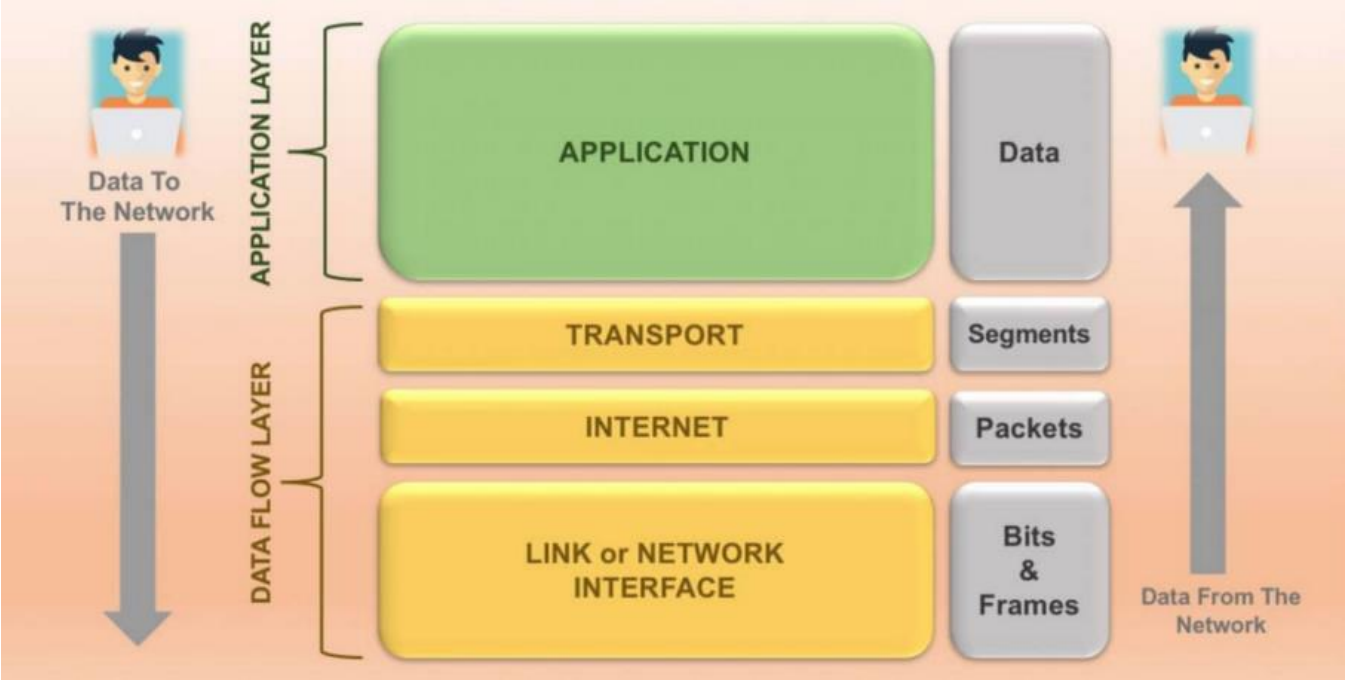
JP Thor [₿ ⚡]

Oct 6, 2018

- **Part 1—Programmable Money**
- Part 2— Using the LN as an individual
- Part 3— Using the LN as a business
- Part 4— Using the LN as a country
- Part 5— When the world is powered by LN

The Layers of the Internet

Bitcoin is emerging as a multi-layer value-transfer protocol, with different layers serving different needs and being used for different things. To understand this, we need to look at the Internet Model, which is a conceptual model around the four layers of the internet; Application, Transport, Internet and Network.



The Internet Model. Source: Stemjar

The Four Layers in Use

When users of the internet send data between each other (you and a website's server), the data transfer takes place across the four layers. Firstly the data is collected from the sending user at the application layer (the website's interface), which uses the underlying APIs to transport encrypted data packets via https (hopefully) to the server. These data packets are routed via the internet's infrastructure, which are essentially bits of information streamed across a high-speed link between servers. The data is acted upon (updating or changing state on the server), and the reverse in the download of updated information back to you.

Most likely the server's database is backed up on a schedule (such as iCloud or any of Google's services), and the changed state is replicated across other servers.

The end result is that you transferred data to and from another internet user (the server) directly, which was done in less than a few seconds and only you and the server knew about it. At some point later the changed data was backed-up across other servers. Overall, the user experience would have met our expectations, and the final data was safely backed up.

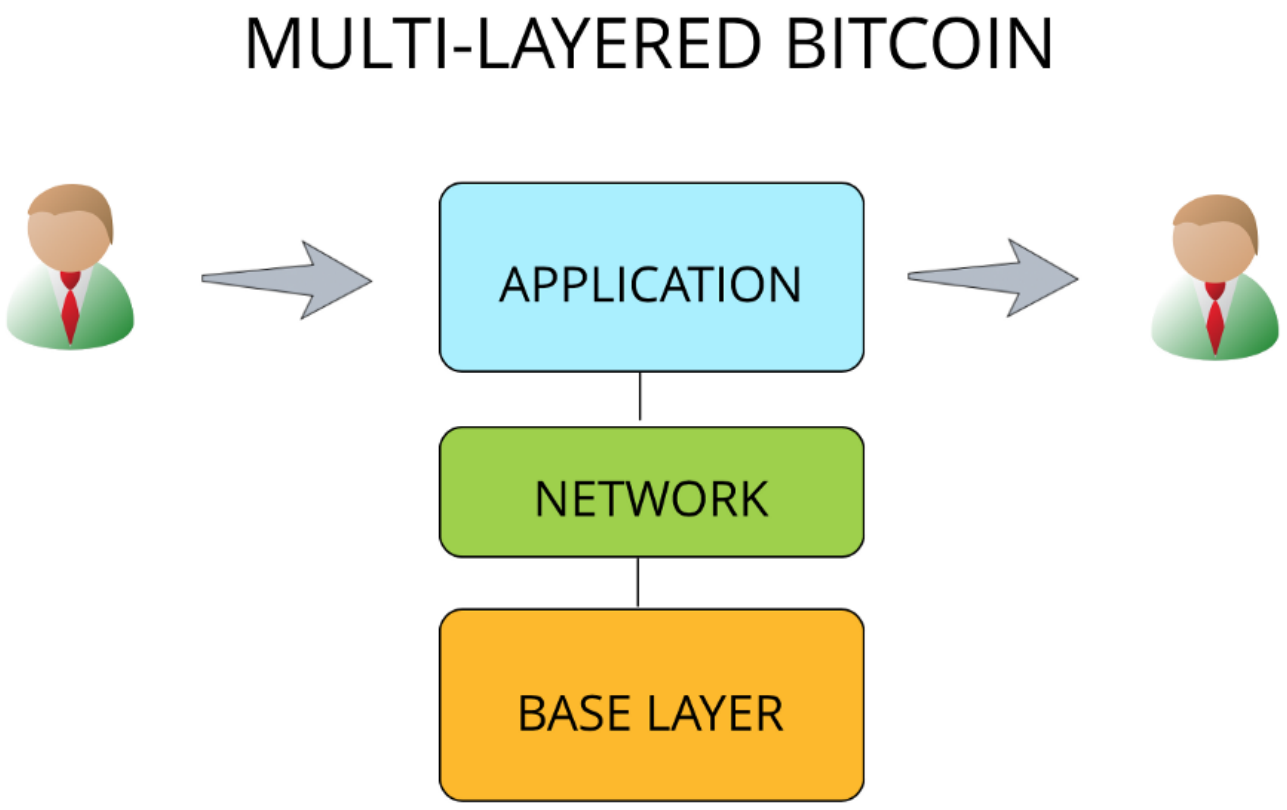
Before the internet as we know it, users would connect directly with each other at the networking layer. It was not possible to simply "go to a website". Indeed the internet that we know of today is mostly thanks to the Application Layer and its micro-services, APIs and browser-side processing.

The Layers of Bitcoin

A multi-layered Bitcoin is no different from a conceptual point of view. The base layer is the chain of blocks containing the immutable transaction graph, the “Layer 1”. This layer is completely public and everyone can view and validate the entire history of the database. This layer defines and secures what Bitcoin is.

Bitcoin Core is part of the network layer, allowing nodes to gossip, propagate blocks and connect with each other. The information in this layer is always only partial, each node may store a different view of the network, the “mempool”. This layer also contains the Lightning Network, a network of nodes that facilitate unicast transactions of value between nodes. This is the “Layer 2”.

The third layer will be the application layer, where APIs are built to interact with Layer 2 and allow highly performant user interactions with the network. This was first observed with satoshis.place where less than a week after it was launched, enterprising users were utilizing APIs to paint complex pictures, such as photos and a copy of the Bitcoin white paper, and even performing state-reversions of the entire billboard.



MULTI-LAYERED BITCOIN

With this in mind, we can see that an on-chain transaction at the base layer is one of the most cumbersome things to do with Bitcoin, and is akin to sending data packets at the networking layer of the Internet. We simply don't do it unless we need to rig to servers together to transfer data at high speed; such as in data-centres, trading desks or agency/enterprise-level infrastructure.

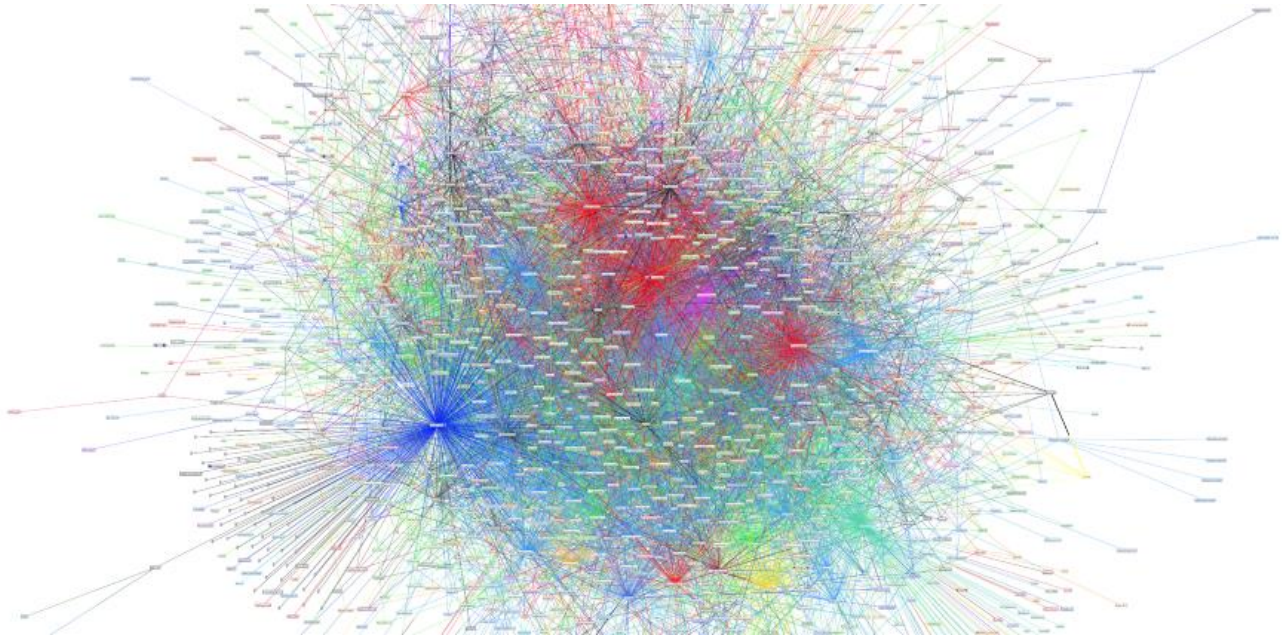
Even sending a lightning transaction itself is one-level too deep for the desired experience. It is substantially more scalable and useable than transacting at the base layer, but for mainstream adoption it is not desirable.

We need to keep building to get ourselves to the Application Layer. We're quite a long way off that (3–5 years), but the good thing is we don't need to rush there. It's actually only necessary to allow 8 billion people to onboard, with performance, scalability and an excellent user experience. In the meantime, base layer and network layer transactions are perfectly fine for early adopters.

The Networking Layer

Lightning Network is a relatively new layer of Bitcoin, but it makes more sense to see that it is the unicast networking layer that sits above the base layer, and below an application layer. However the application layer is absolutely dependent on a robust networking layer. Indeed it is only being realised now that for the LN to work as best as it should, it needs to bring in other aspects of technology never before thought related to Bitcoin, such as machine learning and artificial intelligence.

Autopilot



Lightning Network

In the LN, users choose their route to their destination address. However there can be thousands of different choices of route, and the user may have different preferences between liquidity, fees, reliability and privacy. Each route has different characteristics that are non-deterministic as they are set by nodes that can connect and leave at any time. Additionally, with Atomic Multi-path Payments (AMP) the number of routes actually transacted across for a single payment may number in hundreds or thousands.

This is currently far too much for client-side processing, and indeed there is no algorithm that can easily solve for this. Instead, advanced ML algorithms will do far better in choosing routes between peers, and will allow the user to make payments with close to optimal speed, reliability, liquidity and privacy; all across a permissionless and decentralised network.

Indeed, an advanced AI-powered Autopilot will ensure that the connections made between nodes and users, as well as the parameters chosen for each route, counters most forms of attack on the network. Some of these attacks (such as parasitic, oppressive or censoring nodes) are not yet clearly defined or understood. For LN to ever function securely, it requires building first on a robust, resilient and secure Base Layer. Then once the Networking Layer is mature, then we can build the Application Layer.

Programmable Money

We've actually never truly seen programmable money before. Before Paypal and other payment services, sending money online was extremely difficult. Paypal's innovation wasn't making a better money, it simply created a network effect and consolidated a lot of ecommerce users in one place, so it could transfer money faster. Stripe and Square also didn't create a better programmable money, they just simplified the on-boarding process for users and merchants.

The digital money we have been using the entire time never improved. Even in 2018, the minimum credit card fees have never been lower than around $1 and processing time never less than a few seconds. Beating these limits could only be possible by giving another entity access to your money, and this will never be feasible at scale.

With multi-layered Bitcoin, transactions to the 100th of a cent can be processed close to the absolute maximum limit of performance of the underlying internet infrastructure—and this can all be done completely trustlessly and never giving over control of money. Early tests show a single payment channel of LN processing payments at over 1m transactions per second.

These capabilities are about to usher in a new generation of marketplaces, experiences and economies. It is feasible that in future payments could be paid at the per-byte, per-millisecond, per-millimetre, per-millilitre or per-gram level; and these payments are entirely streamed between machines.

Some examples could be:

1. Your fridge detects emptiness and orders your next meal for you.
2. Your phone pays at the per-byte level for a faster internet connection, spending up to a cap you set.
3. Your self-driving car drives faster than other traffic, paying to over-take.
4. Your browser pays for the per-second view of online content.

Machines understanding value

Once our machines start interacting across the multi-layered value-transport protocol that is Bitcoin, it is conceivable that they will be taught to become aware of value. This will give rise to an entirely new generation of efficiency and effectiveness, as well as intelligence.

With more machines performing redundant tasks, humanity will gravitate more and more to what can keep us occupied, stimulated and happy. This will likely be around entertainment and consumption of content, especially in virtual and augmented reality.

At the same time, creation of content will be increasingly be served by artificial intelligence, reducing the feedback loop between creation of content, and assignment of value to that content by humanity. If an AI is producing video, music, art, virtual sports or games to an audience of humans, and it is being paid at the per-second or per-byte level; then the feedback between creation and consumption will rapidly reduce, and there is no more concise or clearer feedback than being paid for something.

Whether or not this accelerates us to singularity, is up for debate. However, the assuring thing about this reality is that the future with a multi-layered programmable money is that it is owned by all, and controlled by no one. This is far better scenario than a state-sponsored singularity.

Lightning Network

Scalable, Instant Bitcoin/Blockchain Transactions

Lightning for you, now

A multi-layered Bitcoin sounds exciting, but what can be used now? In truth the network is extremely young and under constant development. There is still a strong sense of naivety in what it really all is, and there is a large camp of users who don't yet subscribe to or understand the multi-layer properties of the Bitcoin protocol yet.

The take-away is that Bitcoin is a multi-layered value-transport protocol, just how the internet is a multi-layered information-transport protocol. And the two will converge in a perfect storm.

#getoffzero #buybitcoin

In the next blog we'll discuss how individuals can use the LN. Before then, you should download a lightning wallet: https://play.google.com/store/apps/details?id=fr.acinq.eclair.wallet.mainnet2&hl=en

You should also buy a lightning node to host at home: https://store.casa/lightning-node/

More resources: https://lnroute.com/

Follow me on twitter: twitter.com/jpthor_

I share, write and talk about the decentralised future.

Bitcoin Fundamentals: Mining Profitability Ratio & BTC Dominance

By cryptopoiesis

Posted October 11, 2018

Bullish, bearish? Neah... 100% mellish! Mellivora capensis the binomial name of the

likewise commonly binomial named: honey badger

The **PetaHashDollar** (**PHD**) metric is a robust way to quantifying mining profitability over short timeframe, while also broadly describing the progress in mining efficiency over longer timeframes. As outlined in ***PHD Ratio, Rock Bottom Mining & Peak Tether***, the **PHD** metric is calculated by dividing Bitcoin's Hash Rate (**Daily PetaHashes**) by **Daily Mining Earnings** (USD) to include block reward & transaction fees.

In this article, the data sources on which this metric relies have been changed. The methodology and rationale for doing so are described in the article ***What is the Price of Bitcoin or its Market Cap... Exactly?*** The rest of the data sources concerning this metric have also been changed after analysing and comparing several sources. To summarise, all data is derived from:

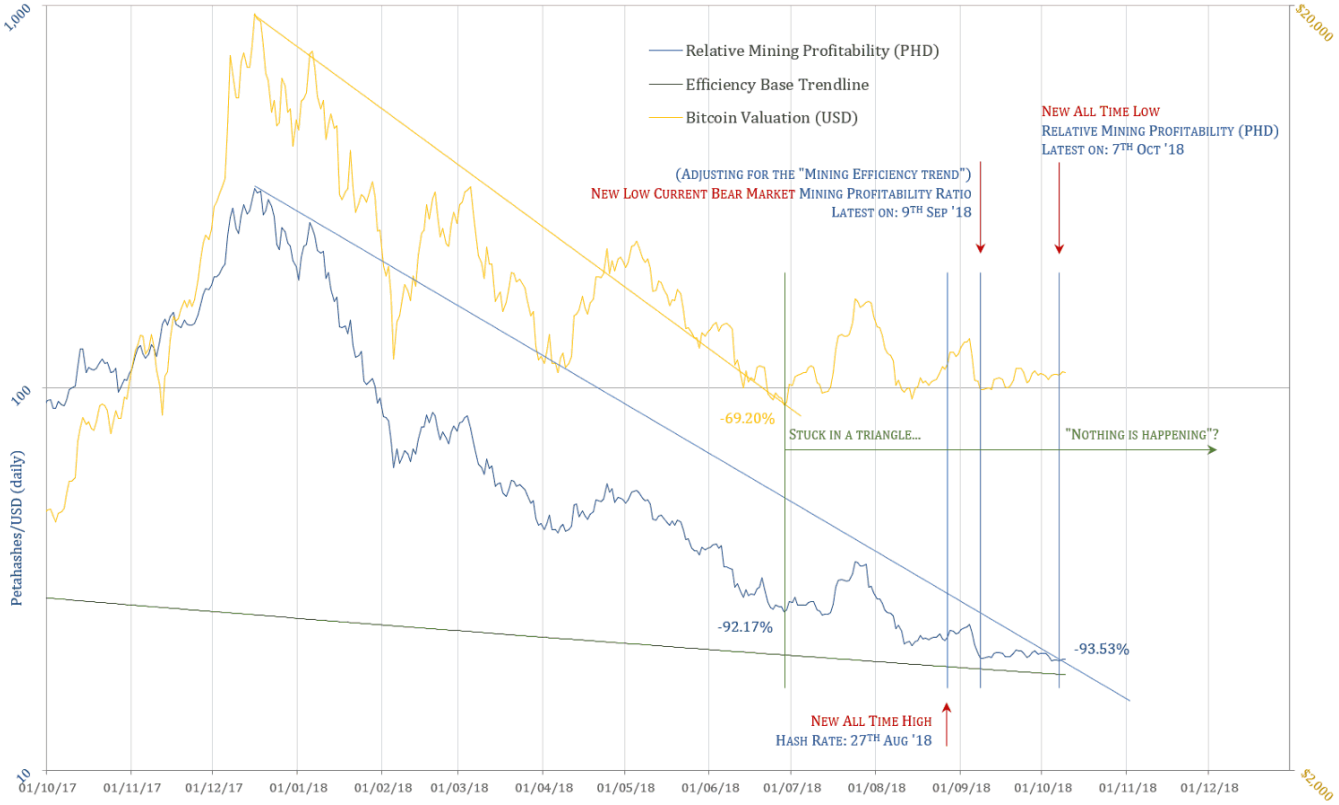
- Daily Market Price, Daily Transaction Fees (BTC): blockchain.info
- Closing Daily Price: coinmarketcap.com
- Hash Rate, Coin Supply: bitcoinvisuals.com

The results of the new methodology/data sources can be compared to the legacy ones in the graph below

Where Are We At?

Challenging the apparent boring aspect of price action in Bitcoin valuation (up until the time the article was drafted, not the case anymore), in just over 3 weeks, Bitcoin has set a few record values:

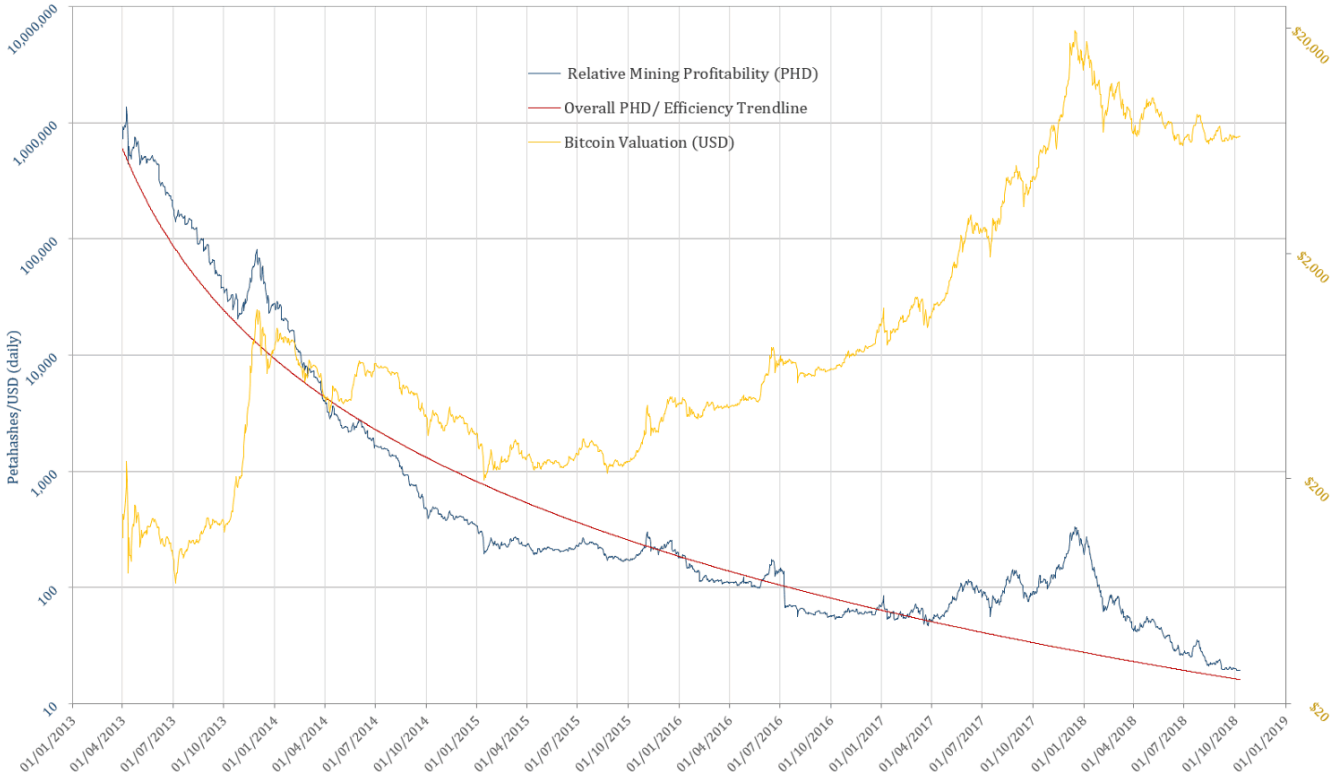
- **New All Time High Hash Rate**: 27 August 2018
- **New All Time Low PHD**: 7 October 2018
- **Mining Profitability Ratio** (PHD adjusted for the "Mining Efficiency trend")
  New Low Current Market Cycle: 9 September 2018



Mining Profitability Ratio

Regression analysis for exponential growth/decay have been unsuccessfully attempted in order to normalise the PHD metric, as to compensate for the substantial increases in efficiency and hash rate. This approach is to be furthered in a future analysis. For the purpose of this article, an eyeballed line of best fit has been derived from an exponential equation which best fits the entire span of the ASIC

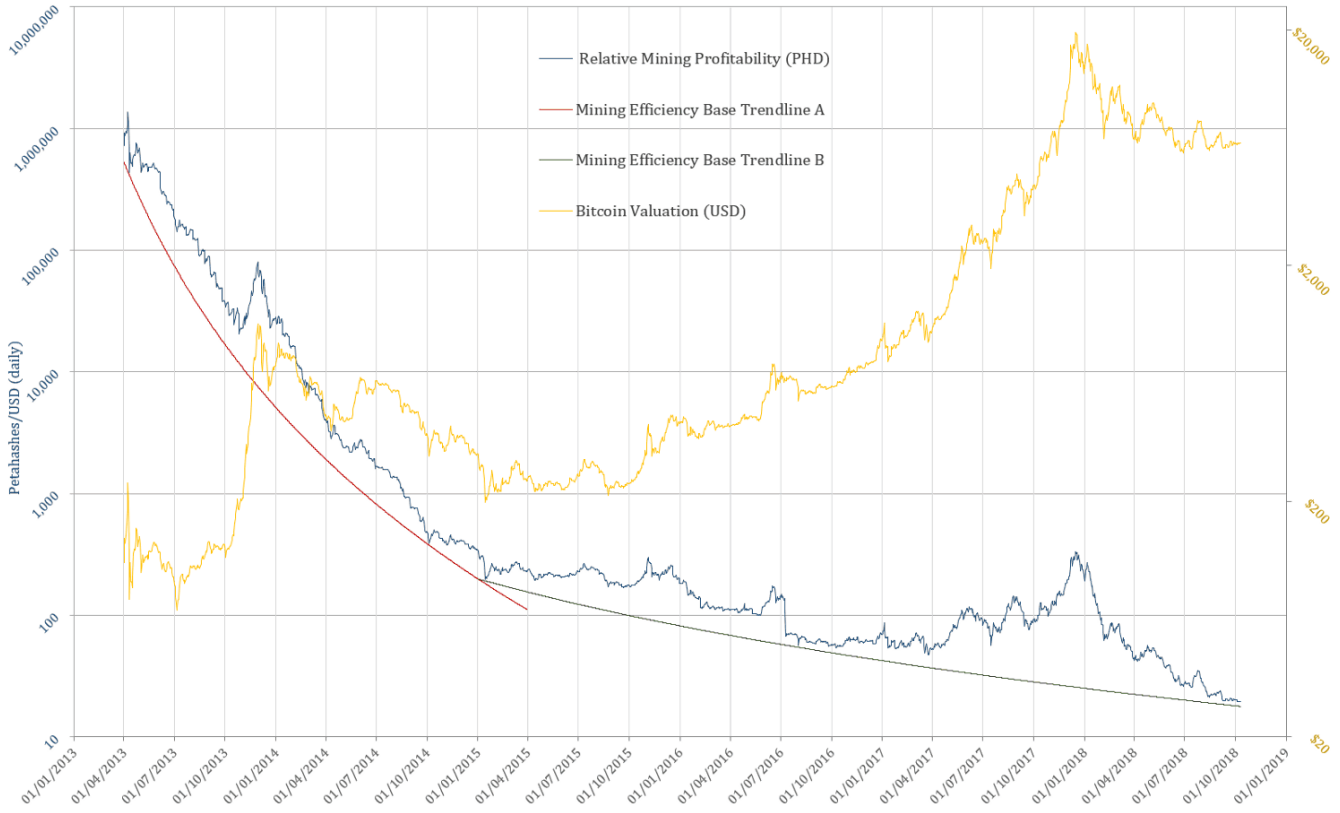
mining era:



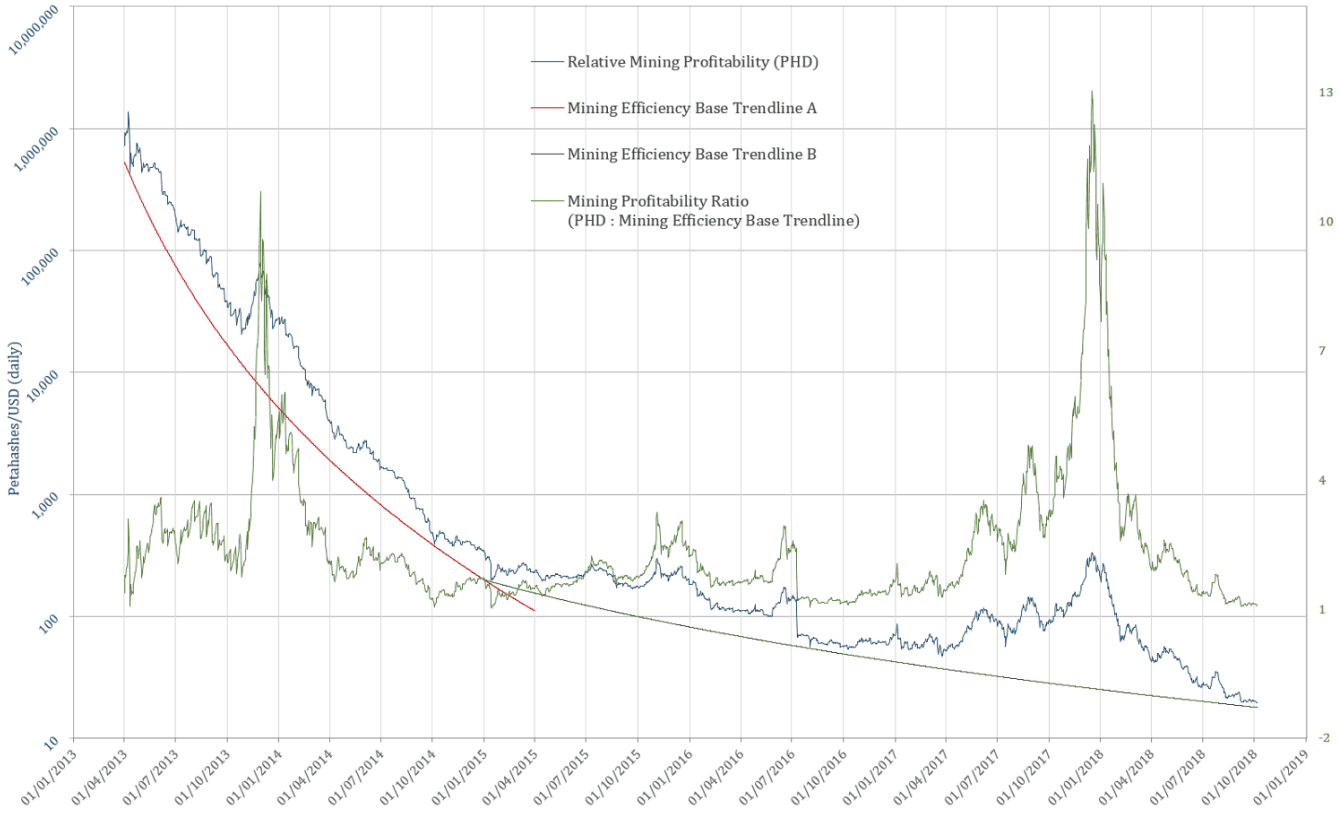
The issue of using one equation for the entire timespan is that it departs too much from the more empirical progress in leaps and bounds (further exaggerated by market cycles). A sensible approach is dealing separately with the two visibly distinct areas of the graph:

- A—the initial substantial increases in terms of efficiency & hashing rate
- B—the tapering off in the magnitude of efficiency increase

The two equations best describing the baseline of these phases have been calculated and plotted below:



From PHD to Mining Profitability Ratio:



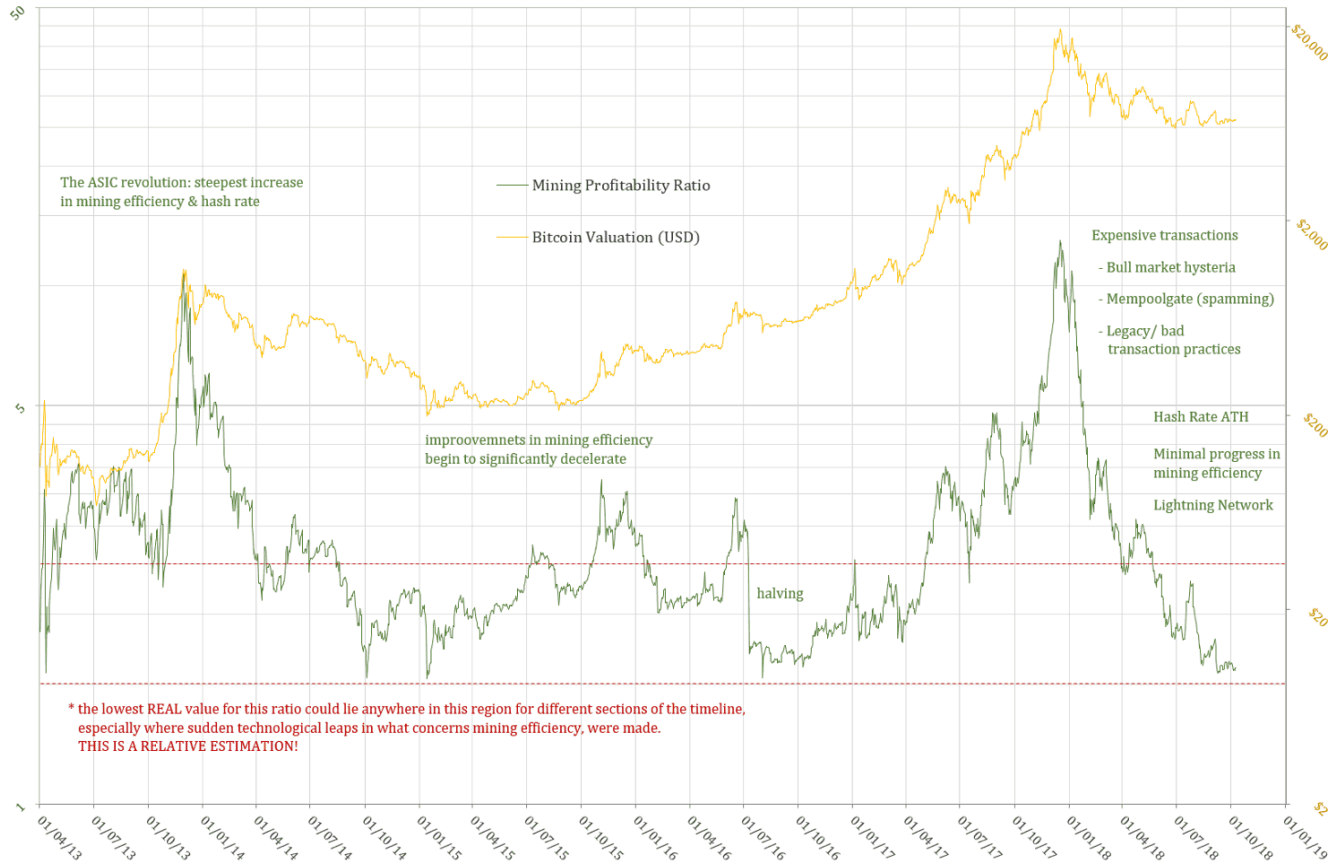
Discussion

For the Mining Profitability Ratio to touch baseline at the end of October, the price of Bitcoin would have to take a dive down to anywhere in between **$5,385**and **$4,406,**assuming 10% increase or decrease from current hash rate respectively, and an average mining revenue of c. 1,842 BTC/day (transaction fees + block rewards)

This scenario would be consistent with a dive to $4,900–5,200 range of resistance and would likely have the effect of bouncing back BTC price, at least for a few months of upside, if not directly into a halving-anticipating bull market, and all-time highs. Outside a major technical/security flaw or some kind of *black swan* event, Bitcoin is very unlikely to just dive to $3000… at least not this year.

Continuing *being boring* at current price levels, or bellow 6K, as well as in the range above (7.5–10 K), are all healthy scenarios for Bitcoin in long term. This lull is allowing the mining operations enough time to recalibrate & refine their workings, both in terms of technical efficiency, as well as in maintaining their operation liquid.

A Bitcoin mining industry in rude health is one core fundamental which needs to be met before even considering a true bull market insight.



Low Bitcoin Dominance Fundamental:

The Flipside of the Altcoin / Scamcoin Argument

Another fundamental which is radically different from all previous market cycles is the low Bitcoin dominance. While this can appear, as it has thus far, as a huge impediment in sustaining any upwards momentum—funds immediately beginning to flow into the plethora of other projects—this state of affairs can also have a backlash effect… if given enough time.

All the printed securities, tokens, altcoins are hugely centralised and, while it cannot be said that the individuals & organisation running them are most ethical, their intelligence cannot be underestimated. While the newly attracted capital and "dumb money" had been pouring in these ventures, it is sensible to assume that a considerable portion of the funds generated in this manner— ***the printing press***— had been, and will continue to be converted into Bitcoin for long term hodl.

This trend, in tandem with the capital required to be sieved out in order to prop up these schemes/ projects, sooner or later is bound to reach an equilibrium with the dumb/speculative capital willing to flow towards them. Once this point is reached, a BTC upwards momentum would have a significantly better chance to be sustained, thus preventing entirely the ***Altpocaliptic scenario***, in which a major capitulation in Bitcoin would evaporate all other speculative capital, along with any willingness to be ***innovative,*** reckless or scheming in this space.

Conclusion

Bitcoin is fundamentally a different beast than in all previous market cycles; any reference or comparison to previous cycles must be treated with extra caution. Nothing is "off the table", anything can go "off the charts"!

DISCLAIMER This content is only to be taken as my personal OBSERVATION & OPINIONS, for the purpose to be further considered, debated or discarded. The analyses outlined are far from exhaustive, and ARE NOT & CANNOT serve as basis for any financial / investment / trading advice.

Work is Timeless, Stake is Not

Hugo Nguyen

Posted October 12, 2018

Much has been written about Proof-of-Stake (PoS).

There are many ways to slice and dice PoS and uncover its weaknesses. Mainly:

Evolutionary Psychology/History: "Collectibles" or "proto-money" in history all had one thing in common, *unforgeable costliness* [1]—or at least unforgeable costliness in the context of their times. From sea shells, furs, teeth, to precious metals to minted coins. As PoS merely involves the temporary lockup of existing capital and does not consume said capital, it does not satisfy the unforgeable costliness requirement that Nick Szabo identified as one of the 3 key properties of money.

Economics: If an object has value, people will spend effort to chase it, up to whatever the object is worth (*MC=MR*). This effort is also "work". Paul Sztorc correctly concluded that PoS is an obfuscated form of PoW.

Work manifests in different ways in PoS, whether it is taking out a loan from the bank, running 24/7 staking servers, or attempting to steal online staking keys.

Not only PoS is obfuscated PoW, it is inferior PoW. Any potential cost saving PoS gives you, it pays back in *equal measure* in the reduction in security.

As we shall see below, a dollar [2] fleetingly locked up in staking creates nowhere near the same level of security as a dollar spent in mining.

Computer Science: Andrew Poelstra wrote one of the first formalized critiques of PoS, in which he coined the terms costless simulation (aka nothing-at-stake) and long-range attacks.

A recent paper by Jonah Brown-Cohen, Arvind Narayanan & co. also showed surprising barriers to having a good and reliable source of randomness in PoS protocols [3].

Engineering: I myself have written a 2-part series [Part 1] [Part 2] looking at PoS weaknesses from the practical engineering perspective, and listed specific worst-case scenarios where PoS is particularly vulnerable: network partition, private keys theft, or low rate of participation in staking.

But perhaps one of the simplest ways to look at PoS is through the lenses of Time, which I alluded to in my series, but want to expand on here.

Proof of Stake is Proof of Temporary Stake

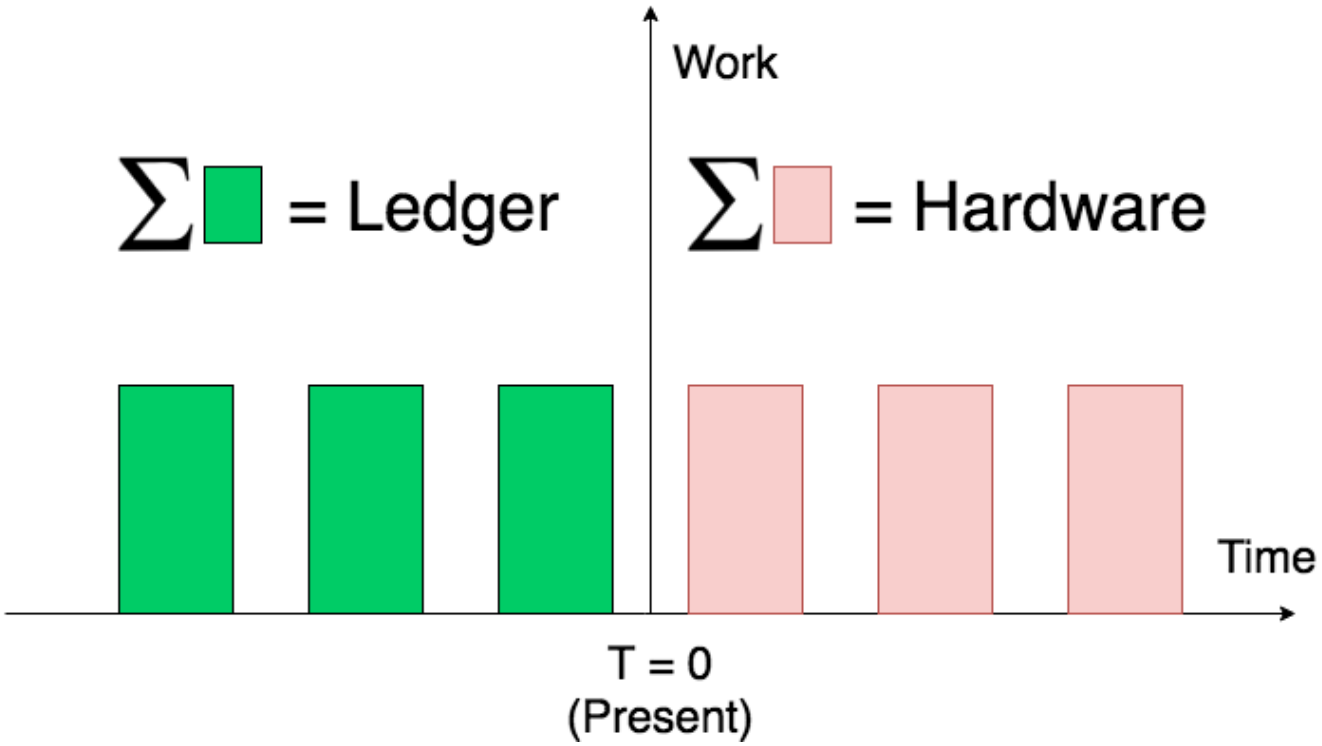
Proof-of-Stake is a misnomer. The correct, fully descriptive name for Proof-of-Stake should be Proof-of-Temporary-Stake (PoTS). This name is more accurate because it captures the time element, or lack thereof, of PoS.

To understand the effects of Time, let's first analyze how Time plays a role in PoW.

The ongoing energy expenditure in PoW contributes to network security in 2 ways:

- Energy expended per block not only secures the UTXOs belonging in that block but also retroactively secures all global UTXOs that occurred in past blocks. The reason for this is because it would be impossible to revert past UTXOs without reverting the current block first. Each new block effectively "buries" all existing UTXOs under its weight.
- Investment in specialized mining equipment, in essence, represents the potential stream of rewards earned in the future, discounted back to the present. When a miner invests in a new piece of mining equipment, it is akin to buying a share of stock that pays regular dividends. What that means is that mining hardware in totality roughly represents potential energy expenditure of future blocks.

One way to visualize this is to imagine a timeline. Units of work expended in the past *accumulate* in the ledger. Units of work expended in the future *accumulate* in the current mining hardware.



Ledger accumulates past work; Mining hardware accumulates future work.

As time moves forward, units of work on the right side materialize and move to the left side. Mining hardware can also be seen as a "buffer", a place where units of work deposit before making their way to their final destination: the ledger [4].

The official term to describe this sort of time-based accumulation phenomenon is *stock & flow*, which occurs often in nature. Bitcoin is essentially protected by high stock-to-flow ratios in 2 areas: the ledger, and the mining hardware. (Go here for a detailed discussion of stock & flow.)

In contrast, PoS has no equivalent of this.

Past stakes (left side of the timeline) do not accumulate in the ledger, as stake is released after some arbitrary bonding period [5]. Long-range attack is the manifestation of this weakness: it works because of PoS's inability to secure the past. Long range attack is at the heart of the problems with PoS, because it shows that in the long run PoS fails to guarantee the integrity of the ledger—the most important asset of all this innovation.

Future stakes (right side of the timeline) also do not accumulate in the validators in the present time, as again the act of staking only has meaning within the short

window that it occurs—what happens in the future does not count *today*. Current-private-keys-theft is the manifestation of this weakness: it works because of PoS's inability to secure the future. Keys theft sidesteps altogether the financial cost supposedly required to acquire controlling stake—whereas in PoW there's no sidestepping the fact that an attacker needs to overcome the mining hardware and ongoing energy costs to pull off *and* sustain a majority attack [6].

(There is one form of accumulation in PoS. That is, the periodic staking rewards that accrue to the validators. However, unlike accumulation in PoW, rewards accumulation is only beneficial to the individual PoS validators, not to overall network security.)

In summary: the further one moves away from the present time in PoS, the faster stake loses its meaning, until stake becomes meaningless.

Work is robust against the ravages of time [7]. Stake is not.

The fact that the cost of PoW mining is irretrievably sunk and accumulates both in the ledger and the mining hardware, is an important feature, not a bug. PoS research is often based on the fundamental misconception that this is a bug and a source of inefficiency.

Acknowledgments

Special thanks to Vijay Boyapati, Bob McElrath, LaurentMT, Nic Carter and Steve Lee for their valuable feedback.

**Note: Another major criticism of PoS is that PoS pretty much guarantees a plutocracy system (rich getting richer). That is not discussed here as it is not related to security strength per se, and deserves its own separate discussion.*

[1] Some might confuse unforgeable costliness with the labor theory of value , but they are not the same thing. Energy cost alone is not enough, the asset must be unforgeable.

[2] Dollar is only used as a unit here for convenience, it could be any other unit of account.

[3] For a PoS currency, relying on an external source of randomness involves circular reasoning fallacy . Therefore it is highly desirable that PoS generates randomness internally, using the content of its own ledger. However, this proves to be a difficult problem that has its own trade-offs.

[4] Not all units of work make it all the way to the ledger. Some are thrown away, but even thrown-away work are necessary to keep the network decentralized.

[5] The concept of " finality " does not change the (lack of) accumulation aspect of PoS, as new/long-dormant/partitioned nodes can see different "finalities".

[6] Hardware seizure (e.g. by a state actor) is a risk in PoW, however this risk can be mitigated as long as mining is sufficiently decentralized. Disperse hardware, however, is not a defensive option for PoS, as PoS validators are just software nodes — which can be targeted from anywhere remotely. More importantly, even with seized hardware, an attacker still can't avoid ongoing energy costs.

[7] Work is timeless / robust in terms of number of hashes, not energy required. New hardware technologies could improve mining efficiency — although at some point the efficiency gains will slow down as we run into hard physical limits. The robustness of Bitcoin's PoW also relies on SHA256 not being broken.

Powered by Lightning—Part 2

Using the Lightning Network as a user

JP Thor [₿ ⚡]

Posted October 13, 2018

In the first part of this series I discussed how Lightning Network (LN) is making money programmable and setting the foundation for a world powered by digital, state-less, debt-free money. In this part I'll discuss how individuals today and in the future will be using the Lightning Network.

- Part 1—The Lightning Network — Programmable Money
- **Part 2 —Using the Lightning Network as a user**
- Part 3—Using the Lightning Network as a business
- Part 4—Using the Lightning Network as a country
- Part 5 —When the world is powered by Bitcoin

In the future we will be able to use the LN for the following time of payments:

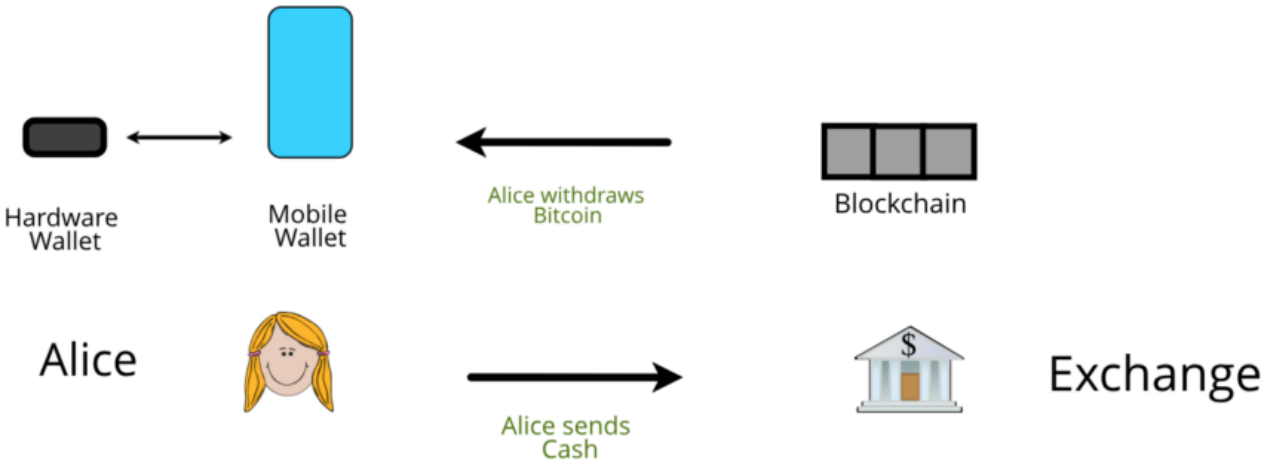
- Paying peers
- Paying merchants
- Programmable money (games, streaming entertainment, services, IoT, etc)

We'll take a look at each scenario and discuss how it can be done with Bitcoin and the Lightning Network.

Entering Bitcoin

Firstly, how does Alice enter Bitcoin? Alice purchases it off an exchange of some sorts, by making a purchase with fiat, and withdrawing her Bitcoin to her mobile and hardware wallets. Mobile wallets for small, quick purchases, often referred to as a "hot wallet" and hardware wallets to store the bulk of her Bitcoin for security, often called a "cold wallet".

The following is the typical flow:



Buying and withdrawing Bitcoin

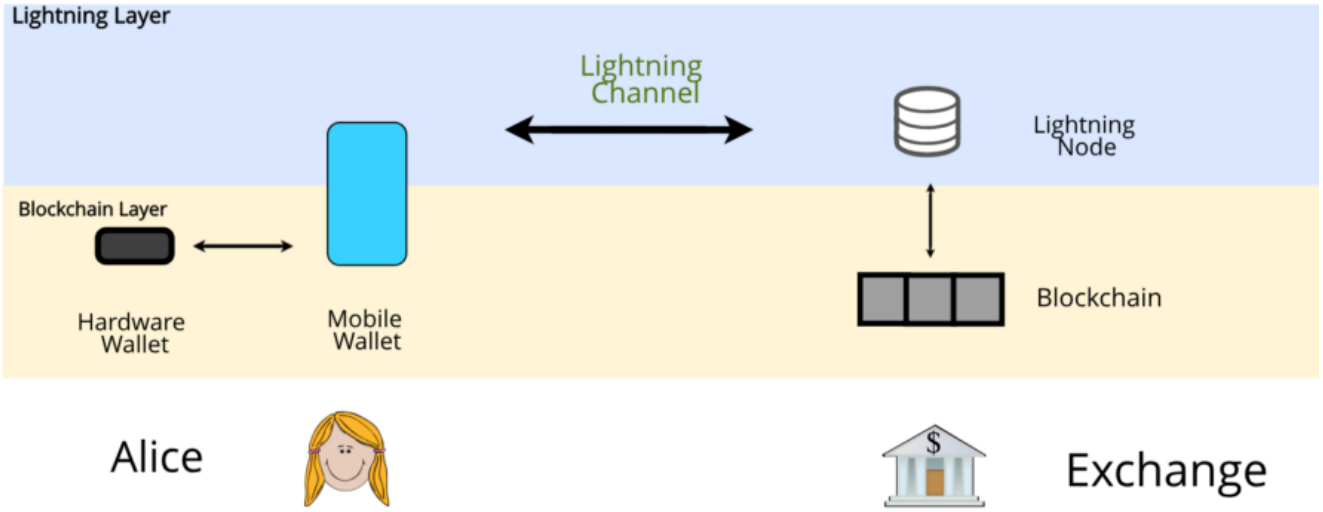
In a lightning-powered future, Alice will do it no differently. From the same wallet that she currently uses as a hot wallet, she will open a channel with her exchange, creating her first lightning channel.

The semantics of "opening channels" will most likely be dropped in the future Bitcoin wallet to avoid confusing users. Instead, users will have a "lightning wallet" which will have software (Autopilot) that will open channels seamlessly behalf of the user; and these channels will be opened with a number of different nodes, not just an exchange node.

The lightning wallet is accessed from Alice's mobile device, but the mobile device is capable of holding Bitcoin at both Layer 1 and Layer 2. Future mobile wallet apps should strive to have very clear user experience around the two layers; most likely treating the lightning wallet as the "everyday cash account", and the blockchain wallet as the "savings account". The hardware wallet would then be the "term deposit" or the "super fund".

We'll soon see why her Mobile Wallet should have both Layer 1 and Layer 2 Bitcoin. Just a note; Layer 1 Bitcoin is always the same as Layer 2 Bitcoin, but Layer 1 Bitcoin can be viewed as unencumbered, whilst Layer 2 Bitcoin has been signed into a conditional wallet. To relate to the legacy finance system, Layer 1 Bitcoin is akin to cash in a bank account, whilst Layer 2 Bitcoin is akin to your Paypal balance—it's the same cash, but both you and Paypal have oversight on your Paypal balance.

Note: with Bitcoin, your assets can never be seized in Layer 1 or Layer 2, unlike bank accounts and your PayPal balance, which are just database entries and can be wiped at any time.



Alice opens a lightning channel with her Exchange.

Alice can now do the following:

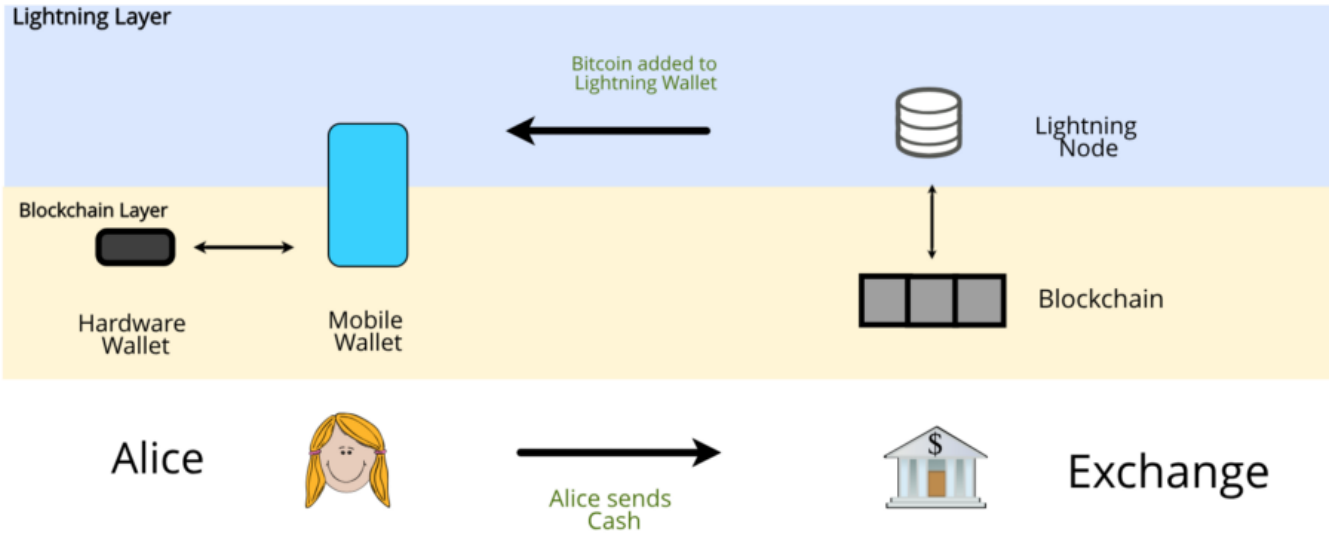
- Add Bitcoin to her lightning wallet, or withdraw it
- Spend Bitcoin from her lightning wallet

Adding and withdrawing Bitcoin

Alice will want to keep topping up her Bitcoin wallet. She can do this by the following:

1. Send cash to her exchange
2. Add Bitcoin directly from her mobile blockchain wallet
3. Add Bitcoin directly from her hardware wallet

Adding Bitcoin directly to her Lightning Wallet is called “splicing”, and Alice can splice-in from any other on-chain wallet she owns. When Alice sends cash to the exchange and buys Bitcoin, the exchange will be splicing-in from their on-chain wallet into her channel.



Alice can keep filling her Lightning Wallet by sending cash to her Exchange

To Alice this is all completely seamless. She can view her Lightning Wallet’s balance and is able to add to it from any mechanism she desires. Under the hood, her wallet is performing a series of atomic on-chain transactions in order to place her Bitcoin into her Lightning Wallet.

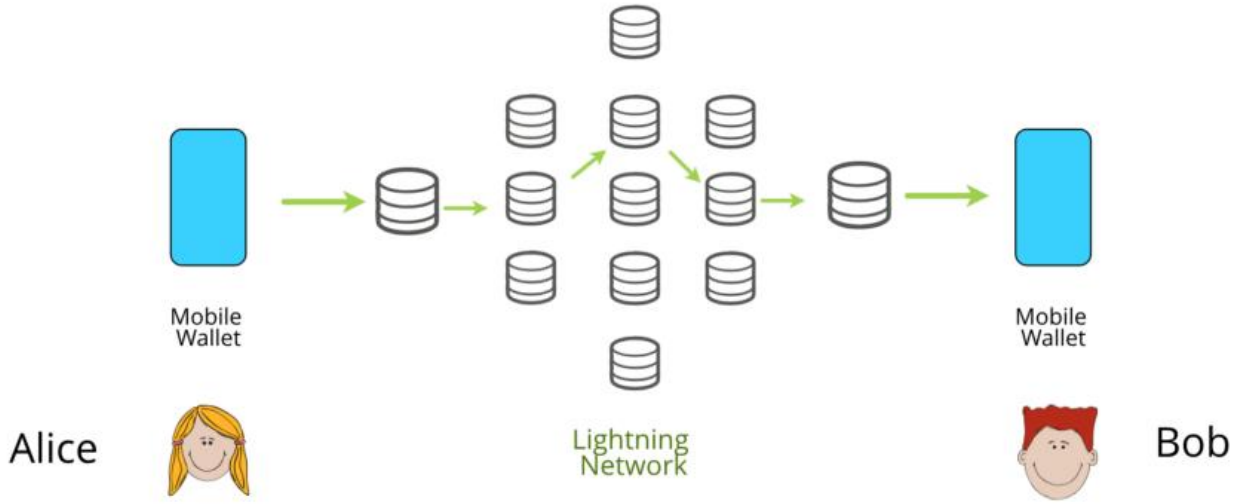
Withdrawing Bitcoin is simply the above actions in reverse:

1. Withdraw Bitcoin to cash: withdraw via her exchange
2. Withdraw Bitcoin to her Layer 1 wallet: splice out from her lightning wallet
3. Withdraw Bitcoin to her cold wallet: splice out from her lightning wallet

Spending Bitcoin

Once Alice has a Lightning Wallet with a balance, she can spend to anyone else that is on the Lightning Network. She enters her recipient’s address and sends the payment. Her mobile wallet performs the following actions:

- Calculates the best route to Bob
- Sends the payment and waits for receipt



In the case that Alice opened her channel(s) with her local exchange, the payment will be routed first via the exchange's node, this is the "gateway node". The last node in the payment route will be the node that Bob's wallet first connected to, also called a gateway node. This is likely to be an exchange node, simply because exchange nodes are in the best positions to on-board new users onto Lightning efficiently. Bridge nodes are nodes that open channels with other nodes, and have more outgoing liquidity than incoming.

Gateway nodes perform important functions in the payment flow, and can make or break Alice's payment experience. Luckily there is a lot of innovation happening right now, so we'll talk about that.

It is in Alice and Bob's interest to open a number of channels with different gateway nodes for privacy, redundancy and reliability.

Issues

Some immediate issues in the payment flow above, as well as their solutions, are discussed:

1. Bob doesn't have a lightning wallet.

In this case, Alice's smart mobile wallet will detect that Bob's address is not a lightning address, and will instead send Bob Layer 1 Bitcoin seamlessly.

1. Alice's lightning wallet doesn't have enough Bitcoin to make the payment at Layer 1 or Layer 2.

The future smart mobile wallet will be able to inform Alice that she will need to either top up her Lightning Wallet, or withdraw from her Lightning Wallet.

1. Bob is not online to receive his lighting payment

If Bob cannot receive the payment as he is not online, then it will fail and route back to Alice. Alice's wallet will then ask Alice to pay Bob with Layer 1 Bitcoin, which can be sent if Bob is not online.

1. The payment route that Alice selects fails due liquidity or reliability

Alice's smart wallet will be able to re-try the payment with a different route.

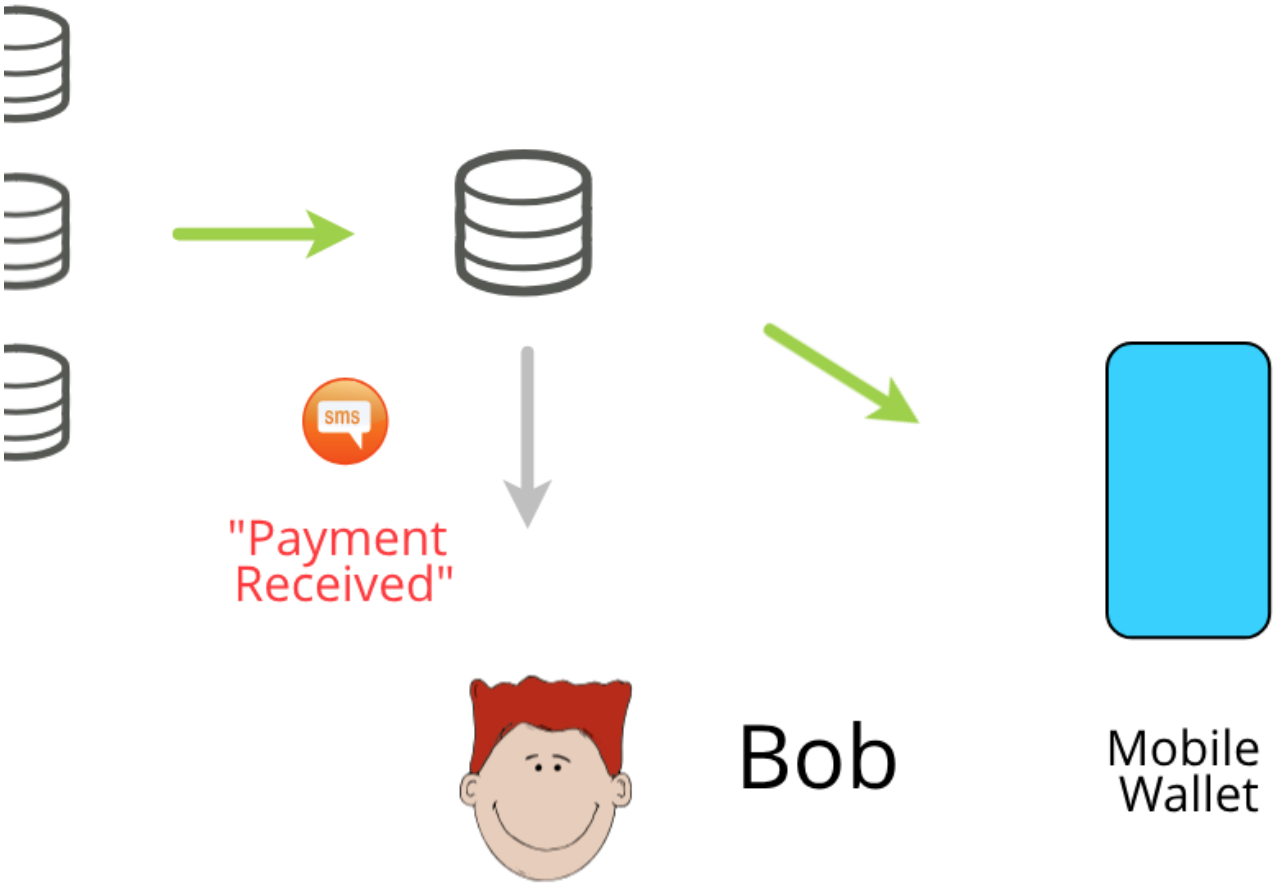
1. Bob's node doesn't have enough Bitcoin to route to Bob.

For Bob to receive $100, then $100 needs to be on the other side of Bob's channel; ie, with his exchange. This may not be the case, in which case then Alice will be unable to pay Bob, through no fault of either Bob or Alice. The solution to this is for Alice to open a channel directly with Bob.

We can see that the main issues circulate around Bob and his node. If Alice encounters any issues with her payment choice or liquidity, she can make corrections *before* she sends the payment. However, she is at the mercy of Bob's payment limitations and his node.

The solution to this is that Bob receives payments *at his node* instead of directly to his wallet. His node can then inform him of an incoming payment via email, sms or push notification, and then he has the ability to go online and withdraw any incoming payments to his wallet.

Bob may choose to run his own node, or he may open an account at his lightning-enabled exchange and let their node accumulate payments for him.



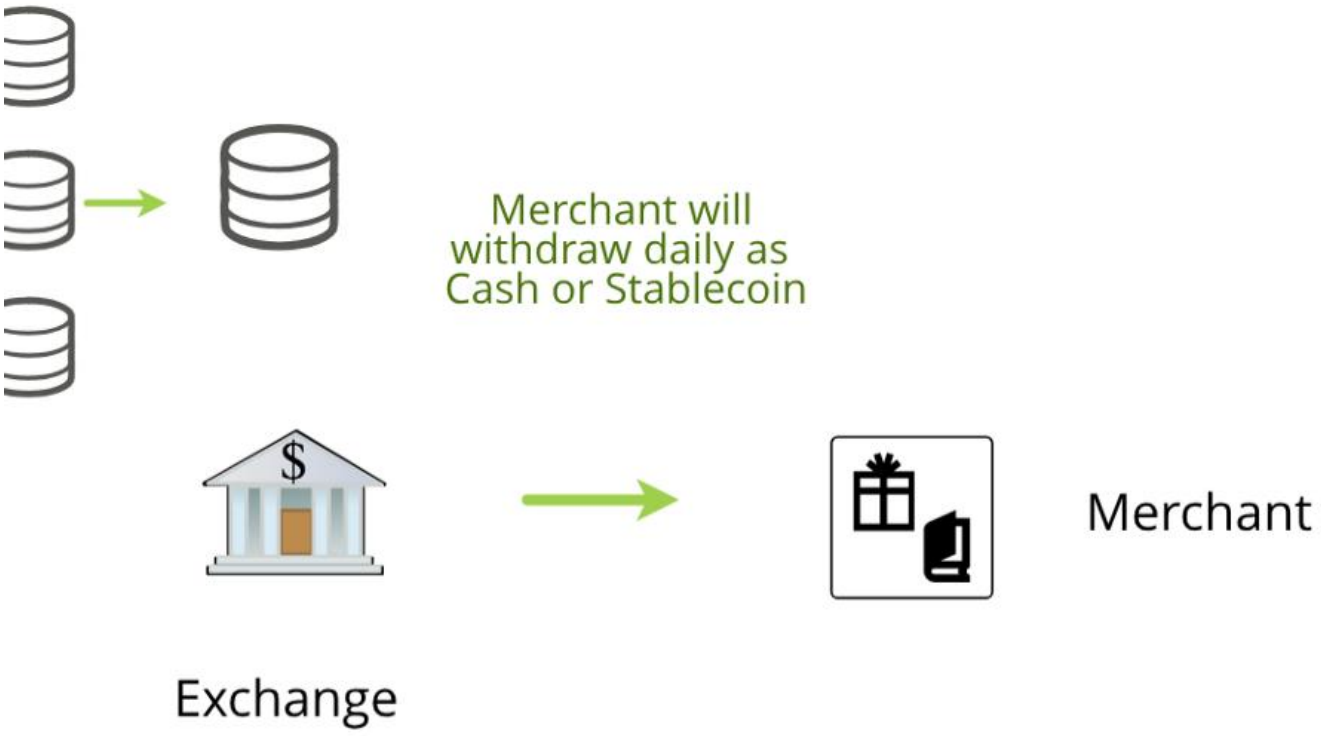
Bob receives a notification of an incoming payment

E-commerce and Paying Merchants

Making payments to peers is fairly easy although with some issues discussed above, but Lightning comes into its own when paying merchants or making e-commerce payments.

The main reason for this is that Merchants and e-commerce payment solutions will be running their own infrastructure and will care less about verifying each payment absolutely. Instead, they will be accumulating daily takings, and making batch withdrawals in cycles.

Additionally, merchants will more likely choose to receive payments in legacy fiat or stablecoins to pay tax, salaries and other business expenses. Thus it makes even more sense that they will have a merchant account at a local exchange and let the exchange handle incoming payments.



A Merchant will likely use Exchange Infrastructure

Atomic Multi-path Payments (AMP)

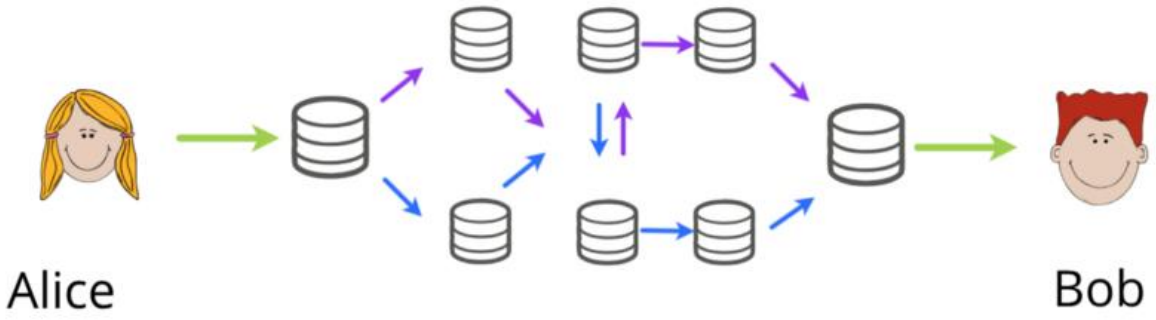
We mentioned before that Alice's wallet will be able to choose the route to Bob, but that's only scratching the surface.

AMP is revolutionary feature yet to be built on Lightning, as it was only conceived recently. The main issue with Lightning currently is that payments can only be made across channels that already have existing liquidity, ie, a $10 payment can only be sent across a channel that already has $10 in it.

AMP allows payments to be atomically sent across many different channels at once, and Bob will receive all of them, or none of them. As an example, Alice wishes to pay Bob $1000. Instead of sending a single $1000 payment that will likely fail, Alice can send 1000 $1 payments. Each payment goes across a different route and when Bob receives them all, he will have the full $1000.

When we thought Lightning allowed unicast payments, AMP allows *multi-cast* payments. This has ground-breaking improvements to the following characteristics of Lightning:

1. **Reliability.** Each channel will have an extremely likely chance of already having $1 in it, so the overall reliability of the payment will quickly go to 100%.
2. **Fee competitive.** Nodes who attempt to charge high fees will quickly lose selection from routes and will lose traffic. They will always have to charge highly competitive fees to attract traffic.



An AMP Payment

Here in this diagram Alice pays Bob $10 with two $5 payments. The routes are chosen to maximise reliability and liquidity. We can see that apart from the gateway nodes, no single node knew of the full payment size, nor who was paying who. As a result, the more payments are made across the network, the faster to re-balance and more healthy the entire network becomes. This is all thanks to AMP.

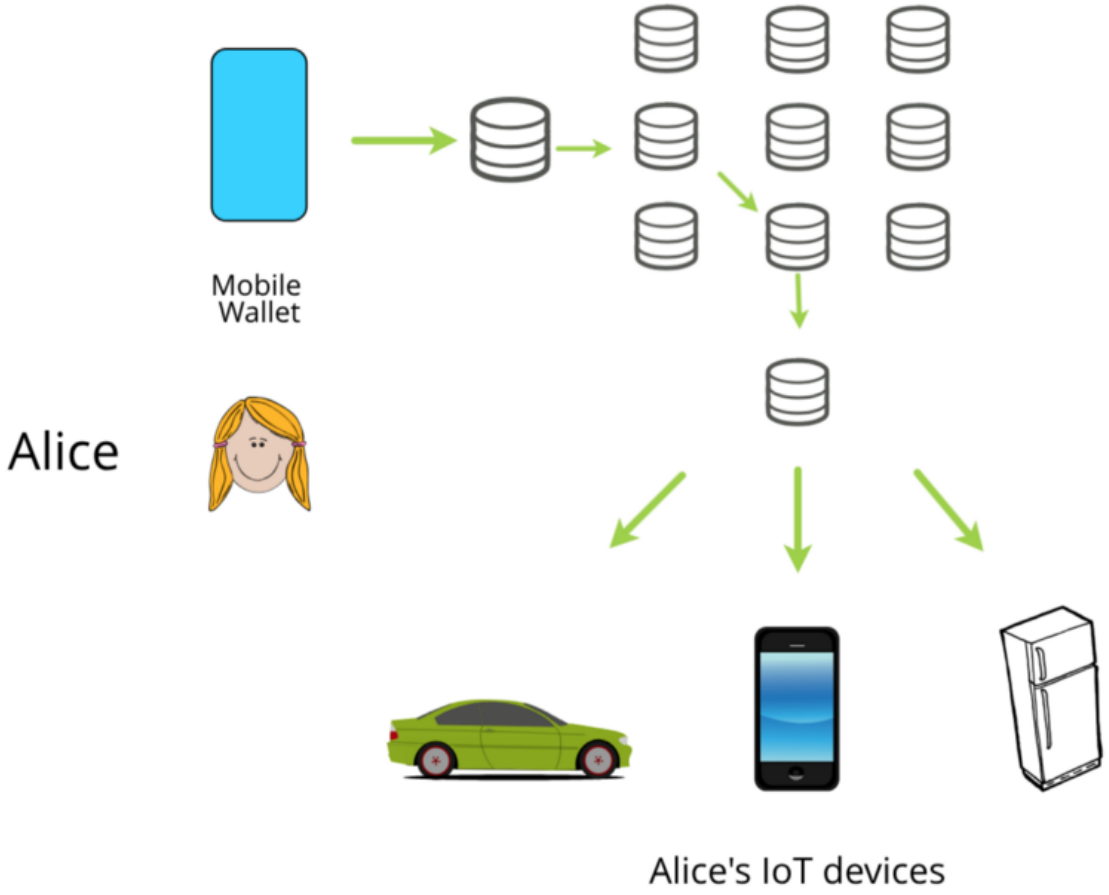
Programmable Money

Lightning enables Bitcoin to become Programmable Money. In the future, all of Alice's devices will have a lighting wallet to enable them to quickly pay on behalf of Alice, programmatically. Her self-driving car, her phone, her fridge will all have wallets and Alice will be able to set rules about how they pay, and how much. Such as:

- Phone to pay no more than $10/month for fast internet
- Fridge to pay $200/week for her grocery bills, set by her menu
- Car to spend no more than $10/week on tolls

Alice will be able to top them all up from her primary wallet, sending liquidity to them. She'll get notified whenever they get low, as well as how much they are spending on behalf of her. As they will only spend with Alice's permission, Alice will never be charged for something she didn't know about, and she'll have complete control of spending.

Alice will never be able to spend more than she has, which means she'll never accrue debt.



The future of Money

A node in every house

We can see that the health and useability of the Lightning Network really comes down to the number of nodes and funded channels there are available. Additionally, it is in Alice, Bob and the merchants' best interests to run their own nodes as they can make better choices around fees, liquidity and privacy.

The good thing is that running a Lightning node will quickly become a very trivial thing, to the point where the household of the future will bundle the internet router with a Bitcoin and a Lightning node. Members of each household will simply connect their mobile wallets with their own node, and it will run 24/7 as they currently do.

Some awesome nodes coming into production include the Casa Node and RaspiBlitz.

Ensuring that the Bitcoin network of the future remains accessible to all, so that anyone can host a node at home, is becoming more and more important. As such I am firmly in the Segwit + 1mb block limit camp. Currently the Bitcoin chain is 185GB, and takes about a day to sync on typical devices. Single chip computers (RPi) can be synced just as fast by being pre-loaded with a pre-validated chain-set.

We'll discuss in Part 5 of this series how we can foreseeably on-board the entire world onto Bitcoin and the Lightning Network with the *no change* to the current Bitcoin blockchain parameters, as well the massive benefits the current design choices of Bitcoin actually give us.

Conclusion

Lightning is a massive improvement to how we can use and spend Bitcoin and is part of a broader movement where we are slowly transitioning to debt-free, programmable money with complete control of spending.

However, there are some limitations to how we will use Lightning, mainly around the recipient of the payment. The good news is there is massive amount of innovation happening in this area and most issues will likely be readily solved.

Get started here: https://lnroute.com/mobile-wallets/

Acknowledgements

Many thanks to @ln_master_hub and BTCPay Server for giving me feedback on this article and some technicals.

Follow me on twitter: twitter.com/jpthor_

I share, write and talk about the decentralised future.

Post-Bitcoin-Maximalism: A call for embracing the currency competition

Ferdous Bhai

Posted Oct 15, 2018

In early-2013, when I learned about Bitcoin, I dropped everything else I was doing and focused on building on, advocating for, and acquiring Bitcoin. This still continues to be the case today, but my stance on "Bitcoin maximalism" has changed in light of lessons I've learned along the way.

Important to note here, I do not favor any particular alternative to Bitcoin. I simply do not think that every other alternative to Bitcoin are scams, nor do I think that the founders and the communities of these competing projects are motivated only by greed or ill intentions. In addition, I think that the altcoins serve an important role today, as we will explore in this post.

The case for Bitcoin Maximalism

Here's a possible version of a future that Bitcoin speculators prophesize:

As the governments around the world continue to steal wealth from citizens in the form of taxes, bailouts, and inflation and enforce more control, surveillance and rent-seeking on financial transactions, the citizens will seek a better alternative: a superior form of money free from government control. Bitcoin, with more sound Austrian monetary policy compared to Keynesian fiat currencies, enforced by code, governed by consensus among a decentralized network of peer-to-peer nodes, secured by miners distributed across the globe, is the superior alternative.

As more people buy into Bitcoin, the price of Bitcoin relative to fiat currencies appreciates, which has a positive feedback loop. More people mine Bitcoin. The network becomes more secure. More serious investors buy in. More end-users transact in it. More development happens. This cycle continues, ultimately leading to Bitcoin's total world domination.

We, the early Bitcoin investors, get rich off this pyramid-like scheme. The new entrants enjoy a superior form of money. Everybody wins.

Hyperbitcoinization

It's a great story, with a happy ending. But the story has a few plotholes:

1) How things scale

The maximalist worldview fails to appreciate how things scale in real life.

A grown-up person is not an overgrown child.

Marriage is not the sum of two persons committed to the marriage.

A family is not the sum total of individual family members.

A tribe is not the sum of families that make up the tribe.

A city is not the sum of tribes that make up the city.

As a unit grows, it undergoes a transformation. With growth, eventually comes a point when it's no longer the same thing it used to be. Bitcoin was founded on certain core values, but as the user base continues to grow, Bitcoin is going to continue the transformation into something else. This is neither good nor bad, it just simply is.

Things we take for granted in Bitcoin today will not be the value proposition of Bitcoin tomorrow. Bitcoin in 2018 is qualitatively different from Bitcoin in 2014, which was different from Bitcoin in 2010. With growth, this identity change will accelerate and we will likely end up in a world where Satoshi, if still alive, would be scratching their head.

2) How complex systems adapt to change

Nothing in a complex system happens in a vacuum. With the rise of Bitcoin, much of the world as we know today will change, for the better or worse.

Bitcoin brings back a sound monetary policy. The central bankers who have abused their power until now have to act carefully. With no way to shut down completely, Bitcoin is a proverbial gun to their head: Act more responsibly or die. What can the bankers do in response?

- **Introduce more sound monetary policies to compete with Bitcoin's.** There's nothing magical about Bitcoin's monetary policy that can't be adopted by centralized entities in a more efficient, transparent and effective manner, using some of the same tools that Bitcoin is built upon.
- **Improve customer service, the end-users of the currency being the customers.** The bankers will have to compete to win over the people empowered by Bitcoin. The citizens will no longer be reliant only on the government mandated currency, so the services offered must be exceptionally better to stay relevant.
- **Build new narratives.**The governments may tap into ideologies citizens value beyond wealth accumulation. This may include human rights, environmental sustainability, philanthropy, social justice, patriotism and anything else that's trendy and popular among citizens. History has shown time and time again that we are motivated by higher purposes beyond meeting basic wealth accumulation goals.Our time on earth is limited, and our value system is the legacy we leave behind.
- **Allocate resources to fight back Bitcoin.** The core features of Bitcoin we take for granted today will be challenged. The P2P network, the social consensus, the market price, network security, the protocol development are all attack surfaces and game-able. Repeated successful attacks might not destroy

Bitcoin entirely from a technical point of view but when combined with social engineering, will shake people's confidence enough that it may just make Bitcoin not suitable for mainstream use.

Aside from the bankers, with the precedence established by Bitcoin, it is possible that people's attitude towards money will change. Competing money-projects will be launched by established and respected enterprises with large followings, and governments will eventually stop the futile pursuit of attacking these projects. "Money" will be denationalized and the competition for the strongest money will lead to a never-ending battle for the best money in ways we have not seen before in human history. Technological innovation will make moving from one form of money to another frictionless and easier than moving from one social media platform to the next.

Does this seem like fiction to you? It shouldn't; in 2018, we are much closer to this reality than the alternatives. If you value libertarianism, meritocracy, and free market competition, then rejoice; this may be bad news for Bitcoin maximalists, but this is good news for you as the end user.

3) The new entrants don't owe us anything

The maximalists assume that new adopters of Bitcoin are perfectly content with buying into Bitcoin at higher and higher valuation with the full knowledge of how much cheaper the early adopters had bought in. Much like everything else with maximalism, this is a simplistic view of the world.

"They thought we were going to buy their gold!"

As we saw with the Ethereum project, launched by Vitalik Buterin, or the EOS project, launched by Dan Larimer, the new entrants to cryptocurrency world prefer to take their chance with the issuance of a fresh new currency than enrich the Bitcoin holders. Like it or not, from a game theory perspective, the incentives exist, and so this is a trend that's unlikely to change anytime soon. After all, from the perspective of an outsider, Bitcoin looks much like a scheme to redistribute real income from new to earlier owners of Bitcoin.

4) Security through redundancy

Redundancy is ambiguous because it seems like a waste if nothing unusual happens. Except that something unusual happens—usually.

— Nassim Nicholas Taleb, Antifragile: Things That Gain from Disorder

Bitcoin nodes are run by software. Just like any software, critical bugs do get introduced over time despite intensive QA and code review. This is, unfortunately, the very nature of software development, and not a criticism of Bitcoin Core contributors.

Bitcoin Core continues to attract brilliant developers, but no matter how smart they are, in a long enough timeline, there is bound to be critical errors in Bitcoin Core.

More serious threats are possible attack-vectors that are expensive and time-consuming, but nonetheless worth it for the states if Bitcoin were to become the only serious threat to the government money.

We are yet to see any serious attempt by the governments to attack Bitcoin.

One of the major reasons I believe we haven't seen a war on Bitcoin is the existence of altcoins. Altcoins are insurance against state-level attacks on Bitcoin.

The thousands of altcoins that have come out following Bitcoin's footsteps ensure that any serious and expensive attack on Bitcoin is futile and therefore unlikely. After all, what is the point in spending resources to attack Bitcoin, which, if successful, will be guaranteed to be replaced by an alternative that is even more censorship resistant, more decentralized and more private? From a game theory perspective, state-wide attacks on Bitcoin is a dumb idea, as long as the threat of one or more altcoins to replace Bitcoin's role exists.

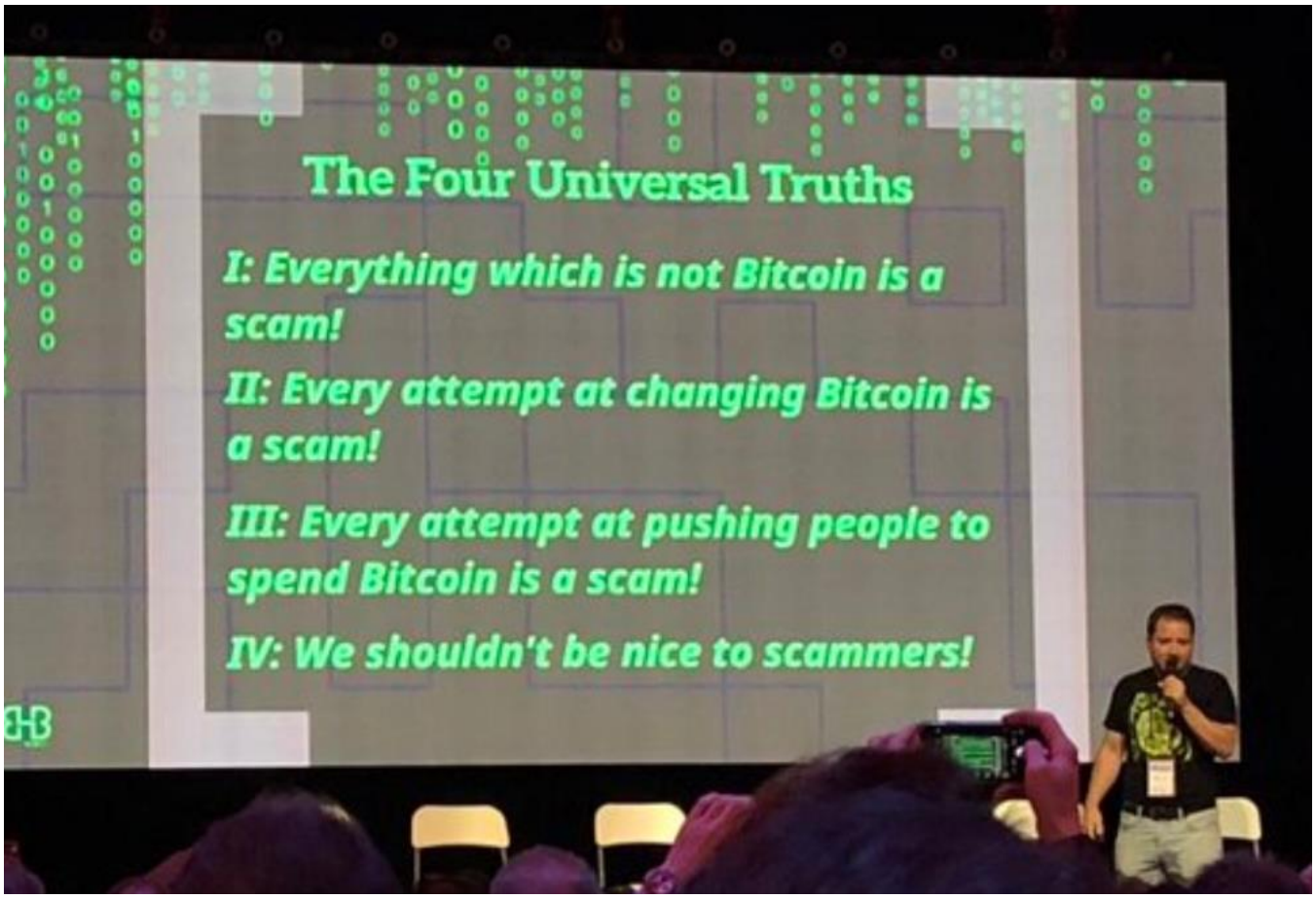
5) The trade-offs of Bitcoin

Bitcoin was born in an environment where governments around the world had a hostile attitude towards private money projects. Only the nation states were allowed to create money. Out of this necessity, Bitcoin had to settle for significant trade-offs in a quest for resistance. Many of the core Bitcoin tech stack, such as proof-of-work, blockchains, P2P networks etc are highly inefficient and present major scaling and environmental problems. But the trade-offs were well worth it to guarantee the core value propositions Bitcoin had to offer: censorship-resistance, permissionless, and decentralization to remove the central points of failure.

It's only been 10 years since Bitcoin came out, and already there are alternatives to Bitcoin that are offering the same value proposition as Bitcoin but are more private, more decentralized, more scalable, more sustainable. Our imagination and pursuit for innovation have no bounds, and therefore it's unlikely that we will never be able to come up with technology that is fundamentally much better and incompatible with Bitcoin. The maximalists would naturally dismiss the tech as an altcoin and so inherently a "scam", and ignore it until it's too late. This has happened over and over in the history of money, and there is no reason to think that it won't happen again.

Why Maximalism is dangerous for Bitcoin

Maximalism started as a harmless meme but has gradually turned into an actual cult. The cult members have a few books they swear by, a short list of influencers they follow, regular conferences they attend, and recently, even a diet plan they adhere to. All this was fun at first, but now the comedy elements have gone stale and the cult members have become the dominant voice representing Bitcoin. Bitcoin has become a fetish. All alternative forms of monetary experiments are labeled as "scams". This general direction is dangerous because not only does it alienate new-comers, make Bitcoin users look like a bunch of lunatics you want nothing to do with, but also this is completely in contradiction to the cypherpunk ethos that Bitcoin was born out of.



Bitcoin conferences these days

Bitcoin, like all money, is ultimately a shared delusion; it's not real. Money only exists because we agree as a society that they have value and so we can exchange them for goods and services. This allows everyone in society to cooperate with one another. Today, everyone believes that Dollar has value; our hope is that tomorrow everyone would agree that Bitcoin has value, and is even a superior alternative to Dollar. But if we keep alienating the users by taking extreme and nonsensical positions, then the network effect of Bitcoin will stop growing, and other alternative currencies with a healthier ecosystem will eventually win.

This is already happening. The market share of Bitcoin is continuing to plummet and new cryptocurrencies are continuing to step up their game.

Frustrated by fellow Bitcoin activists, I recently took on Twitter to criticize the maximalism movement.

What followed is a massive outcry of Bitcoin maximalist cult members hurling insults, blocking/muting me and overall being outraged. Not a single Tweet actually addressed the content of my tweet with integrity. The behavior of prominent Bitcoin maximalists in response to this tweet is a signal that we are witnessing the birth of a cult that may be the largest threat we Bitcoin proponents have endured so far.

Bitcoin doesn't scale socially if we don't learn how to be more civil.

Currency Competition

The opposite of Bitcoin maximalism is currency competition. It's not a utopian future. Scams and abuse of power will always be possible and will leave many victims in despair. Despite that, a free-market that encourages experiments and innovations is the best tool we have found historically for societal progress. The upside of free-market competition is that it leaves it to the users of cryptocurrencies to self-govern, not to gatekeepers.

Bitcoin is still the best candidate we have today as an alternative to government-issued money in terms of liquidity and adoption. I think of existing alternatives to Bitcoin as necessary test cases for permissionless innovation, as well as insurance against a state-wide attack on Bitcoin or Bitcoin users. The market and the passage

of time will naturally punish currencies with poor fundamentals and reward those with strong fundamentals.

I want to see Bitcoin win, and I will continue to build and support businesses that make Bitcoin better, stronger and more accessible. In this process, we must never lose sight of the goal. Bitcoin is not the en-dgoal; it's a means to our goal of censorship-resistant, permissionless, denationalized money that we can opt in and out voluntarily, not by coercion, social engineering or threats of violence.

True decentralization is when there are many competing money projects, not just one.

May the meritocracy win.

Bitcoin's Buyers of Last Resort

By Pierre Rochard

Posted October 18, 2018

What stops the price of bitcoins from crashing to zero in a bear market? Let's start with what a lender of last resort is.

Lenders of Last Resort

Trigger warning: if you are very familiar with interbank lending, fed funds rate, open market operations, etcetera, you may be frustrated and/or annoyed by this simplified explanation. It's safe to skip since you already know what a lender of last resort is.

Today's existing fractional-reserve banking system creates new currency when it lends to you. The bank's accounting, in simplified form, is to debit the bank's Loans asset account and credit a Deposits liability account. Your accounting is to debit your Deposits asset account and credit your Loans liability account. This process of money creation is limited on the supply side both by banks' self-discipline as well as central banks setting reserve requirements. On the demand side it is limited by the quality of borrowers and their financing needs. These factors create a ceiling for how much new money gets created when the system is growing.

When the system is contracting you have the reverse process and money is "destroyed". This gets into a negative feedback loop as money destruction causes

deflation, making existing loans harder to pay back and new loans harder to make. One by one, the system's banks become insolvent and collapse from a bank run. To "break" the negative feedback loop of a contracting fractional-reserve banking system, the central bank steps in as the **lender of last resort**. Here is a good paraphrasing of Walter Bagehot on the role of a lender of last resort:

Central banks should make clear that they stand ready to lend early and freely (ie without limit), to sound firms, against good collateral, and at rates higher than those prevailing in normal market conditions. This is an integral part of a monetary economy with fractional-reserve banking.

Central banks, as lenders of last resort, create a floor for how much money gets destroyed when the system is contracting.

The Bitcoin system itself does not create new currency through lending. New bitcoins are created as a subsidy to the proof of publication function of the system, which provides a decentralized transaction ordering service. A difficulty adjustment mechanism creates a ceiling for how many new bitcoins are issued, this mechanism is enforced by block validation rules. Read more about Bitcoin's governance here.

The Bitcoin system does not have a mechanism for destroying bitcoins, though individual users can choose to do so. Thus there is no deflationary negative feedback loop that plagues today's fractional-reserve banking systems.

Bitcoin's monetary crises occur due to a "hangover" from adoption waves. If humans were asocial animals without any herd mentality, we could imagine a world where Bitcoin's system accumulates users at a steady rate. The price of bitcoins would slowly appreciate over time. However, humans are very social animals and highly susceptible to herd mentality. Adoption happens in waves, causing the price to go parabolic as new adopters compete for space on the UTXO set at the same time. On top of organic new adoption, there are highly speculative momentum traders who are just trying to profit off the adoption wave by buying high and selling higher. When adoption and momentum peak, there is a massive unwinding. Leveraged long positions are liquidated, marginal adopters panic sell, momentum traders reverse into shorting. With everyone expecting the price to go lower, buyers disappear and bitcoins become a high-velocity hot potato. The lower the price goes, the more panic and selling there is.

The negative feedback loop of a crisis of confidence is broken by two groups (which have plenty of overlap): **holders of last resort** and **buyers of last resort**.

I first heard the phrase "holders of last resort" when Trace Mayer came on the Noded Bitcoin Podcast to talk with Bitstein and me. The phrase amusingly repurposed the fiat system's "lender of last resort" phrase and captured the imagery of unwavering

conviction and calm stubbornness in an environment of anti-"HODL" gloating, panic selling, and pervasive FUD. Holders of last resort break the negative feedback loop by **not** panic selling.

Before I continue, I'd like to illustrate how a generic order book works. Let's say the previous price at which BTC was traded was $10,000. A *bid limit order* says "I am willing to buy 0.2 BTC at $9,999". An *ask limit order* says "I am willing to sell 0.2 BTC at $10,001". A *market sell order* says "hello bid limit order, you said you're willing to buy 0.2 BTC at $9,999 and I'm taking you up on your offer", a *market buy order* says the same with the ask limit order. The limit orders create liquidity, the market orders consume liquidity. The larger the total quantity of USD in the bid limit order book, the less the price moves when large quantities of BTC are market sold. There are numerous BTC / fiat order books, at different exchanges and with different fiat currencies. In an abstract sense, these can all be rolled up into a hypothetical "global order book". This global order book includes not only visible limit orders, but also hidden limit orders which can be as casual as someone thinking "if the price goes to X, then I'll buy or sell Y bitcoins". We each have our own internal personal order book!

Buyers of last resort break the negative feedback loop in two ways. **Bidders of last resort**put in limit orders—buy bids. This provides liquidity that is consumed by panic sellers putting in market orders. They are a damper on slippage in a disorderly and volatile market. Absent these liquidity providers, the massive "gapping" on downticks increases the price impact of panicked selling. **Buyers of last resort** put in market buy orders. This consumes seller liquidity. As market orders set the marginal price, they are the upticks that eventually turn the panic around and reestablish confidence in BTC's price.

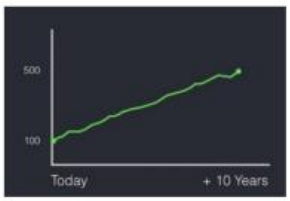
In either case of a limit or market order, the buyers of last resort fall into one of the following categories (shout at me on Twitter if I'm missing one):

1. People paid in bitcoins. Their employers or clients may already own bitcoins or have to go buy them, in either case people receiving bitcoins as income are the economic equivalent of buyers. The value of the transfer is likely denominated in USD, so the demand pressure is constant.
2. Recurring buyers. For example, someone who set up an auto-buy on Coinbase, every two weeks they market buy BTC regardless of what is happening with the price. Some have even forgotten they have it on, like a monthly charge for a gym they don't go to anymore. Individually it may be a small $50 buy, but in aggregate these accumulators could be a large pool of buyers of last resort.
3. Windfall buyers. They've been wanting to buy more BTC for a while now, and their employer just had a successful IPO or they landed a big new client. They take the cash from the windfall and go buy a nice spot on the UTXO set. The timing is unrelated to the BTC price.

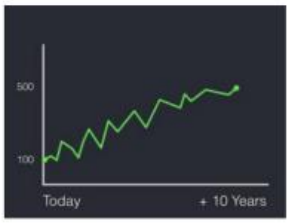
4. Opportunistic buyers, market timers. They sold the BTC top or knew the market was overheated. They're back to buy the bottom.
5. Relative value and flight to safety traders. This can range from someone selling their altcoin mining rig for bitcoins, to someone dumping their portfolio of distressed illiquid ICO tokens for bitcoins. They were trying to make more bitcoins during "alt-season" and now they are guiding their ship of bags into port during the storm.
6. Transactional buyers. They're not actually speculating on the price of BTC, they're buying to use the underlying payment rails. The person they're sending value to may be quick to sell, so transactional buyers only affect the market with the residual amount and time held. Individually this is small but it can add up, especially as the "Bitcoin economy" scales up and closes the loop between buyers and sellers. We'll also end up seeing transactional users who are buying BTC to fund Lightning Network channels. There are also lower-velocity transactional users, for example corporate multisig contracts, using properties unique to Bitcoin's programmable money.

Together, Bitcoin's buyers and holders of last resort help break the negative feedback loop in a bitcoin exchange rate crisis, setting up the base for the next bull market. Is being a buyer of last resort a sensible approach to speculating on the value of BTC? If you think that Bitcoin is going to continue to attract adopters due to BTC's monetary properties and the network's payment processing capabilities, buying into a volatile bear market is indeed sensible and here's why from Wealthfront (they're applying it to equities but this particular point about the price path is relevant to BTC)...

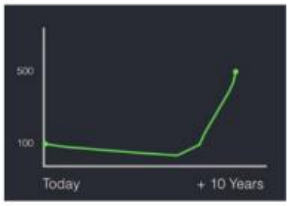
Many facets of investing are counterintuitive. Investment strategies that feel right seldom are. A classic example of this is how to deal with market volatility. During a recent investment seminarI gave to Dropbox employees, I asked the audience which type of market they would prefer to invest in periodically each year if they didn't intend to withdraw their money until 10 years from now. I showed them the three charts below and asked them to vote.



Market Behavior Chart A



Market Behavior Chart B



Market Behavior Chart C

You probably won't be surprised to learn that Behavior Chart A was the vote's biggest winner while Behavior Chart C garnered the fewest votes. However, you may be surprised to discover that **Behavior Chart C actually displays the best market to invest in**and Behavior Chart A is the worst.

Read the full piece here. Granted, these charts are assuming a positive outcome. Could BTC continue to drift downwards and never see another parabolic bull market? To make that case you would have to point to a fundamental break with the past: a material, negative change to Bitcoin's ability to attract new adopters. We've seen positive changes over the past few years like SegWit and an order of magnitude increase in liquidity. There are more positive changes on the horizon from the Lightning Network to financial infrastructure.

Whether you are a buyer of last resort buying $20 or $2 billion worth of BTC, please work with a financial planner to see how Bitcoin fits with your financial objectives and experience, time horizon, risk tolerance, and financial situation. Don't over-extend yourself and become a panic seller of first resort!

Bitcoin's Existential Crisis

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

By Nic Carter

Posted October 31, 2018

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

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

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

The Ship of Theseus Paradox

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

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

This comes up even in human contexts: Your cells replace themselves so often that the present you shares very little physical matter with the version of you that existed a decade ago; prisoners held for violent crimes are paroled with the assertion that they have become "a different person" in some vital sense; or—perhaps the simplest example—you might at some time have credibly apologized the day after an

intoxicated argument by asserting, “I wasn’t myself last night.” In all these cases, the person is clearly the same person in one sense of identity, but in another sense, many of the traits that make up the person are mutable.

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

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

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

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

The Theseus Problem of Blockchains

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

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

Both sides had credible cases. There was no constitution that specified, one way or the other, that Bitcoin’s blocksize was permanently capped or that Ethereum couldn’t use a hard fork to reverse (ostensibly) illicit transactions. (Ethereum has a

formal specification, but that is a more technical rather than constitutional document.) Instead, there were messy processes of social-consensus formation, appeals to authority, deep readings of original documents, and, ultimately, rancorous splits.

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

Two Approaches to These Problems

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

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

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

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

The other approach is to throw caution to the wind and spurn any external marker of identity, relying instead on an intersubjective consensus, such that the system can change over time while remaining faithful to its original goals. This is the approach leaderless (or, more accurately, leader-minimized) systems like Bitcoin and Monero go for. Of course, there are influential individuals in both systems, but neither has a

foundation or corporation in control of a trademark or a clear decision-making body. Many critics would say that Bitcoin Core, as the author of the dominant implementation of Bitcoin, wields disproportionate control, but that's a reductive reading. It is not an official body, and the dominant implementation that they create does not define the essence of Bitcoin but rather its instantiation. Pierre Rochard puts it well:

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

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

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

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

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

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

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

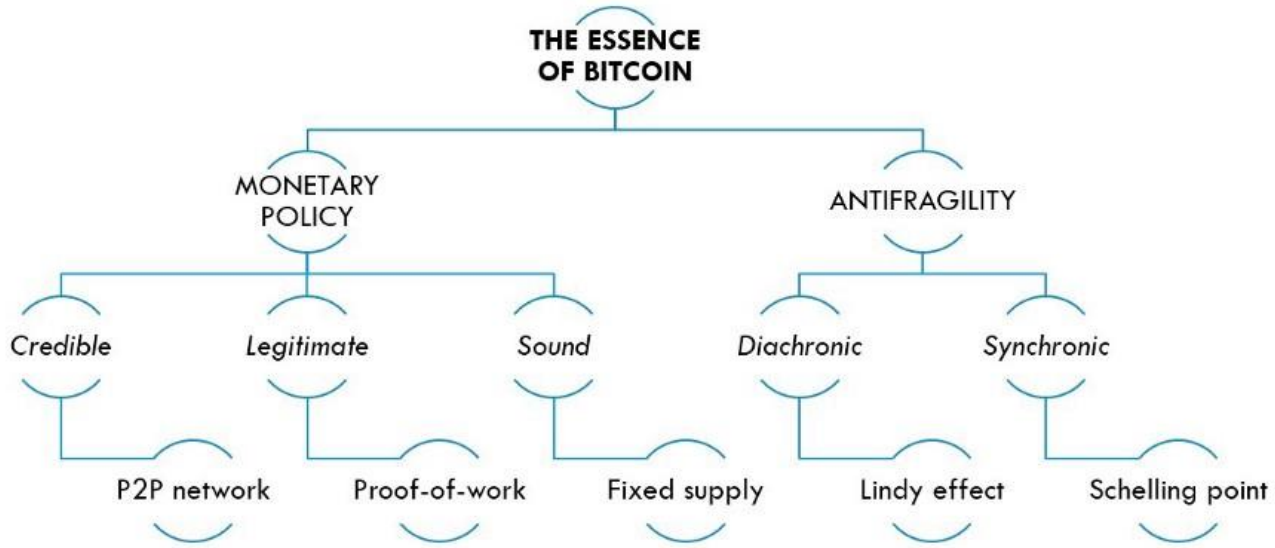
One Solution to Leaderless Identity

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

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

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

The challenge is that these rules cannot be "found" anywhere. Much like the U.K.'s government, there is no single written constitution. The rules aren't in the white paper, which is incomplete in many respects. They aren't exclusively in Satoshi's writings on the mailing list or the forum—and given his departure after two years, Satoshi sought to resign from the position of ultimate arbiter anyway. The system is best described by the original codebase, although that has changed over time. More fundamentally, the core values of Bitcoin are an intersubjective agreement around a few concepts. David Puell makes a credible attempt to capture it here:



Source: [David Puell]

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

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

Toward a Bitcoin Ontology

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

In this context, it is not only difficult to forge consensus on key technical issues but also to organize the expenditure of political capital to actually implement those changes. The dispersion of decision-making power and the lack of a unified developer entity is the "problem of governance" that Bitcoin is said to suffer from.

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

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

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

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

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

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

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

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

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

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

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

---

Murad Mahmudov: The Ultimate Bitcoin Argument

Anthony Pompliano interviews Murad Mahmudov

Posted October 31, 2018

The following is a transcript of a conversation between Anthony Pompliano and Murad Mahmudov, one of the highest conviction Bitcoin Maximalists in the world, about what Bitcoin is, how it works, the importance of its deflationary monetary system, why all Fiat Currencies are doomed to fail, and how central banks and institutions should be thinking about Bitcoin.

You can find the recording here: ***Off The Chain Podcast: Anthony Pompliano and Murad Mahmudov***

Anthony Pompliano: All right, guys, I am here with Murad. We are going to do our best to create a podcast episode that becomes the de facto episode you can send to

people when they ask “What is BitCoin, and why is it important?” So Murad, tall task in front of us but thank you for coming.

Murad Mahmudov: Thank you for having me, Anthony, pleasure to be here.

Pomp: Absolutely. All right, so before we get into this, let’s go through your background, and then we can jump into everything.

Murad: Sure. So I’m originally from Azerbaijan, was until recently an international student here in America. Got into BitCoin quite heavily after spending a semester abroad in China during the previous bubble in late 2013, early 2014. A lot of the exchanges back there, as you may know, still didn’t have tremendous liquidity yet, and some of my foreign friends were trading BitCoin P-to-P, sort of bringing it into China, selling it, et cetera. Attended a bunch of Beijing meetups, and sort of been in the rabbit hole since.

Murad: Made a small pause, as many of us have, up to 2015, and then as 2016 rolled in, got back into this game. Briefly worked in finance, and then now doing several different crypto things full-time.

Pomp: Absolutely. So let’s just start with the simplest question, right. What is BitCoin?

Murad: This is a very good question, and a BitCoin is something that can be described with more than 100 different definitions. A lot of people debate what they are, but to me personally, BitCoin first and foremost is a new form of money. It’s a new form of thinking about money, storing money, transferring money, and just dealing, organizing, and understanding money, and all kinds of second order financial effects that come out of that.

Pomp: Absolutely. So let’s walk through some of the core components of BitCoin. Obviously, it’s built on a blockchain, and then it is divisible, it’s fungable, it’s all these things. What are the important components to you?

Murad: Blockchain is definitely one of the components. A lot of people thing that that’s the core one, but really, that’s one out of four or five core moving pieces. I don’t wanna give the term ‘blockchain’ too much legitimacy right now, because it’s really been over-abused, I would say. Up to this point, it has become little other than a marketing term at this point. I mean, I’m not as fascinated with blockchain as I am fascinated with the BitCoin blockchain, but as I said, there are many moving parts.

Murad: Another is the proof of work function of BitCoin, and how the time-stamping and the security come into play in this regard. BitCoin governance, in particular, is very very unique and very very complex and hard to understand, hard to explain. I just want to underline the fact that it’s not just a currency on a blockchain, it’s really

very very interdisciplinary, and multi-variable phenomena, where a lot of different things come into play and blockchain is merely one out of several.

Pomp: Absolutely, so let's go into proof of work. How does that work, and why is it important?

Murad: Proof of work is very important because it is the first workable, in my opinion, solution to the double-spending problem at scale. As we know, a lot of different alternative currencies and alternative money forms were created in the 90's in the early 00's. Unfortunately though, they didn't work quite well, because most of them were centralized more often than not, of course.

Murad: When something is centralized, it is very easy to shut down. A privilege of creating and controlling your own money, let alone a monopoly on it, is something that gives the controllers of that system a tremendous amount of power, arguably more than anything else in the world. With BitCoin, proof of work, once again coupled with several other things, allows the system to be secure and decentralized at scale, as well as allows us to time-stamp transactions on the ledger in a decentralized trustless, or rather, trust-minimized manner.

Murad: Which allows BitCoin, for the first time, to be an alternative monetary system and an alternative currency which is several orders of magnitude much harder to shut down, to censor, to stop, and to manipulate, than any other project of a similar variety that has ever arrived in the past.

Pomp: Absolutely. So this idea of the decentralization, right? In a centralized world, whether it's the traditional banking system or other attempts like DigiCash, Hashcash, BeMoney, et cetera, the centralized versions don't have the double-spend problem, right? So the double-spend problem is this idea, if I have a single U.S. dollar, physical dollar, and I give it to you, I no longer have a dollar that I can give to anyone else. So I only can spend that dollar one time.

Pomp: In a digital currency, the actual unit of value is a digital file. It could be copied, and so therefore the problem that many of these early attempts to build a digital currency ran into, is the doubles-spend problem you described. That was where I give you one unit of value, one BitCoin, and then I would be able to send that exact same unit of value to somebody else, therefore spending it twice, double-spending it, right?

Murad: Right.

Pomp: The blockchain structure is what solved this. Do you think that the solving of that double-spend problem is why BitCoin has been able to thrive when other previous attempts didn't, or do you think it's something else?

Murad: Technically, centralized currencies and centralized financial systems have a double-spend problem as well. However, in order to solve it, you need to … we need to place our trust in a central party, in a centralized authority, who often control the transactions, they control the settlement, they control the issuance of the currency, they control many different things, right?

Murad: Sitoshi, in one of his earliest posts on the cyberpunk email list, he noted that the traditional currencies have several layers of trust that you have to essentially give in to in order to use the system. You need to trust the central banks not to dilute the currency too much. You need to trust commercial banks that they're going to let your transactions through, et cetera, et cetera, et cetera.

Murad: The amazing thing with BitCoin is that, now in a very very unique way, Sitoshi Nakamoto has managed, in a very elegant way, combined several innovations together, one of which is proof of work Hashcash, together with a chain of blocks, as well as several other things that we can get into, to create a digital currency where the double-spending problem is solved in a trustless manner. This allows as Nick Zabos says, for the system to be much more socially scalable than anything else we've had before. A lot of anthropologists have argued that expanding social scalability with various technologies that allow us to connect with as many people as possible, in a way where we don't have to rely on any single party, with more and more inventions of this sort we can really expand the horizons of commerce and human civilization at large.

Pomp: Absolutely. Those previous attempts at this all either had lack of adoption or they had technical problems. There was issues that they couldn't solve. One of the things that often doesn't get talked about with BitCoin is the governance. Everyone is focused on the technology itself and how that is executed. What is so special about the governance of this digital currency?

Murad: Governance of BitCoin is not formally defined, and I would argue that in a way, it is a strength rather than a weakness. Technically, the governance has to do a lot with the BitCoin improvement processes, and how those get proposed, and how those get reviewed, how those get added in, et cetera. It's a very conservative, extremely meticulous process, which I consider a strength. A lot of people consider that, a lot of people complain that BitCoin is not evolving or BitCoin is too slow.

Murad: To me, those people are exhibiting high-time preference and impatience. I think the alt-coin boom and the ICO boom, a lot of the blockchain boom as well, has it's origins in part because of this. True BitCoiners understand that this isn't a six-year get rich quick scheme, but it can be an 80 year project. It's something that perhaps will continue going on until the end of our lives. So every changes to the system, need to be extremely extremely careful.

Murad: I like to compare it to a nuclear reactor or heart surgery or a moon mission, because there's a lot at stake. 100 billion … more than $100 billion already, and potentially tens of trillions of dollars someday. So this … because it is software, it lends itself to flexibility. This malleability has allows us to create a money that is harder and sounder than gold, and fiat, of course. But at the same time, this malleability is also makes it fragile in a number of other ways.

Murad: Because of this, and precisely because it is software, we need to be extremely careful. But the governance process of BitCoin is what Pierre Rashad calls a P-to-P anarchic network governance. The fact that it is slow to change is something that really makes BitCoin far, far stronger than everything else. The number one reason, and I can give dozens of reasons, but the number one reason why alt-coins are far, far behind BitCoin is precisely because they are much more centralized in relative terms, and everything about it is much easier to change.

Murad: Currencies, first and foremost, are all about trust. As I like to repeatedly say, these crypto-assets are unlike many people in the VC world, San Francisco, California, they think of these things as software platforms. They try to apply the late-00's early-10 tech paradigms to this thing, but really to me, it's a monetary phenomenon. In very loose terms, I like to describe these things as digital monetary metals.

Murad: To me, that's arguably the closest metaphor for now. I like to even say that they aren't, BitCoin being compared to digital gold is an understatement. Really what it is, is digital monetary nuclear weapons. Because if you really dig into the third and the fourth orders game theoretic effects that are likely to arise when this things gets just a little bit bigger, which to me, it inevitably will, there's just so much that it is going to cause and reorganize in this world.

Pomp: Absolutely. One thing that I think about a lot, is if you were to draw a spectrum, and on the left side you have the slow development cycles and carefulness of BitCoin, and on the right side you have optimization for innovation. I think that BitCoin obviously is pretty far on the left side of that spectrum, and a lot of the ICOs and alt-coins, et cetera, are pretty far on the right side.

Pomp: They wanna quickly build something, they wanna get it out, they're trying and experimenting and innovating and doing all these things. So what ends up happening is, because BitCoin's speed of development is slower, more methodical, more intentional, it can pull from the things that work on the innovative end, and it can avoid the landmines of the things that don't work. Do you agree with that?

Murad: I agree with that, and I would even add that a lot of people who've started alt-coins have gotten into that wave in the last couple years, come from the technology world or the startup world, venture world, and one of the schools of thought, i.e. move fast and break things, it completely does not work for

cryptocurrencies. Because once again, this is not a dog-walking app or a dating app, or a food picture app.

Murad: You need to be extremely extremely careful with this. We want to make it so that a huge chunk of the world financial system eventually gets absorbed into this one digital currency. So conservatism is definitely the way to go here. Some people would even argue that we need to even e more careful and review in an even slower fashion.

Murad: I definitely agree with you that BitCoin can definitely take whatever … if there's ever something that is actually useful and truly innovative that any alt-coin does better in any capacity or function, BitCoin can eventually adopt that, for sure. However, and this is why I believe that privacy coins or coins with more programmability et cetera, et cetera, they really don't stand a lot of … they don't really stand a chance against BitCoin at this point in time. Because I believe people will soon realize the truth, and the truth is that the value aka the price is determined by the monetary premium.

Murad: The monetary premium is determined by a combination of the current monetary network effects, monetary liquidity, salability, marketability, recognizability, the Linde effect, and most, first and foremost, the credibility of the monetary policy, and just the general trust. In all of these terms, in all of these criteria, BitCoin is so far ahead than everything else, that the way I see it, yes there may be two or three more mini alt-coin bubbles, particularly as more people enter into the space.

Murad: There's a natural incentive to find the next big thing, of course. I believe that once BitCoin goes above several trillion dollars or so, a big divergence will happen. Really, all the other cryptocurrencies will be similar to what penny stocks are to the big caps in the equity world right now.

Pomp: Got it. So would it be fair to say that, if you take that same spectrum, on the left side you've got security, and on the right side you have low levels of security. BitCoin conservatism pushes it on the extreme end of the left side, around security, right? Do you think that these other blockchains, tokens, et cetera, are lacking focus on security, or do you think they're making a rational trade-off between security and, let's call it innovation or something like that?

Murad: I think it's a rational trade-off. The reason for that is because if you even want to compete in BitCoin in any capacity, then you … it's really difficult to compete against it in terms of monetary disinflation, which really is the most important thing here.

Pomp: So what you're saying is, if somebody wants to compete against BitCoin, another project, you can't beat it on security today, because of the network effect. And then you can't beat it on the monetary policy, and therefore you have to go to other areas in which you may be able to build a competitive advantage.

Murad: That is most of the thinking in alt-coin creators heads. I believe that it has worked a little bit, not really. It might even work a little bit in the upcoming waves. But it is doomed to fail eventually.

Pomp: It's like winning the second or third most important aspect, right? It's like saying, look, the most important thing around security-

Murad: It's like sixth or seventh, you know.

Pomp: Yep. It's super interesting. Okay. So let's talk about the design of BitCoin. Obviously there's proof of work, there's governance, et cetera. But the actual monetary design, walk us through the disinflationary and deflationary nature of the actual design.

Murad: So before I delve into that, I will say, and I think this is something that people will increasingly realize in the coming years. Uncensorability's cool, unsiezeability's cool as well, but to me these really are perks. In terms of the prize going up and this thing taking over the world, if we create a pie chart, then 90% i.e the dominant force which will be doing that, is BitCoin monetary policy. Really, its unprintability. The fact that nobody can print beyond 21 million. That is by far the strongest and the most important innovation here.

Pomp: Okay, so the monetary policy of this system is by far the most important part.

Murad: Precisely.

Pomp: Okay.

Murad: People need to use something as money. Right now, some of the better currencies are the U.S. dollar, euro, the Swiss franc, et cetera. But really, people use those because essentially, they're picking the least bad thing. I believe the supply of the U.S. dollar in the last year has increased by 6.2%. BitCoin's stock to floor ratio, today, is around 3.8%, and after the next halving, if you go off of the 21 million number, it's going to be 1.7%.

Murad: Actually, I believe that that switch from low three percents to high one percents is going to be the number one driver of the next big wave in 2020. But to answer your question more directly, unlike other currencies which their respective central banks, in the case of fiat, can print essentially whenever they want, as well as their respective local commercial banks can create more of when issuing that.

Murad: BitCoin is limited to strictly 21 million units. Some of them, it is believed that several million have already been lost. I believe that when all is said and done, the global supply of BitCoin is going to be somewhere between 16 and 17 million. The fact that nobody can print beyond the 21 million limit, and the fact that the users, the miners, and essentially everybody in … the developers, everybody who has as little as one Sitoshi of BitCoin, they are incentivized in having that rule be the number one and the most important rule, and the number one focal point, the number one selling point, which the community is gathered around.

Murad: Really, this is the number one thing which allows BitCoin to continuously increase in value. People are already pricing in, it's extreme scarcity. I like to say we've never had an object, let alone a money, as scarce as BitCoin before. Even gold is expanding at a rate of around 1.6% per year over the last 10 years. I believe that after … by the late 2020's, that number for BitCoin is going to be lower than one percent. Every year it's getting lower and lower, so technically, that number is getting lower every ten minutes.

Murad: As you might know, every four years there's a particularly additional sharp drop as well. I believe that that soundness, that hardness of currency, isn't palpably felt by people yet. Even a lot of participants in the market, a lot of traders and investors, they don't really quite grasp this aspect yet. But I believe that this is the revolutionary thing here, and this is why I believe BitCoin is going to be in the hundreds of trillions, in today's terms, in the future.

Pomp: So there's a couple of key terminology and components that you just described. There's the total supply of BitCoin, right? So when it's all said and done, 21 million BitCoin. We can get into why that is, and if that could change or not later. But for right now, let's just say that there's 21 million totally supply of BitCoin.

Pomp: At the same time, there's the circulating supply. So how many BitCoins have been produced, and are currently available for ownership by people or organizations? And then, what we see is, every ten minutes, every block, there are more BitCoin that are added to the circulating supply, but that 21 million fixed supply never never changes.

Pomp: So what occurs is, the disinflationary, right? So yes, the circulating supply continues to expand until it reaches that 21 million, but that number goes down every four years or so, in terms of how many BitCoins every ten minutes are added to the supply. So that's a disinflationary model. What you described is, once all 21 million BitCoin have been mined or are now part of the quote unquote 'circulating supply', we now get into a deflationary model.

Pomp: So it's no longer disinflationary, because actually there's no more being added, and now we can only go reverse. We can only lose BitCoin in the circulating

supply. So let's talk about the pros and cons of an inflationary system, and the pros and cons of that deflationary system. I think people hear these terms, but they don't really know what they mean or why there's pros and cons to either side.

Murad: We're taught in a lot of schools and the contemporary mainstream neo-kings, anachonomists argue that mild inflation is best. To me, I think that governments around the world, particularly in the Western world, are incentivized for that kind of academic discourse, to be the dominant one even in the best institutions.

Murad: In my research I've found that there's a lot of academic grants and academic sponsorships financing that central banks and ministries of finance, ministries of economics, et cetera, that allocate to certain schools of monetary thought than others. But I believe that those currencies are local monopolies, and those currencies are forced upon us from top down. BitCoin is a free-market phenomenon.

Murad: I would argue that BitCoin is an experiment in Austrian economics that so far, in it's 10 years of existence, is succeeding massively. My belief is that money is a product, just like anything else. I think we will not have truly pure capitalism and truly pure free markets until money, which is a product that we utilize ... which is a product which is a half of every single transaction in our society, is something that originates from the free market as well.

Murad: I believe that money is ultimately a product of the market, rather than a product of the state. I think the last 47 years in history have ... are a temporary phenomena. For thousands of years, gold was the predominant money, or gold and silver were the predominant two currencies around the world, until the paper notes became more widespread as a technology. You can think of paper notes as a layer two technology, on top of monetary metals.

Murad: At that point, once you had paper notes, which were redeemable for metals, there was no longer ... the divisibility problem of gold was solved, so the need for silver was drastically reduced, and thus silver was demonetized further. It's very interesting to look at the gold/silver price ratio. After 1881, you see gold skyrocket in silver terms.

Murad: But I believe that something similar will happen with BitCoin versus all other monetary instruments, and even other financial assets. Which is really quite eerie. I think that when all is said and done, BitCoin will be the second or the third single biggest asset class, the single biggest asset in the world. Maybe real estate will be the only one bigger.

Murad: This is my reasoning around this. Right now, it is believed that the total money supply of all fiat currencies around the world is somewhere around $80 trillion. If you consider M1, M2, M3, if you add them all up around the world. I strongly

believe that that number is artificially diluted and artificially kept small, because essentially by continuously printing, governments are disincentivizing the world, and disincentivizing investors and even average people, to store too much money in currencies.

Pomp: And they're doing this because, if I take $100 and I put it in my bank account, as they print money, that $100 loses purchasing power every single year.

Murad: For sure. Every single day where the money creation occurs … it's interesting, because the cost of creating that money for the government is near zero. All it takes is just a push of a button. But essentially, every single unit of fiat currency that gets created, reduces the wealth of the fiat holder around the world.

Murad: BitCoin is an unimaginably new phenomena, where for the first time, nobody can seize your wealth. Not just directly, like they did with gold in the 30's, but just like they do with stealth inflation in fiat. Nobody can print more. For the first time, you have this currency that you can have full, or at least very strong confidence, that for the rest of your life, the percentage of the money supply of this entire system will always remain the same. Which, really, is completely unprecedented, because even with gold you don't have that.

Murad: So here's the thing. The total amount of wealth that is stored in currencies is artificially small. People … essentially, the system doesn't want us, and doesn't want people, to have a good robust unseizable store of value, because if that were to exist, then governments and central banks would lose a tremendous amount of seniorage privileges, because every time they print, they essentially enrich themselves at the expense of everyone else a little bit.

Murad: So this current system, because the money's constantly getting diluted, people like surgeons, artisans, dentists, et cetera, engineers, they either have to play part- time investors on the side, or they have to outsource those services to registered investment advisors and brokers, et cetera. That's part of the reason why the financial system is much bigger than it has to be, and why Wall Street is just a ginormous part of the world's economy.

Murad: If we had something like gold, or better yet, BitCoin, then you could save your wealth and it would actually gain a little bit of purchasing power every year, without having to have this anxiety-riddled wave of activities that you need to do. It's actually quite crazy how in today, I'm not even talking about the second or third world where this isn't even an option, even in the first developed, civilized Western world, you have to create a diversified portfolio of equities, bonds, small caps, moonies, commodities, FX, derivatives sometimes, et cetera, just to preserve your wealth.

Murad: I'm not even talking about making some termendous outside returns. I'm talking about just to save your wealth. This is crazy. In the Biblical times, there's a famous Jewish proverb which says, "Keep a third of your wealth in money," which was gold, "keep a third of your wealth in land, and keep a third of your wealth in your business." Even as recently as in the 50's and 60's, you could notice that in portfolio allocations, some of the traditional mutual funds and the early big asset allocators, they had a much bigger allocation to cash when the trust in currency was much greater.

Murad: You saw that reduced as years went by, and in recent decades with quantitative easing, the trust in currencies gets incrementally reduced. I believe that if BitCoin were to become global money, which I believe it will, or something like it definitely will, because genie's out of the bottle and the idea is here to stay forever, the percentage of people's average portfolio that will be in cash as opposed to today will be much greater. Perhaps not a third, but it will be much higher than it is today, and much closer to a third than it is today.

Murad: Precisely because of that, I believe that the total wealth in the world that is held in a currency, and note that this one currency will not be inhibited by inflation, it will not be inhibited by borders, it will not be inhibited by centralized control. All these things will contribute to it being the single biggest currency in the world. I think that eventually, I incresingly believe that the cryptocurrency market, even soon, not just in the future long-term equilibrium, it will be a winner take all rather than a winner take most game. I believe that BitCoin, as it currently stands, will probably take 94–95% of this entire market.

Pomp: So there's a lot here to unpack, and I think it's really important. What you're describing is the idea, an inflationary model like what we have with the U.S. dollar for example, incentivizes me to get out of cash, and get into either hard assets, or to spend that capital, because if I hold it, it loses value. So that inflationary model, for many people, they spend or they take that cash and they buy real estate, or they buy other investment opportunities, because they know that they have to at least do better than two percent on their yield for the year. Because if they leave it in cash, they're gonna lose two percent, give or take, based on inflation.

Pomp: So the argument that you're making here is, let's take, I don't know, 5–10–20–30% of the real estate market, is actually wealth preservation, right? If people were given the choice, rather than buy real estate, they would rather take that exact same value and hold it in the cash equivalent. They don't do it because today that loses money. But if there was a global digital deflationary currency, the-

Murad: Deflationary currency. The real estate total market cap would shrink because people would move from real estate back into that global currency, and this would

not only happen in real estate but a number of, kind of store of value type asset classes where people today find safety to get out of cash and preserve wealth, but that may not be true in the future.

Pomp: Precisely. And I think that this really, the global total [inaudible] market for monetary instruments is a zero sum game. For bitcoin to win, other things have to lose.

Murad: Other currencies or other asset classes, or both?

Pomp: Both.

Murad: Both. And that is part of the reason I believe that bitcoin, the single currency will be bigger than, in their "market cap" or in the amount of wealth that is stored inside it will be greater than not just any, but all of current Fiat currencies and monetary metals added together because I believe that bitcoin is such a good store value, that it will take more than 95% of the current market cap of Fiat currencies. It will take more than 75% of the current market cap of monetary metals, and then, and this is sort of the interesting part, I think because the current Fiat currencies are inflationary, a lot of the high net worth individuals and asset managers around the world use the stock market, use the fixed income markets, use the real estate markets as a store of value. That is part of the reason why, if you try to buy an apartment in Tokyo, London, or New York, the prices are insane, and this is because both American high net worth individuals and foreign high net worth individuals use these sort of prime city luxury apartments as one of their stores of value. And I believe that sort of because the Fiat currencies are constantly diluted, at the same time this has caused an artificial sort of increase in the value of other asset classes and other financial instruments as people are hunting for yield.

Murad: The aggressive sort of quantitative easing and the aggressive sort of unorthodox negative interest rate monetary policies of some central banks says the financial crisis have exacerbated this effect even further and if you look at the inequality and the Gini coefficient it has increased sharply since 2008, in the last ten years even more.

Murad: One of the reasons for that, out of several, I mean of course it's a very multi varied topic but one of the reasons because the working class and the lower classes, they mostly store their wealth in cash. Most of them live pay to paycheck and whatever savings they have, they do keep it in cash.This for simplicity's sake.

Murad: Now the asset owners are those who own real estate, stocks, bonds, et cetera, and a lot of the wealth has flown there, and a lot of people although essentially the people who've benefited the most from this grand wealth effect experiment are people who are holding these assets. Much of the time it is the central banks

themselves who are indiscriminate and price insensitive buyers of these financial instruments.

Pomp: So this is imporqtant because there's a thought process that inflation is merely the act of stealing wealth from the poor and enriching the elite and wealthy.

Murad: Right.

Pomp: And, so what that means is, if you live paycheck to paycheck, and you leave a high percentage of your net worth in cash, then every year, you're losing value, or you're losing purchasing power. But if you actually have other assets, and a lot of them, inflation continues to drive the price of those assets up and therefore, those that own non-cash assets actually benefit drastically from inflation and are incentivized to keep the party going.

Murad: Right.

Pomp: And so, if you switch to a deflationary model, actually the people with the preference to have a high percentage of their net worth in the currency will benefit drastically and those in non-cash assets will actually not benefit in this scenario.

Murad: For sure. And I like to describe bitcoin and sort of the entire phenomena as a grand wealth transfer event and I believe that it will be arguably the single biggest wealth transfer event in human history. It will be a wealth transfer from the old to the young, from the tech savvy to the more conservative, from the open minded to the more closed minded. And of course from the people who will be holding these crypto assets, most of all bitcoin, and the losing side in this case, will be the people holding Fiat currencies, gold, et cetera.

Pomp: Absolutely. So, let's say that everything you've described is true, right? And you just laid out the blue print for how this is gonna play out over the next, decade, 2, 3, 4 decades, right? How big is the opportunity? Right? What is the market cap of bitcoin 10 or 20 years from now?

Murad: So, before I answer that question I'll say that as bitcoin, let's say in six to eight years from now, as it- it's a bit bigger, much more volume, much more Lindy effect, much more trust, much more credibility, et cetera; much more mainstream. People will simply compare two things and bitcoin, will be in a free market battle against Fiat currencies and gold simultaneously, and even other things when you just isolate the store value component as we have discussed.

Murad: People will simply say, Okay, this thing is expanding at 6% per year in its supply, and this thing is expanding at 1% per year in its supply. Which one should I pick as a store value?

Murad: And that's why to me, sort of this feed back loop is inevitable. It would be so difficult to stop-

Pomp: The math becomes undeniable.

Murad: Really, if you extrapolate this phenomena and extrapolate this sort of financial change, bitcoin will be a black hole that will absorb a tremendous amount of value. I believe, the total addressable market is somewhere between 100 and 200 trillion. I'd like to say it will be 160 trillion, so if bitcoin, and that is if we go off of the $10 million dollars per bitcoin price, in today's terms without even counting the inevitable hyperinflation of Fiat currencies. And, so this is my reasoning -

Pomp: So, you think that a single bitcoin will be worth $10 million dollars?

Murad: In today's money,

Pomp: mm-hmm (affirmative).

Murad: Yes, I do.

Pomp: Which would give us a market capital of what? Like a hundred and ...

Murad: 160 trillion. Right now the current market cap of bitcoin is 110 billion. I believe when this bare market is done, give or take, will bottom somewhere around 80 billion, and so, that's a 2,000 x that is still possible between right now and what is probably our death, and I think there is still a tremendous opportunity here. And I think high net worth individuals are more edgy, open-minded, tech savvy institutions, and eventually, government institutions will push this to the extreme.

Pomp: These are big numbers you're talking and you realize that very few people in the world believe what you believe right now.

Murad: I realize that but, if you spend months and months studying this, it sort of becomes self-fulfilling prophecy to you. I'm very confident bitcoin will be bigger than the U.S. dollar and potentially even bigger than all of them combined. Because, there's an interesting table that Vijay Boyapati has made and he says that crypto currencies, or bitcoin in particular: are harder to tax, harder to seize, easier to transfer, harder to steal, cheaper, easier, faster to send around the world. They're borderless, they are uber competitive, they're highly deflationary, et cetera and there's dozens and dozens of reasons. And all of these combined, I believe, will make bitcoin incredibly big. Similar to what the gold standard was in the late 19th century but, given the fact that the economy is much bigger today and given the fact that it is digital and much more fluid, I believe it will be far, far greater than even that, and yeah, these are my thoughts.

Pomp: Absolutely. So, let's talk about this idea of hyperinflation in the Fiat currency experience. Our experiment, right? So, 1971, was it, Richard Nixon takes us off the gold standard. The gold standard being the thought process that for every paper currency, every U.S. dollar, you could go and redeem the equivalent in gold, where it was being held in the central banks.

Pomp: At the time, what a lot of people don't realize is, Richard Nixon said, We're gonna go back to the gold standard. It was a temporary decision, right? Or, at least that's how this was presented.

Pomp: And so, we obviously didn't, and since 1971, what we have seen across the world, at different times and different locations is Fiat currencies start to fail. And these Fiat currencies, where they appear to be failing most, is in regions or countries where a government or the overseeing organization loses discipline, right? And the thought process is, in the developing world, we have much more discipline, right? There's checks and balances and the Fed can't press the print button too much, right, because there's those checks and balances. But let's say in a country where a dictator comes in to power, there's less checks and balances. There's a higher probability that they will lose discipline. They can hit the print button too much and you get into hyperinflation, devaluing other currency, and we know how that ends, right?

Pomp: Let's talk about that hyperinflation period. Why are we seeing this in the countries we're seeing it today? And do you think that this is gonna happen to every Fiat currency in the world? Why or why not?

Murad: I believe it's a combination of incompetence as well as outright grasping for power. And, I do believe that this will eventually happen to all Fiat currencies around the world, but it will happen stage by stage. Of course, the second and the third world currencies will be the first to collapse, and the more established Euro, then Dollar. The financial leak from there towards bitcoin will be a bit more gradual. It will be more like an "S" curve and then it will reach a point where the money will just rapidly flow into bitcoin, because as I've described, people will realize that this money is harder than the other one. The other money, there's people behind it and these people can do whatever they want. However, this is governed by such a strong, unbreakable algorithm and the community of people strengthening it, that I believe the credibility, and the faith, and the trust in bitcoin relative to Fiat currencies will keep growing. And as I've said in the beginning, currencies and the cognitive monetary premium that's placed atop them is, first and foremost, it's about trust and it's about credibility.

Murad: The Swiss franc, for example, people like it because the Swiss don't print too much. They have 300 years of credibility. They have temperance, they have discipline, as you've described. And it's important,[Savty Namoose 00:45:09], in his work, he

often says that hyperinflation has never occurred with metals, because there are natural limits to creation and there are natural free market balances there.

Murad: But, in 99% of cases, it has occurred in Fiat currencies because they are the behest of humans, and [Jorg Gudahusman 00:45:30], who's arguably the most prominent Austrian communist today in the world. He says that, this money supply inflation has traditionally been the means of financing war. But, as of late, it's not just used in wartime, it's being used perpetually. And I'd like to say that, this inflation, it essentially shifts some activity from longterm projects and longterm capital goods production, to more short-term consumption.

Murad: I'm a believer that it is not the consumption that really drives the sustainable longterm growth of the economy. The kind that actually increases our quality of life, but rather us engaging in longterm projects, longterm capital goods production. Longterm production of: tools, instruments, research, innovation, and things like that. And really, the best things that have ever been created, they were 10, 20, 30 years efforts. Rather than us going and buying something useless, right?

Murad: And so, I believe that if we have a currency that's more deflationary, people will be incentivized, instead of going out there and as you've described, investing in something else, or even buying a pack of crisps or just new shoes, or really, something that's really useless right now. Instead, people will be, just due to the deflation and nature of it, it will be seen and felt as more precious. People will be more incentivized to: A) save and B) invest in longterm projects and longterm craft.

Pomp: Absolutely. And so I think with this hyperinflation, right? What we're seeing for maybe the first time or one of the first times. Humans have a choice. Do I trust the machines, the software code, the math, right, and the algorithms? Or do I trust the humans? And, as more people elect to take Fiat currency and convert it to bitcoin, they are electing to trust the machines over the humans, right? And I've described this before as, the machines are unbiased, they're unemotional, they're disciplined, and they do what they're supposed to do.

Pomp: The humans are undisciplined and greedy. And, when you lay it out that way, I think this is gonna happen in a lot of different facets of our life, right. You already see some of this with the advent of Uber and that type of stuff. But, with money specifically, the problems arise from human lack of discipline, and therefore, as more people trust the machines, they are rewarded because money acts how money's supposed to act. Agree or disagree?

Murad: Definitely. I definitely think we'll see a similar phenomenon in different sort of facets of technology and capitalism as a whole. And, as I've sort of described in the beginning, bitcoin- I don't wanna use the word entirely trustless, because there are still certain things you can trust- but they are far, far more distributed and in my

opinion, harder to change than centralized solutions. And this allows commerce to happen on a global scale, and this allows you to trust this payment rail like never before.

Murad: Bitcoin is extremely secure and it allows us to- I believe another thing that it will do to finance is, it will eliminate the Forex industry completely because if we only have one global currency instead of these dozens of currencies that we have today, hundreds of currencies, then the foreign exchange market will cease to exist because we will just have one currency.

Murad: Hans-Hermann Hoppe describes the current state of affairs and the state of Fiat currencies as a mild state of barter. Whenever one company or one corporation in one country has to do business with another they first have to exchange their currency to another country's currency, then need to change that for goods, and then need to go back and forth and every time. So it's kind of like barter, in the sense that you first need to make these extra transactions. But with bitcoin, like several layers of those transactions will just get abstracted away. And I believe that this will expand the economy, and accelerate capitalism and free markets, and borderless commerce even more.

Pomp: Absolutely. So, all right. Here's what I wanna do. I wanna play devil's advocate, right? I wanna take the seat of the bitcoin detractors, the people who don't believe or think that your view of the world is wrong, right? And so, you- I'm gonna throw some ideas out at you and some detraction and you kind of respond as you see fit.

Pomp: Can bitcoin go to zero?

Murad: I believe that theoretically it could. But with every ten minutes that it successfully adds another block to the blockchain and doesn't fail, the probability of that is reduced every ten minutes or every single day.

Pomp: Okay. So there's a non zero chance it could happen, but the addition of time makes it less likely.

Murad: Precisely. And this is precisely where our constant discussion of Lindy effect comes from. The longer a piece of technology like this exists, the more likely it is to persist even more in the future. And the longer it exists, it also gives trust to the people, because say you discovered bitcoin in 2011, a lot of us thought oh, it's a joke. It's whatever. We've seen that before right? Now you read again in 2013, you're like oh, this is still not dead? In 2015, you're like oh, this is still here?

Murad: Now in 2025 people are going to be oh, this thing is here for almost 20 years. This is here to stay. You know and oh, like, they still, in 20 years haven't printed any additional bitcoin beyond 21 million, this is really, really strong, you know? Bitcoin, yeah, it's not just the trust in the security, not just the trust in the decentralization.

But also the trust in the currency as money is also growing, which is very, very important. And, like I've said, trust in market cap over the long term is really the same thing.

Pomp: Absolutely. If it did fail, if it did go to zero. What's the most likely reason why?

Murad: Catastrophic bugs probably. It is software. And software, it's an increasingly complex software. So many thousands of lines of code. So many things, so many moving parts at the same time. And really, unfortunately, very few people of that caliber, and that are simultaneously working on these kinds of technologies right now. And so, the main 10 to 15 contributors to the bitcoin project are people. Sometimes, once every four, five years- they do make mistakes as we've seen recently with the bug. Luckily it was fixed pretty quickly.

Murad: There will be bugs. I mean, as I've said, this is a multi decade project. This is a 50–60 year project. This is software we're likely to see, 3, 4, 5 bugs more before this sort of thing takes over. But this is inevitable and as I like to think, it's better we take care of these things right now, when it's only a couple hundred billion, rather than, when it's a $ 20 trillion dollar system with the world's economy running on it.

Pomp: Of course. Okay. Bitcoin is too volatile to be a store value.

Murad: So, to me, this is the easiest piece of myth or misconception to parry, because you actually want bitcoin to be volatile. Bitcoin cannot go from $1 to being the global digital store value standard global currency without volatility. In fact, you desperately want bitcoin to be volatile, preferably upwards of course, but you do want it to be volatile especially verse a Fiat. When you use the term volatile you need to understand, volatile verses [vaught] and typically we mean, verses the U.S. dollar, right.

Murad: I think that bitcoin's volatility is great. If you zoom out and look over the last years, especially on a log chart, this volatility has been predominantly upwards and this volatility is so good, it shows people that bitcoin's strength verses Fiat currencies is strengthening. And Fiat currencies per unit of bitcoin are weakening and this volatility isn't just inevitable, it's desirable.

Murad: By the time bitcoin completely takes over and in the long term equilibrium. But a more practical answer is that, as bitcoin's trader volume grows, as bitcoin's liquidity gets deeper, as bitcoin's order book become more abundant, as more and more people cognitively recognize it, as there are more hodlers, as there are more users, as there's more infrastructure, as there's greater security. And most importantly as there's a bigger market cap, bitcoin's volatility will decrease.

Pomp: So what this tells me is that bitcoin is a net positive volatile asset, right? There's violent volatility, but over a long period of time, it continues to increase in

value and therefore the only way to go from worthless to worth a lot, you have to have volatility, and that's a good thing.

Murad: Precisely. I mean you can't have all these trillions of dollars of wealth stored in one asset, flow into another asset without volatility being there on the way. And money is really a technology. It's a financial technology that enables us to do a lot of things. And bitcoin, to me, is a far superior technology than any monetary metal or any state currency. And so people will- the world- because it is a superior technology, it will win in the free market and the world will adopt this better technology, and this better technology will expand everything

Pomp: Okay. Bitcoin can't scale. The transactions, the blockchain can't handle the number of transactions needed for a global adoption.

Murad: So, a lot of people make a very big mistake. They think of a bitcoin as exclusively a payment rail, where it's only like one of the six things it does. And they compare it to say, VISA or PayPal. Now, bitcoin, the main blockchain is sort of the layer one of the whole system. You have to think of VISA as, it's like a layer three or a layer four of the current status quo financial system. Which is like the dollar, then you have the central banks, then you have the commercial banks, then you have rails, and then you have VISA or PayPal, that all sit on top of ts thing.

Murad: And so, we will- bitcoin is also as you might know, developing layer two, layer three solutions already. Ad so those are the ones that you will eventually need to compare against VISA and PayPal.

Murad: The base layer isn't so much as a payments rail for daily transactions when you're buying crisps or a cup of coffee, but it's a settlement layer for very big, and very serious transactions that require a lot of security. Eventually, I believe the base layer will be much more expensive than it is today, but rightfully so because most of the security will come from fees. And it will be large institutions and large business transactions, large commercial transactions that will predominantly and ultimately, eventually be settled on layer one.

Murad: But I believe that trillions of transactions will be occurring on layer two if not higher. As well as possibly on the sidechains, drivetrains et cetera. But my argument, and Nick Carter has put it very, very well. He said, These are- the layer one is not partials, it's containerships. So, they will eventually be used as settlement for very, very big transactions. And if you compare it with gold, for example, today. Do you know how much it costs- and gold right now is a means of final settlement between central banks, which they do once every several years.

Murad: When moving gold from Europe to America or vice-versa, today, takes tens of millions of dollars and months, if not years in time. Bitcoin, even if you're on the math

at the very equilibrium, the price to settle, like several billions of dollars on layer one of bitcoin will still be [inaudible] cheaper than you can do with gold today. Which is still a huge, huge advantage and all of those daily, small, minuscule transactions that doesn't require hypersecurity and hyperdecentralization, will be done on much cheaper, much faster, layer two, layer three solutions, which sacrifice some security for greater speed, greater availability, et cetera.

Pomp: I think that's fair, that bitcoin is not being compared, not to the U.S. dollar, which it is superior to in a lot of ways, right. But, it is being compared to payment rails that aren't accurate comparisons.

Murad: Precisely, and a lot of people have pointed out very, very well. [Savty Namoos 00:58:46], I believe, was the first one who pointed this out. Bitcoin isn't competing against [inaudible]. It's not competing against PayPal or VISA. Bitcoin is competing against central banks or even more precisely, it's competing against the Bank of International Settlements as a major settlement network for large transactions as well as against central banks for currency issuance. Those are really the two things that, where it has a competitive advantage, and those are the things you need to be comparing and not the small value transactions.

Pomp: Absolutely. Okay, bitcoin is not accepted anywhere.

Murad: So, I believe that people and this is sort of what a lot of people behind bitcoin cash and nano ripple, et cetera. Lytecoin, even, they don't understand. I believe that the monetary progression- and there's a lot of debate about this, but this is sort of my strong belief- is that money has to move. A new pre money, a new synthetic commodity that has properties of becoming money. It needs to got through this evolutionary process and if you go on my Twitter page, it's pinned right on the top. It sort of shows the step by step progression and I believe- and this is historical, what has happened to gold and silver as well- and I believe it's what's going to happen to bitcoin.

Murad: First, it needs to be a collectable. Then, it needs to become a store value. Then, it's going to be a medium of exchange and finally it's going to be unit of account. So, this sort of merchant adoption, to me , that's more for later. Right now, we have to develop bitcoin in the criteria that make it as the best store value. I believe that bitcoin right now is still somewhere between the collectable and the store value phases. But every year it's moving ever closer to the store value stage.

Murad: Early on, a lot of people argued that it was a collectable for cypherpunks, and nerds anarchists, libertarians, et cetera. And right now, as we've discussed, as market cap is getting bigger, as liquidity is getting bigger, as the comparisons to gold are becoming ever more obvious, as the market cap increases a bit more, as custody solutions improve, it will be seen more and more as a store value.

Murad: Now, as it grows, as we've already concluded, volatility decreases. It is my strong belief that prefer their day to day currency, i.e. their medium of exchange to be relatively priced stable in terms of purchasing power. And that's why I believe the goal isn't to spend bitcoin right now, the goal is to make bitcoin as good of a store value. As bitcoin grows, it's disincentive to spend also decrease. Right now, I'm not spending my bitcoin. Frankly, I'm not going to be spending my bitcoin for another 15 years kor more. I'm not going to spend my bitcoin until it's at least 15–20 trillion dollars, in today's terms.

Murad: As bitcoin gets bigger, say its reached 20 trillion, then the amount of gains in percentage terms that you can have from there on until the ultimate future become less. There's no longer going to be the thousand x still possible today. The maximum from then on is going to be like, what, five, six x and at that point the disincentive to spend that are very, very present today are no longer there. So, you know- everybody knows the pizza story, where in 2011, somebody spent 40,000 bitcoins on a couple of pizzas, and today that could've been like, half a billion dollars or something, right. And so, a lot of people now know that they don't want to be the pizza guy, right. And so right now the key is to optimize bitcoin for store value. And as more liquidity pours into the system, we will optimize bitcoin for a medium of exchange after, I believe, the store value functionality has been more or less saturated.

Murad: Of course in monetary academic terms the medium of exchange and the store value functions of money are an execrable length, but right now, I believe, we need to optimize for the latter and then the former will come with it.

Pomp: Today, bitcoin is 21 million, total supply. Right? That is what is written into the code. Detractors would argue that, that can change through two different ways. One is, if the miners all agreed to allow an increase in the total supply. Or, two is, a hard fork, like a bitcoin cash, that would incorporate a different supply schedule, would then have bitcoin not be 21 million fixed supply. How do you respond to either one of those?

Murad: Yeah, so … the latter is easy to respond. It's like saying des the printing of Zimbabwe dollar hurt the U.S. dollar? Not really. In fact, I think over the long term, this kind of currency competition is impossible. If bitcoin is really not government money, that we're saying, this is the only one that you're allowed to use, and that it actually needs to win in the free market. And bitcoin still has to win 20 other contenders before- and as it wins these contenders, the trust in those 21 million becomes evermore and people realize that these 21 million are much more precious than all the other stuff.

Murad: And bitcoin is far, far more unique than any other cryptocurrency in this sense. So, once again, bitcoin cash printing their own 21 million, is like if Zimbabwe or Venezuela prints their currency, it doesn't weaken the U.S. dollar.

Murad: If anything, it makes it stronger because you have wealth into the quality one and over the long term, I actually think these alt coins are good for bitcoin because they're showing that this one is far, far stronger and over longer term periods, the way monetary instruments work is that you want [inaudible] the risk your wealth as much as possible and your incentivized to instead of being to contrarian, eventually you want to bet on what's the most converging asset.

Murad: And people will eventually- the one that's less liquid, is riskier to store your wealth in and eventually, I believe that, not just with other financial assets, before it has to fight with gold and Fiat, it will first have to predominantly defeat other cryptocurrencies.

Murad: And to answer your first question. Miners aren't in control of bitcoin.

Pomp: Okay

Murad: Full nodes, i.e. users, are in control of bitcoin and the user activated softfork is something that has essentially proved that. More than 93% of miners wanted to increase the blocksides in sort of their way. More than 85% of the company's exchanges wallet providers were on their side as well. Essentially all of the- even many of the wealthiest bit coiners were on their side. However, so, the users, and those people running full nodes, they decide what kind of code to run and as well as what kind transactions to approve. Miners cannot make these changes to the code without consensus and at the end of the day, bitcoin is this impenetrable fortress of full nodes, which really collectively as we've previously discussed in a p-to-p network fashion control the network and I strongly recommend StopAndDecrypt's article ...

Murad: ... The network and I strongly recommend stopping decrypts article titled Bitcoin is an impenetrable fortress of, for more nuanced on this topic.

Pomp: Awesome. All right. Let's switch to the creation of bitcoin. Right. One of the things that bitcoin is able to point to that most other cryptocurrencies and, and even Fiat currencies cannot, is that the creator of the system is unknown, right? So anonymous, anonymous, et cetera, we don't know if it was a man, a woman, a group, and there is folklore and myth around who this may be. Who do you think it is? Should we spend our time trying to figure out who it is? Is it important? And if we do figure out he, she, they is Satoshi, is that good or bad for bitcoin?

Murad: I have certain suspicions, but I'm not going to say any names out loud precisely because nobody knowing who that is for sure is what makes bitcoin so strong. As a bitcoin evangelist, I am incentivized in this pseudonyms myth and

pseudonyms strengths to come to continue going. Frankly, I don't think that the search for who the bitcoin creator is, is it productive activity and the fact that it is still unknown and it is still nearly a thing of theories is once again, one of the dozen things that makes bitcoin far stronger than 99% of other cryptocurrencies.

Pomp: Absolutely. Because you won't say names, I think that's completely fair. Will you at least tip your hand and whether you think it is an individual or a group?

Murad: I think it is one person.

Pomp: One person. All right. Well, at some point somebody is going to get that out of you.

Murad: Sure, but I mean there are sort of six or seven theories on this topic. Frankly it really doesn't matter. Even if we found out who it is, it doesn't matter. It wouldn't even damage bitcoin at that point. I mean it's good right now that we don't have any quote unquote heads of the dragon to cut and that note, there's no single party in control of it as well as the myth is a nice sort of cherry on the cake. But-

Pomp: The story is almost just as important as the technology.

Murad: For sure because I mean, you can have an emergence of this neo money phenomenon without just like religious, like wave the accompanying it, right, but it doesn't matter. The work that has been done on bitcoin since 2010 is so immense, and now there are so many contributing individuals, contributing coders, contributing companies that it wouldn't even matter. Bitcoin is far bigger than Satoshi right now.

Pomp: Absolutely. All right, we're going to read quick message from the sponsors and then that will be right back. All right, so what I want to talk about now, I had Travis calling on, right? Travis previously was at Steve Cohen shop. Right now he's got a crypto fund. One of the things that we talked about was this idea of musical chairs in the institutional world. There's a fixed supply of bitcoin 21 million and right now the music is playing and everyone is walking or jogging around the chairs and at some point the music will stop and people will have to grab a chair, they'll begin to sit down. One of the ideas that Travis presented was this idea that some institutions aren't going to wait for the music to stop.

Pomp: They're going to just start sitting down. He recently tweeted and said, "You know look, I talked about musical chairs, Yale came out and it's now public that they've invested in two separate crypto funds." Travis made the point that Yale just sat down. Yale just grabbed their seat. The music hasn't stopped, but Yale sat down and said, "We're going to make sure we have a seat at the table." How do you think institutions, central banks, world leaders et cetera, should be thinking about bitcoin,

thinking about how to diversify assets into bitcoin and possibly even fearing bitcoin? What do you think that kind of rational thought process should be?

Murad: David Swensen, who is the head of the Yale and diamond company, has been the trend setter in the endowment space as well as the large asset sort of allocation space for the last 20 years.

Pomp: Legend, absolute legend.

Murad: Right. Now that he has invested in 254 I believe, I strongly believe that we will see other ivy league syndicates, other ivy league endowment companies as well as big asset managers and even hedge funds in general start dabbling in the space.

Pomp: It's important to call out. They invested in funds that aren't just bitcoin, but it's not like they just went and bought bitcoin and put it in custody account.

Murad: Yes.

Pomp: They invested in funds that from my understanding, a majority will go into liquid kind of late stage opportunities like Bitcoin, Ethereum, et cetera, but some portion of it will still go into ICOs, venture capital equity investments, et cetera. It's kind of a broader basket than just bitcoin but bitcoin, Ethereum, these liquid Cryptos or a big percentage of the allocation. Obviously if they had just bought bitcoin and bitcoin alone and just put it in their own custody account, that would be an even bigger deal but this is still pRetty big deal. How do people respond other than just backing funds? If you're a central bank right now, what do you do?

Murad: The two best things to do is to either invest in bitcoin directly or to invest in a GP of one of the top five best funds. The latter, given the superiority of the fund over others, might be the single best decision. Then the third best is to invest in the LP of the best funds of course. Those three are the best opportunities. I don't quite agree with the portfolio construction without naming any names of the … I don't quite personally agree with the portfolio construction of the two funds that are relevant to the story here. I believe that a mildly leveraged play on bitcoin will have a better sharp ratio then dabbling and altcoins.

Murad: I think it is … I mean I will personally be having 10 to 15% of my portfolio in two or three premium altcoins as well. But really my heart predominantly belongs to bitcoin and I believe that at this point in time from a technological perspective, it is fiduciary irresponsible not to have at least 60% of your cryptocurrency portfolio in bitcoin. My own fund will be engaged in a more active management, but the sort of the longterm portion of our portfolio will be prominently bitcoin or long leverage place on it. Here's the thing, a lot of people perhaps rightfully believe that the sort of altcoin a game, so to speak, in this blockchain project game will still go on for two or three more cycles and that might be true. Given that, that is true, the two funds that

we're discussing, they have tremendous pedigree and tremendous sort of networks that they can tap into-

Pomp: They have the names and they've got their track records.

Murad: They also can't really justify putting three quarters of their portfolio into bitcoin because then essentially many, if not most of their LPs will be able to just do the same themselves. They need to take advantage of sort of the opportunities that they have, the tremendous deep discounts on future altcoins and the future ICO projects that they will receive undoubtedly. Perhaps even they might, some of these things might outperform bitcoin in the near term and thus if they sort of changed their direction at a precise enough time, they might even make more bitcoin for the investors that way. I actually think that something like this is a strategy.

Murad: A lot of sort of similar people that I've talked to, they believe that when all is said and done, there will be six or seven currencies. I think that's nonsense because if you study monetary history and given sort of the globalized increasingly fluid increasingly interconnected at interoperable nature of these technologies and the world at large, I believe, I used to think it was winner take most as well. I used to think it would be like 70/264 a like in a Pareto distribution type way, but I increasingly believe that it will rather be winner take all rather than winner take most, and I would also say too many of these investors that you have to, you absolutely have to think of these crypto assets as money first and software second.

Murad: A lot of people who come from the entrepreneurial VC or the technology world day, they think about it the other way around and I think that is going to lead to a lot of losses. It's going to lead to a lot of losses and a lot of events, sort of the premium big hedge funds will not perform as well as those who managed to position themselves in accordance to more correct monetary theories.

Pomp: Yeah. Look, I'll even take it a step further. In most cases you have more extreme views than I do, but in this case I may have more than you. In that, if you're an institution today and you have zero exposure to the crypto currency asset class or market, you're violating your fiduciary duty given that it was the best performing asset over the last decade. It has very unique characteristics when it comes to lower levels of correlation, upside the per unit of risk that you take by allocating capital here. Those institutions that are on zero percent exposure have to do what we call get off zero.

Pomp: Each portfolio is different, so some it's 10 basis points, 50, 75, 200, 500, whatever the basis point number is, it's all about what their goals are, what their current allocations are, all of that, but zero is the wrong number. That's much easier, I think for longterm macro investors who have experience and even expertise in the alternative space, so Dave Swensen is a perfect example at Yale, but I think that this

iS actually true at the central bank level, at the individual level, et cetera. Let's go into a hypothetical world where the US central bank is playing that game of musical chairs and they sit down and it comes out that the US central bank bought five, 10% of the network on the open market. What happens to bitcoin, the price and kind of the macro economic world, if that was to come to light?

Murad: Oh, well then buying five percent would be impossible.

Pomp: Why?

Murad: Because people need to realize that I'm more than 10 million of bitcoin, I believe somewhere between 10 to 30 million are held and not like actively trading are actively circulating. Only three or four million are being actively traded. As bitcoin's price will be increasing, I believe that people will be realizing that there's really a financial revolution going here and this is something to be kept for a long time. Relative to the amounts of capital that are sloshing around in capital markets around the world, bitcoin is really so small still. It's really liquid really. As they even tried to buy half a percent, like that very act will raise the price so much in a vertical fashion that just buying the next half a percent will be eight times more expensive and like this continuous compounding in an exponential fashion.

Murad: It will need to be done in an extremely stealthy, in an extremely clever, in an extremely patient manner over months, over years maybe even and maybe even then they'll only be able to get to two and a half percent ballpark. Here's what I like to say. Government's buying bitcoin, really, I think they will be buying bitcoin last. There's two things I want to say here. First of all, governments buying bitcoin will essentially be a putting the final nail in the coffin of reducing their own size by half, because bitcoin is unprintable, which you have discussed how it was going to destroy fiat currencies and bitcoin is increasingly on taxable. I mean the privacy technologies around these technologies, as you know, we'll also keep improving rapidly. This is inevitable.

Murad: I believe that, government's buying bitcoin will probably be the latest group of people to buy them and that will be the final ultimate credibility because essentially the biggest competitor is capitulating. Something like that will not just be a rumor or something like that, given bitcoins the liquidity will be extremely difficult to hide. I like to joke that once a and some asian central bank over, or a sovereign wealth fund announces that they put in two percent of their assets into the portfolio of blue chip cryptocurrencies, it's game over. I don't think that central banks will, are really the people by the time they will try to be accumulating any of them, bitcoin will already be huge.

Murad: I actually believe, and this is one of the things that my views differ from many people in the space actually. I actually think that bitcoins are a cent will be driven

predominantly by the wealthy. The three people, the three sort of the three initials of investors that will sort of make bitcoin's price skyrocket over the coming decades, will be open minded, ultra high net worth individuals. It will be a savvy funds and fund managers and it will be, I think politicians and dictators and sort of these fringe, third world, second world individuals who will need this currency perhaps more than anyone else.

Murad: I liKe to joke that, essentially the people and the institutions who bitcoin was designed to destroy will be precisely the people who will drive a bitcoin's price and bitcoin's success to the sky. Because if you think about it, the people who censor the most, need uncensorable currency the most. The people who sees the most, need unseasonable assets the most and of course the people who print the most neat unprintable currency the most. These people, every week you read about some fringe countries, wealthy individuals and government officials, bank accounts in Switzerland, in Luxembourg, in the Caribbean, being frozen in America, being blocked, transactions being censored.

Murad: This technology allows those very precise people to have unseasonable store value where they can essentially accumulate wealth with absolutely no one else in the world being able to take it away from them. For better or worse, this is how free market … instruments on free market technologies work. It will be of course, used for the good and the bad, but irregardless of these very people whose bitcoins, it's fighting against ideologically will be the same people who will helping it financially.

Pomp: Absolutely. I attend to think that you are more right than wrong on that. Before we kind of go into some rapid fire questions, if an institutional CIO, a central bank authority, a government leader, is listening to this, give me your 60 second pitch to them why they should buy bitcoin.

Murad: Bitcoin is the soundest hardest currency that has ever been invented in the history of human civilization. This is disinflation is second to none. It's monetary policies known years in advance and it is becoming increasingly credible. It will also be increasingly a threat to the very currencies that you guys control. I think getting in before most other central banks and most other sovereign wealth funds and most other rich people will, in the next decade will prove to be one of the smartest investment decisions in the course of human history. If you are able … the countries that are able to stealthily accumulate bitcoin and adopt bitcoin more than other currencies, will thrive in the age of hyper organization while the other countries that haven't done so will suffer tremendously.

Pomp: Long bitcoin, short the bankers and I think we are in agreement there. All right, so you've answered some of these already, but what do you think is your most controversial thought? Is it the opportunity that exists for bitcoin stuff?

Murad: I Mean, the opportunity for bitcoin is better than ever. I would say the risk reward ... so the award is technically low in and of itself is lower than it was in like 2013 or whatever, but the risks are also massively reduced. We already have 200 accompany building for this thing, building on the side of this thing, building on top of this thing. The number of engineers involved are ever greater. If you watch this slides and the lectures from a scaling bitcoin Tokyo that's happening over the past couple of days, the amount of just genius interventions that are being potentially added to bitcoin and the improvements added to bitcoin are incredible.

Murad: The liquidity today and the volumes today and the marketability of the brand today is far greater than back then. Risk reward might even be higher I would say. The opportunity is still there. It's at least a couple of hundred x and in the very, very long run more than a thousand x. There's still a lot of wealth to be created here, doing a mildly leveraged play via various instruments or derivatives is a way to boost returns even further. I believe that the opportunities are, is definitely here and other controversial opinion is what I've described is that bitcoin isn't necessarily sort of going to be adopted bottom up, but rather, and it's not necessarily going to be adopted pop down either, but it will really be the wealthy who will be adopting it. Unfortunately due to the nature of the world, those are the people with the money and it's the people with capital who are going to be sort of boosting the market capitalizations of these assets.

Pomp: Absolutely. What's the most important company in crypto right now?

Murad: Chaincode Labs.

Pomp: Why?

Murad: They have some of the most prolific developers and block stream as well. Of course.

Pomp: Got it. Those working on bitcoin?

Murad: Yes. John Newbery, Alex Marcos, Matt Corallo, they're just on a whole nother level of genIus.

Pomp: Absolutely. All right. If you had a magic wand and you could wave it, what's the one regulation that you would improve or change?

Murad: I would reduce taxes and I would prioritize a lot more things around the world.

Pomp: Interesting.

Murad: I believe that a free market capitalism and individual entrepreneurs are much more efficient at providing solutions and a much more efficient at making

world Austrian economists call economic calculations. In very, very crude terms, a thousand clever, smart, talented entrepreneurs with a million dollars each, we'll do a lot more both for themselves and the world. Then I'm just an emotion's burka with no connection to that particular money will do with a billion dollars. I believe that a lot of the things that governments do around the world today, if you privatized or even partially privatized, those things that the world will be much more efficient because I'm essentially seven fiercely competitive companies will always achieve the results much better than one sort of bureaucratic, fat government institutions.

Pomp: I don't think anyone is surprised that you believe that and I tend to, I tend to agree-

Murad: of course,

Pomp: The most fastest there. Okay, so let's talk about something for two minutes, that's non crypto related. So aliens, we just got to admit that they exist. Most people think of aliens as a human equivalent. They're depicted that way and movies and saifai, et cetera, but nobody ever really talks about alien animals. Do we think that there are multiple species of aliens? And if so, do we think aliens have pets?

Murad: Well, if you make the assumption aliens exist, then it is likely that many different kinds of aliens exist. Just due to the vastness of space, statistically speaking, this vastness is so immense that if we do go off of the assumption that at least one other specie exists, it is likely that hundreds of others do as well. It is also likely that several species exist on sort of one planet or ecosystem flora, fauna, whatever together and I wouldn't be surprised if those civilizations have animals as well. Yeah.

Pomp: Yeah. You think they have pets though? You think they take the animals and they make them their pets in like a domesticated?-

Murad: It is hard to say some of the alien species would have pets. I think probabilistically speaking that's very likely. It really depends sort of on the culture and the order of that particular world.

Pomp: Yeah. I think that's fair. All right. I end each one of these with allowing the guests asked me one question. What one question do you have for me?

Murad: I guess you've asked this question to me, but I would like to sort of hear your version as well. I know we've already previously talked about this, but I just sort of like to rehash these bullet points in my head as well. You personally and sort of on with your work with Morgan creek and other ventures, how do you go about pitching bitcoin and sort of this ecosystem at large to not individually that says, but the more conservative large asset allocators?

Pomp: Yeah. Look, I think that it's custom given who we're talking to. There's kind of different things that we emphasize or deemphasized depending who we're talking to. A lot of it is informed by who they are, what their current allocation is, what their goals are, et cetera, but there are some common threads through each conversation. One of them is this asset class has some of the highest yield opportunities per unit of risk across the entire world. Any asset, any asset class, any strategy, this is one of if not the highest potential yield per unit of risk. That's one. Two is that the idea of scarcity around bitcoin specifically, is something that they have likely not thought deeply about, nor do they actually understand the gravity of the implications.

Pomp: It's one thing to just understand, okay, if there's a fixed supply, an increase in demand price should appreciate. It's another thing to understand 21 million bitcoin exist and there are hundreds of trillions of dollars of wealth in the world that are going to be competing for those 21 million. Hundreds of trillions of dollars exist. If you manage 500 million, a billion, 10 billion, a hundred billion, you're nobody. If you don't have your seat at the table now, you may not get a seat later.

Pomp: I think that's the second one. Then the third one is, we actually make economic argument looking at other asset classes. The opportunity cost, if you do not invest in cryptocurrencies, bitcoin, block chain, et cetera, what else is out there? What you find, depending on who you listen to, my partner Mark Hughes is very well versed in kind of the endowment model and it comes out of that world and he walks people through this idea that they yield that they target or goal on may not be available in other asset classes. If you look at stocks, bonds, currencies and commodities, and only four assets you can own.

Pomp: The ability to drive six and a half, seven, seven and a half, eight percent annualized yield, may not be there over the next decade. If that is true, that doesn't necessarily mean you should take a hundred percent of your assets and go put it into bitcoin for example, but you should have exposure. Those three core components make up this kind of verbal campaign that we're on, called Get off zero. It's the idea that, if you sitting in a fiduciary seat and you have a zero exposure to the asset or the asset class, you're wrong. There's a qualitative argument, there's a quantitative argument, we're happy to discuss either one of them, but your wrong. Zero is the wrong number and you have to get off zero.

Pomp: Whether it's 10 basis points, 50, 100, 500, that's a customized conversation for who it is, what their goals are, what the current allocation, et cetera, but zero is the wrong answer. What we find is that specific argument of you have no skin in this game and this could be the most important game available really residents. I think that Yale jumping in very big deal. We've got some institutions that I think when people find out are going to be shocked and again, more people grabbing seats.

Pomp: I think what we're going to see over the next, I put it at like 36 months, is a formal or just an inflow of capital from very, very sophisticated people that most of the financial world is not expecting. There's a, I think it's Bill Gates says, "We overestimate what we can accomplish in two years and we underestimate what we accomplish in 10 years." I'm probably with you in that even the most hardcore bitcoin believers are actually drastically underestimating what we're talking about here and what the potential is. If that is true, this is the most important piece of technology that the world seen.

Murad: Without a doubt and those are amazing points. To add to the discussion on yield, I would say one of my old bosses told me that making money for you guys will in general as an aggregate, as a demographic will be much harder than it was for our generation or the generation before that. As you might know in the 50s or 60s, you could have just a regular job and still be able to buy one house or even two houses, have a big family, et cetera. Today that's impossible. The world not just America, but the world as a whole is becoming fiercely competitive. We are sort of, obviously not at the end of the esker, but we are sort of, it's kind of sloping down. Innovations are harder to create, the technologies are more sophisticated to sort of incrementally push further and the amount of, I guess, ideas that are easy pickings are scarcer nowadays. I generally like obviously becoming wealthy takes a decade at least or more for anybody but I like to say semi jokingly that crypto might be the last easy way to rich in my generation.

Pomp: Look we obviously today have the richest man in the world over a hundred billion dollars of wealth, Ryan Jeff Bezos. It would not surprise me that the richest company in the world which is over a trillion today, is matched by the richest person in the world in the future to we'll have a trillionaire and the odds of that person comes from the cryptocurrency world, in my opinion, is the highest probability out of any other industry. If that is true, the amount of millionaires centi millionaires, billionaires centi billionaires that will be created in this asset class will be unparalleled and anything else in history. I think that's part of the excitement.

Murad: For sure in monetary terms within that particular asset, a bitcoin will actually increase inequality because the way it is, the distribution is improving with every cycle of course but if hyper bitcoin quantization of work to actually occur, the gini coefficient of bitcoin would probably be higher than any fee at currency today among the predominant ones. We would definitely see a couple of trillionaires and today terms, I think without a doubt.

Pomp: Absolutely. All right man. This is epic. I really, really appreciate the time. I hope that this is valuable to everybody and want to do this pretty regularly to check back in and see kind of how all this is progressing, so thank you.

Murad: For sure. Thanks for having me.

Pomp: Absolutely.

Disclaimer:

THANK YOU, CREATORS.

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 members of the any specific business, that means any business I am associated with. Bitcoin, shitcoins, and related technologies can be volatile, Don't fuck around with this stuff because you might get burned.

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.

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 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.

DYOR | BTFD | HOLD