WORDS

September 2019

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

Contents

Goals and Scope

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

History

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

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

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

Support WORDS

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

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

Spread the word

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

Follow us on social media

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

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

Twitter

Subscribe to our newsletter

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

Subscribe

Our pledge

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

Bitcoin's natural long-term power-law corridor of growth

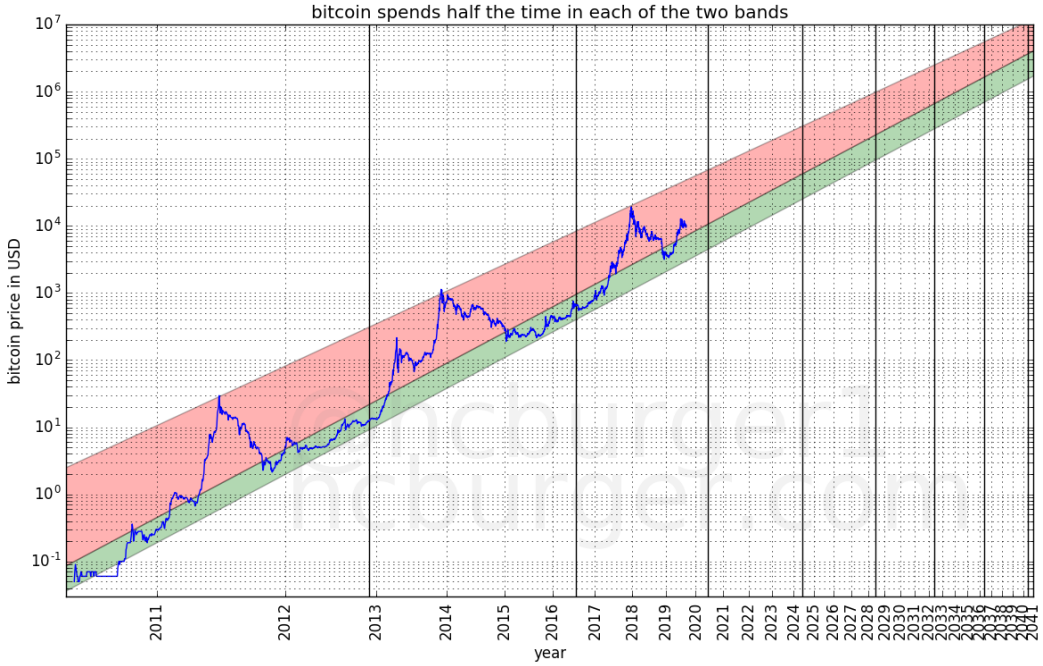
By Harold Christopher Burger

Posted September 4, 2019

Disclaimer: This article is not financial advice.

With growing adoption of the cryptocurrency, its future price has been the subject of more and more speculation. Predictions are all over the board, with some economists like Nouriel Roubini predicting a price of 0 within five years, whereas John McAfee has famously predicted a price of $1 million per bitcoin by the end of 2020. Others have made predictions that fall within this very wide range [1].

Overall, bitcoin's price has risen very quickly since it's initial inception in 2009 and has also been subject to booms and busts. The rapid rises and boom phases seem to encourage people like McAfee to make very optimistic predictions about the future price, whereas the busts seem to encourage some economists to predict a decline toward 0. In this article we look at the full price history of bitcoin and see that bitcoin's price evolution can be understood as moving within a corridor which is defined by two power-laws based on time. While the idea of modelling bitcoin's price using a power-law is not new, in this article we give more support to this idea and provide some additional interpretations.



This model allows us to make broad predictions concerning the long-term future price of bitcoin, e.g.

- the price will reach $100 000 per bitcoin no earlier than 2021 and no later than 2028. After 2028, the price will never drop below $100 000.
- the price will reach $1 000 000 per bitcoin no earlier than 2028 and no later than 2037. After 2037, the price will never drop below $1 000 000.

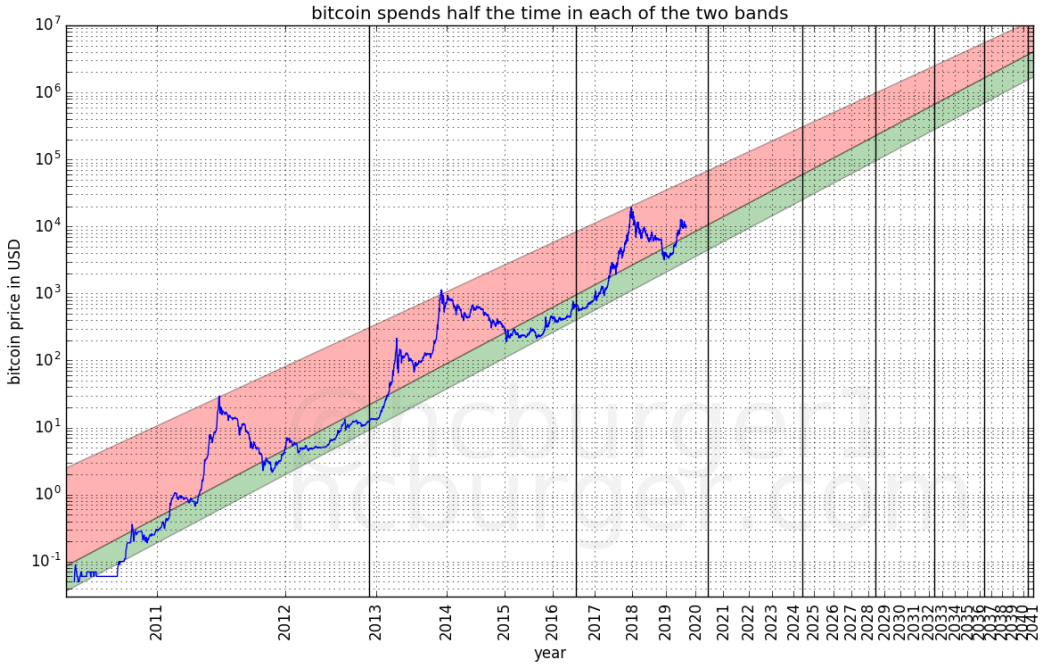
Furthermore, we will see that the price corridor can be divided into two bands, one which lies at the lower-end of the price predictions and is rather thin, the other one being much larger and lying at the higher-end predictions. Bitcoin's price spends about equal amounts of time in both bands. This implies that large bubbles and busts are likely to continue to exist. The above predictions might seem very broad, but they are sufficiently precise to disagree with the predictions of some other people. This price model should also help determine good points to enter or leave the market.

I am quite confident that in the long-term, the price will indeed evolve approximately as stated in this article. In fact, I think it is more likely for these predictions to be too low rather than too high: I believe that bitcoin has more potential upside than downside to large exogenous shocks. But this article will not try to make any predictions regarding large exogenous shocks. Instead, we will assume that things continue "as usual".

Different ways of looking at the price

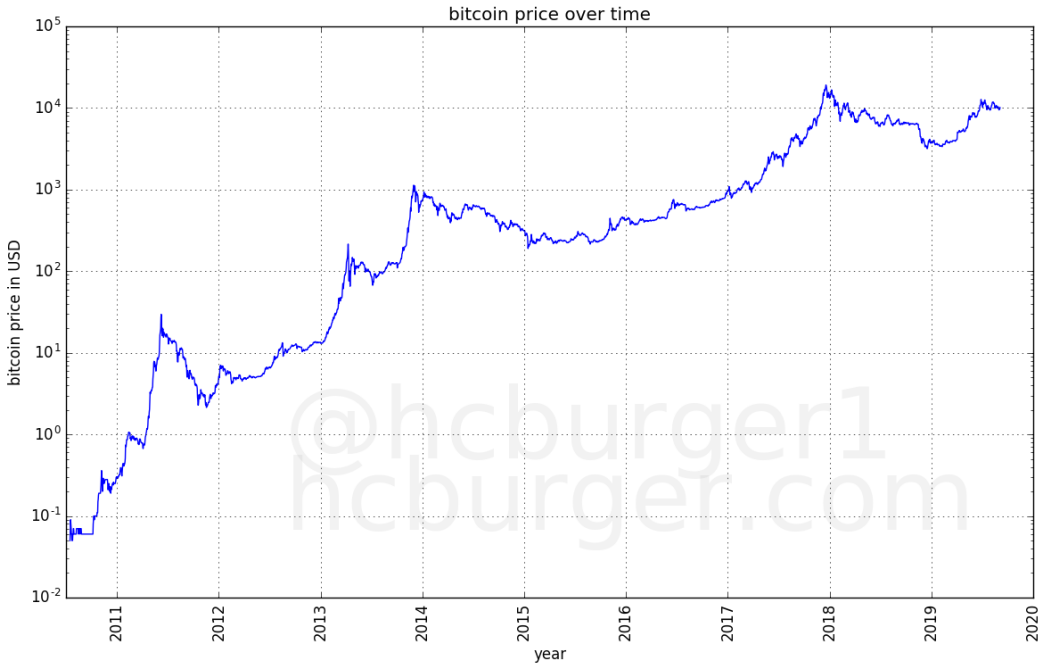
The most interesting and amazing aspect of the price of bitcoin is that it went through many orders of magnitude within a few years. The first instance of a publicly listed price I could find was $0.05 per bitcoin on the Mt Gox exchange, on 17th of July 2010, but prior to that date, many bitcoins have changed hands for a much lower price, such May 22, 2010, when Laszlo Hanyecz paid 10 000 btc for two pizzas, which roughly corresponds to a price of only $0.0025 (0.25 cents) per bitcoin. At the time of writing, the price of one bitcoin hovers around $10 000, which is about 4 million times more than the price at which Laszlo Hanyecz valued them at the time.

Going through so many orders of magnitude is unusual for a financial instrument, and indeed looking at at plot of the price of bitcoin over time might be somewhat confusing (if the price is represented in linear scale). The below is a chart of the price of bitcoin going from the 17th of July 2010 to approximately the time of writing. Similar plots can be found at any website which lists the price of bitcoin.



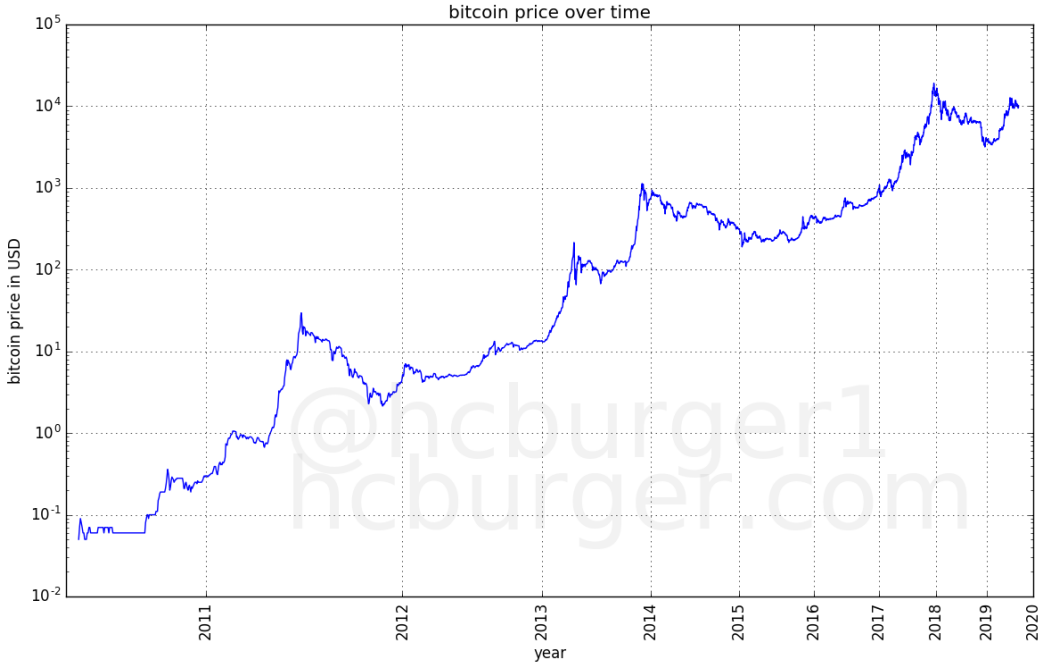
Any price swings close to the present are so large in magnitude compared to the price in the past, that past prices seem meaningless. However, to make sense of a long-term price trend, all past prices should have some importance. The reason for the above effect is that using a linear scale is inconvenient for anything that goes through so many orders of magnitude. Using a logarithmic rather than linear scale is more useful [2]. The logarithmic

scale gives equal spacing from e.g. 0.01 to 0.1 as from 1000 to 10000. Seen in this way, the bigger picture of the price evolution of bitcoin becomes more visible:



What becomes apparent is that the rate of growth of the price of bitcoin seems to be slowing. The price went from $0.1 to $1 — a factor of 10 — in only a few months. Subsequent gains of a factor 10 came slower.

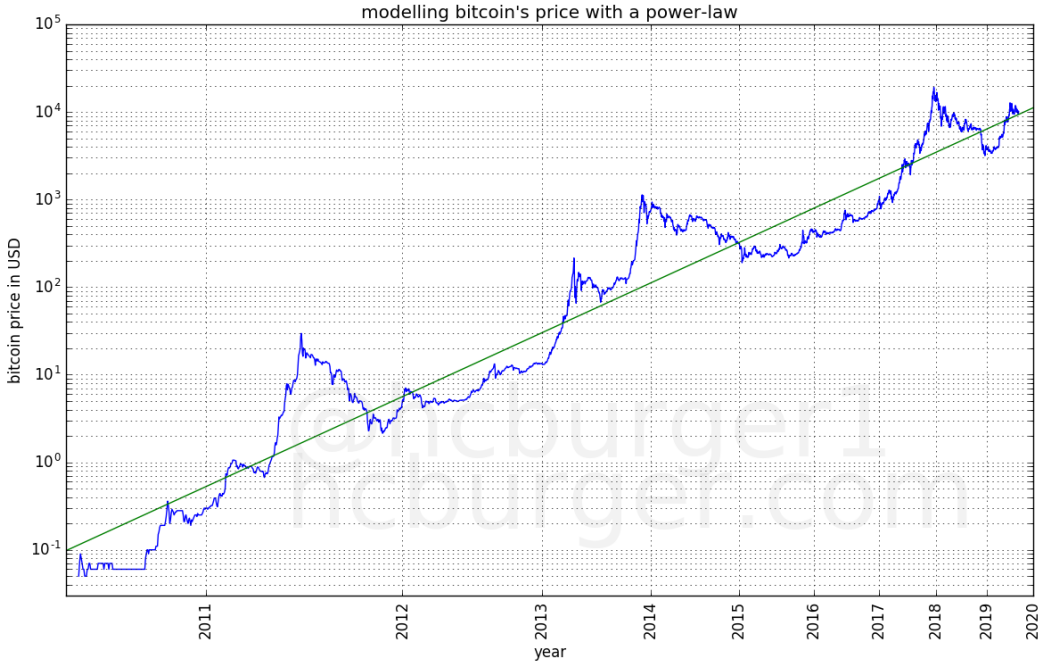
In the above plot, the price (y-axis) has been scaled logarithmically, but not the time (x-axis). Let's see what happens when the x-axis is also scaled logarithmically, in a so-called log-log plot [3]:



Now the price curve looks remarkably linear!

Linear regression

Since this data looks so linear, let's try to use linear regression on it [4]. This idea in itself is not new, e.g. I found a post on reddit which did exactly this [5].



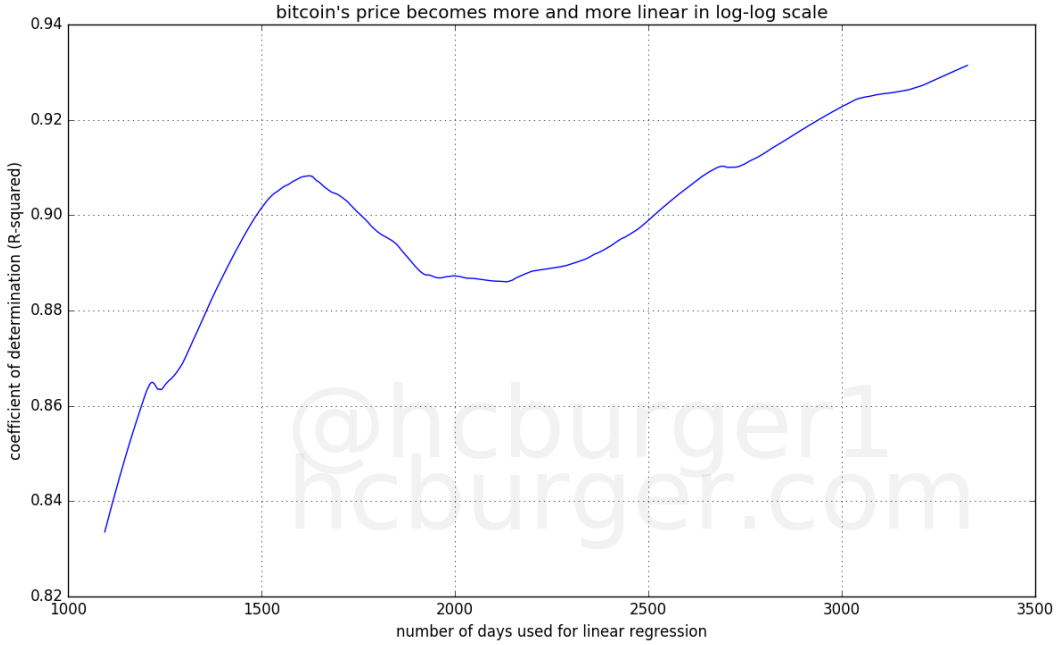
The green line is the result of linear regression. Linear regression gives us the following power-law to predict the price of bitcoin on a given day:

$$price = 10^{a+b\log_{10}(d)}$$

with a = -17.01593313 and the slope b = 5.84509376 with d the number of days since 2009.

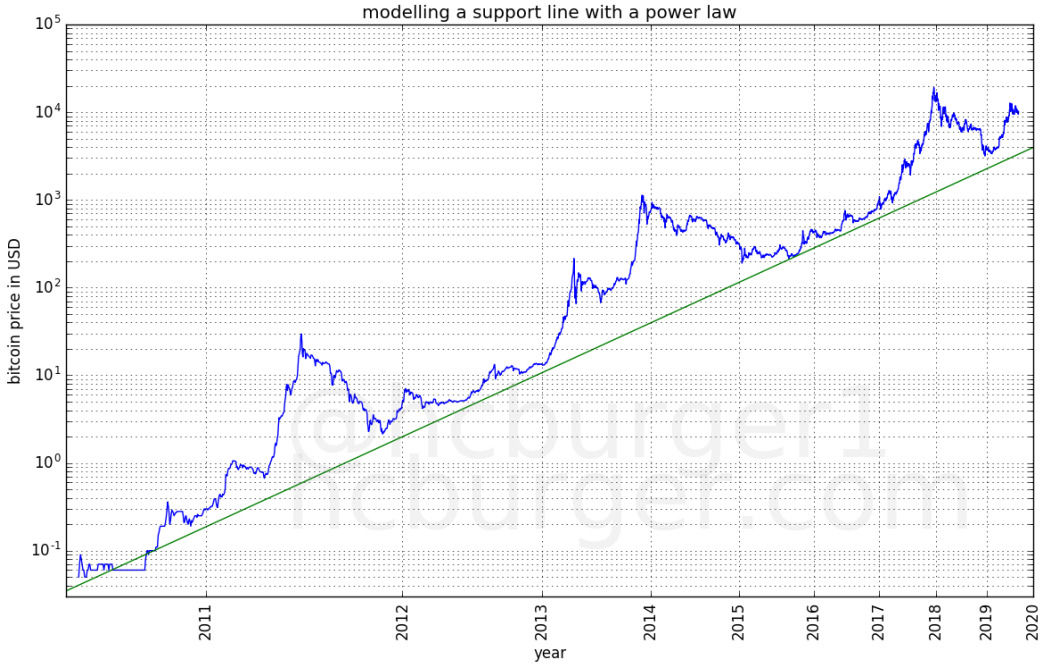
Note: We obtain a power-law, which is non-linear because we did linear regression in log-space.

Visually, this fit works very well. It works well all the way back to the first prices that were listed by exchanges. Interestingly, the post on reddit was written about a year ago, and the results are still remarkably similar. Also, the coefficient of determination is high: 0.93139763, which gives us another indication that we have a good model fit [6]. We can look at how the coefficient of determination evolved over time. Surprisingly, the model tends to fit the data better as time goes by:



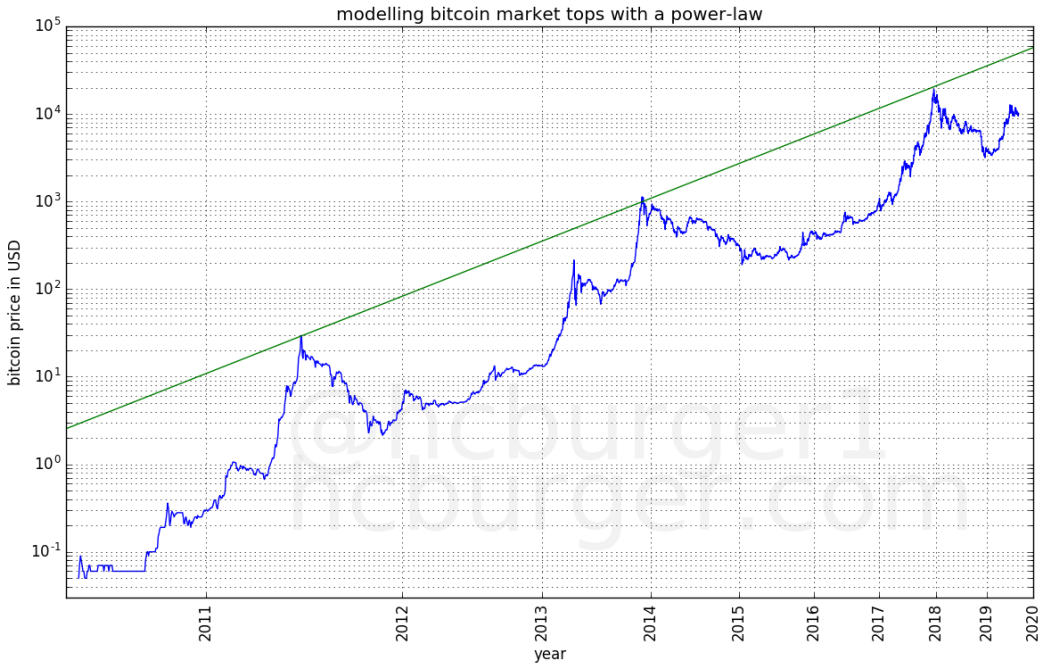
The x-axis represents the number of data points (days) used for the linear regression model, whereas the y-axis represents as a measure of goodness of fit. Bitcoin's price fits the power-law better and better.

Let's play around a bit more. If we move the above fit a bit lower (but do not change the slope), we find a support line which seems to work remarkably well: Except for one instance in 2010, the price has never breached this line:



There seems to be a fundamental level of support for bitcoin's price which has historically followed a power-law.

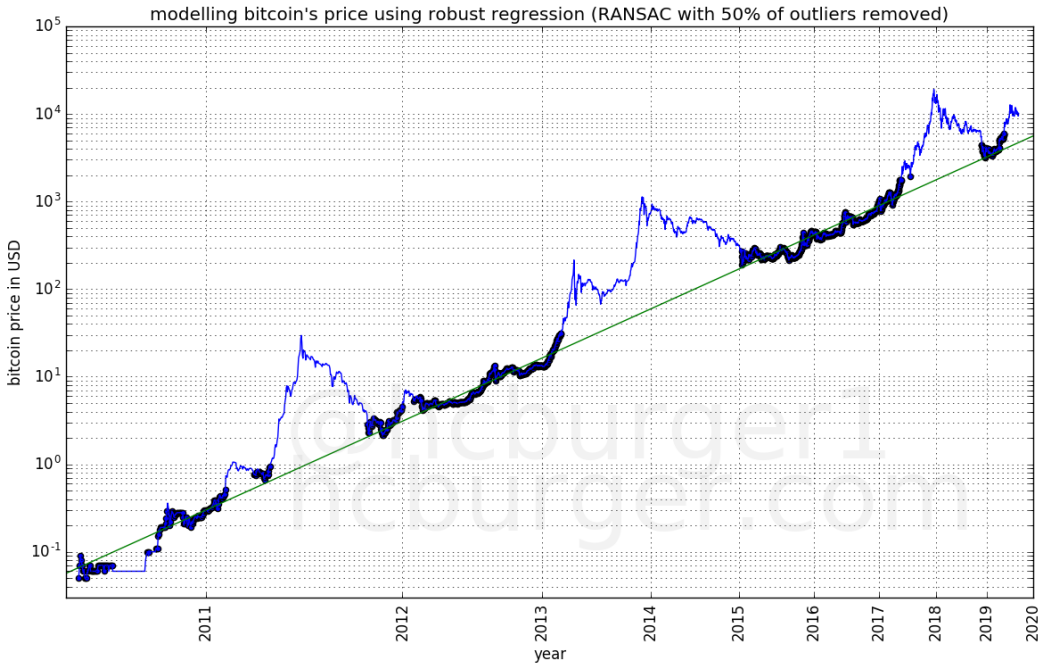
We can also try to perform linear regression on only the three tops achieved in 2011, 2013, and 2017. Interestingly, this fit works very well: All three data-points are remarkably close to the line:



The market tops also seem to follow a power-law. If the next market top also follows this power-law, the market top will lie on this line. The slope of this power-law is 5.02927337, whereas the fit on all data gave us a somewhat larger slope of 5.84509376. This indicates a relative taming of bitcoin bull markets compared to the overall trend-line. This is perhaps expected, as the market matures and order books become deeper, one should expect less volatility.

We now have two power-laws between which the price of bitcoin moves: the lower support line, and the higher line defined by the three market tops.

Now, let's see which data points fit the model best. We are going to use random sample consensus, or RANSAC, which is an iterative form of outlier removal: First, linear regression is performed on all data points. Then, the data point which fits the data least well is removed, and linear regression is performed again [7]. We're going to stop when 50% of the data points have been removed. This plot shows the result:

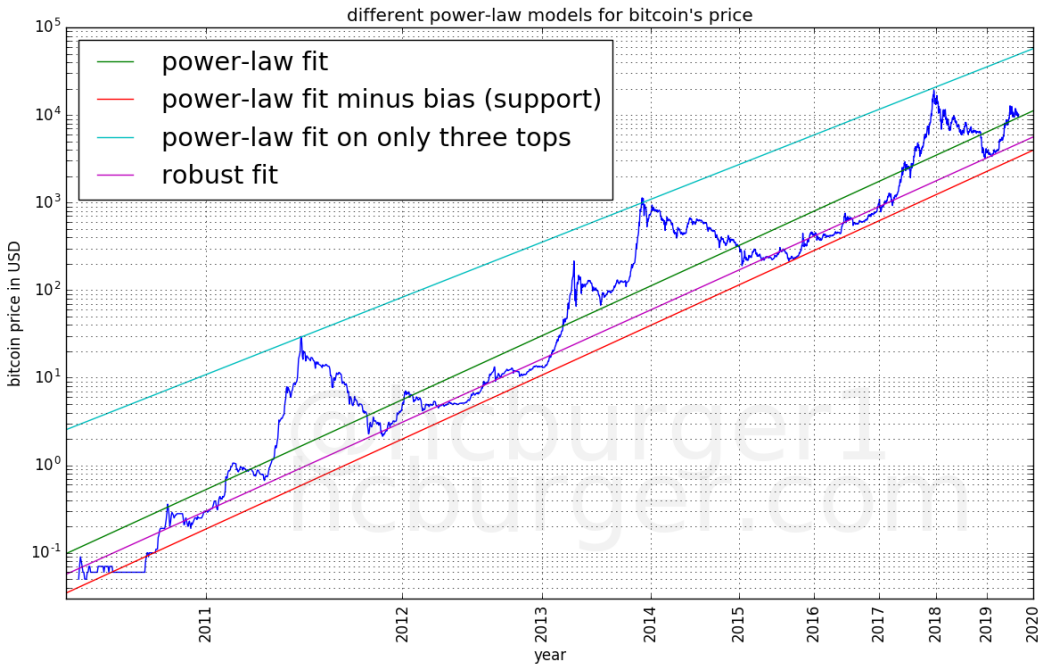


The data points that have been chosen by RANSAC are highlighted in this graph. It seems that there are two groups of data-points: Those that have been chosen by RANSAC are very close to the model fit. In the group of data points not chosen by RANSAC, the values are almost all above the model fit. In fact, some of them are much higher than the model fit. These data-points occurred mostly in bull markets. The price of bitcoin seems to follow two modes:

- the normal mode, during which the price is very well defined by a power law, and
- the bull mode, during which the price can be much higher than in normal mode and during which there is more price volatility.

The price spends equal amounts of time in each of the two modes.

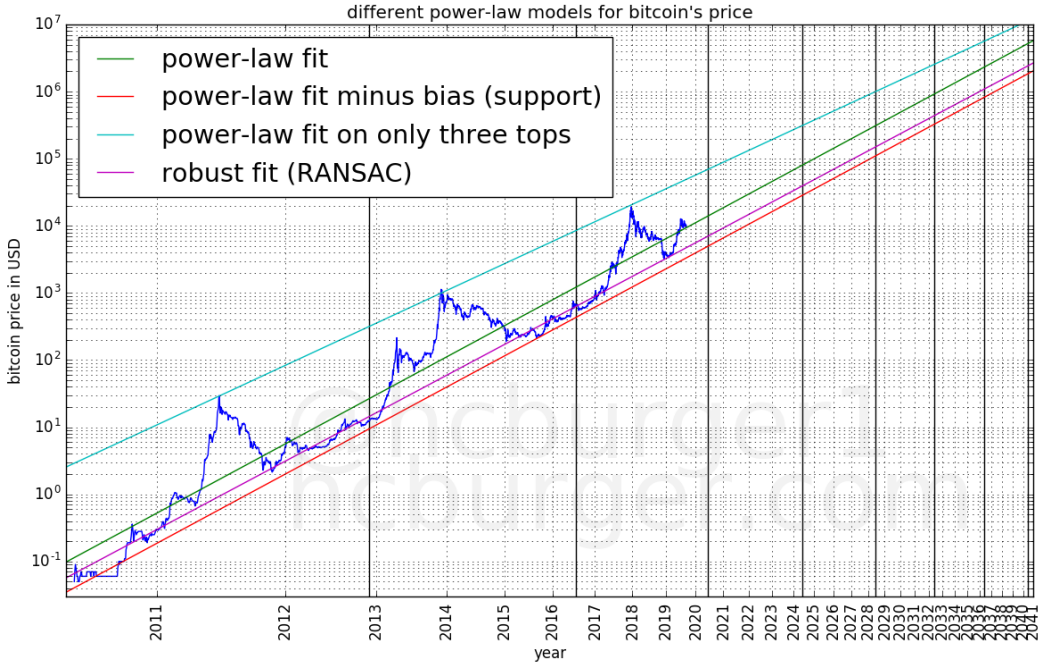
Finally, let's combine all the previously mentioned model fits into one graph:



We see that the fit using all data and the result of RANSAC have very similar slope, but a slightly different offset. This is because the bull market prices have been mostly excluded as outliers by RANSAC.

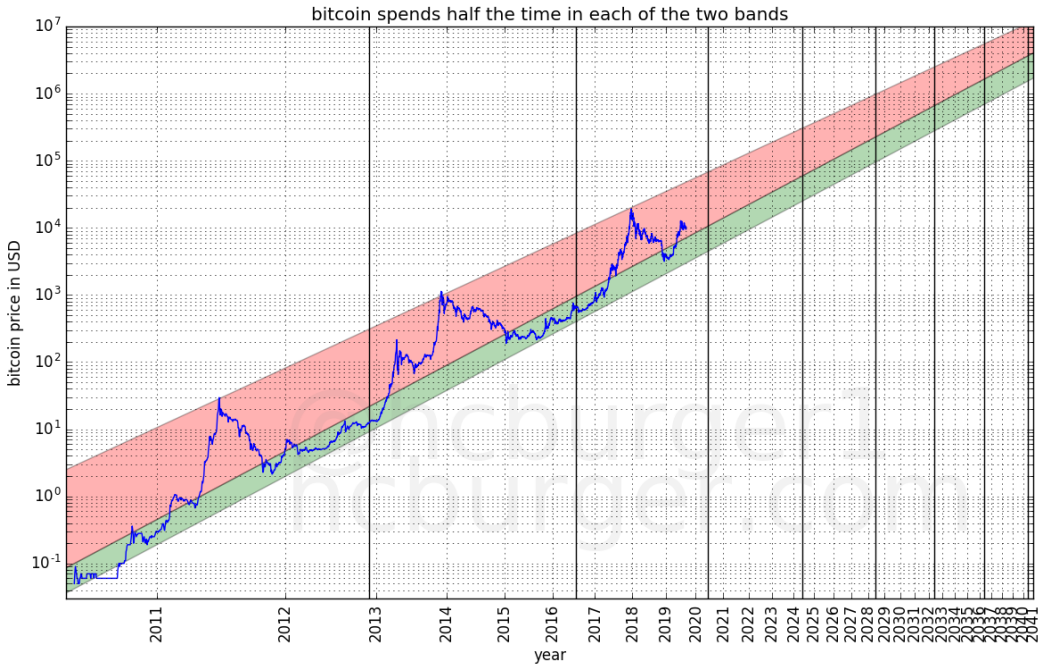
Model predictions

We now have various models to predict the future price of bitcoin. All we have to do is extend the graph:



The model predicts that the price will move between the red support line and the blue top line. The purple robust fit / RANSAC line defines the center of the "normal mode". The two past halvings as well as estimated future halvings have been marked with black vertical lines.

We can further divide this corridor into two bands, one corresponding to the "normal" mode and one corresponding to the "bull" mode. The price has so far spent half the time in the lower "normal mode" band, and the rest of the time in the higher "bull mode" band.



Interpretations

This power-law model predicts a continued, but slowing growth of the price of bitcoin. It also predicts reduced, but still large volatility in the future. It predicts that the price will not reach $100 000 before 2021, but it also predicts that the price will not be lower than $100 000 by 2028. It predicts that the price will not reach $1 000 000 before 2028, but also that the price will not be lower than that after 2037. The model predicts ever increasing prices, although at a slower and slower rate.

These predictions appear to be somewhat middle-of-the-road compared to other predictions. According to this model, McAfee's famous prediction is far too optimistic.

The combination of the fact that the price corridor is rather wide combined with the fact that the rate of growth is slowing means that unlucky investors will have to wait longer and longer before their initial investment is safely recouped. E.g. investors who bought bitcoin at the top of the bubble in 2011 only had to wait about two years until 2013 for the price of bitcoin to recover permanently. However, investors who bought at the peak of the 2013 bubble had to wait about four years, until 2017, before the price recovered from that price and stayed above that price. The model predicts that the price point reached at the peak of the 2017 bubble might not be secured until the end of 2023, about six years later.

Until now, each four-year halving period had a bubble whose price was exceeded by the next period's bubble. Due to the above point of slowing growth and corridor width, this is not guaranteed to continue to be the case in the future. As an example, the model allows the following scenario:

- A price of about $150 000 at the beginning of 2022, which is the next and fourth four-year period.
- A price that is lower than $150 000 until mid-2028, which is in the sixth four-year period.

Such a scenario would give bitcoin detractors ammunition for criticism, but is otherwise not something that should be especially worrisome, as long as one is prepared.

Why does bitcoin follow a power-law, and should we expect it to continue? The observation that bitcoin follows a power-law is admittedly ad-hoc. In addition, there are other factors than just time that should influence bitcoin's price, such as its scarcity. However, bitcoin's scarcity is programmatic and therefore also time-based. In is therefore not implausible for a simple time-based model to continue to hold true in the future. The fact that the power-law fit works better and better in terms of the measure in the log-log plot is an indication that this might indeed hold.

Conclusion

In this article we presented a simple time-based equations to model bitcoin's price. It is remarkable that the equations are both 1. simple and 2. use time as the only variable, yet work remarkably well over a long period of time.

This model does not attempt to predict bull markets, which seem to occur periodically. However, bull markets are expected to fall within the corridor defined by this model.

In an upcoming article, we will use a time-based power-law to attempt to find good points in time to enter and exit the market.

References

1. https://blockonomi.com/bitcoin-price-predictions-2019/
2. https://en.wikipedia.org/wiki/Logarithmic_scale
3. https://en.wikipedia.org/wiki/Log%E2%80%93log_plot
4. https://en.wikipedia.org/wiki/Linear_regression
5. https://www.reddit.com/r/Bitcoin/comments/9cqi0k/bitcoin_power_law_over_10_year_period_all_the_way/
6. https://en.wikipedia.org/wiki/Coefficient_of_determination
7. https://en.wikipedia.org/wiki/Random_sample_consensus

Bitcoin, Not Blockchain

By Parker Lewis

Posted September 6, 2019

Have you ever heard a smart sounding friend say that they aren't sure about bitcoin but they believe in blockchain technology? This is like saying you believe in airplanes but you're not sure about the wings; and there's a good chance that anyone who thinks that may not understand either. In reality, bitcoin and its blockchain are dependent on each other. However, if new to bitcoin, understanding how it works and parsing the landscape can be incredibly difficult. Frankly, it can be overwhelming; given the complexity and sheer volume of projects, who has the time to possibly evaluate everything? There is in fact a manageable path but you have to know where to start. While there are seemingly thousands of cryptocurrencies and blockchain initiatives, there is really only one that matters: bitcoin. Ignore everything else like it didn't exist and first try to develop an understanding of why bitcoin exists and how it works; that is the best foundation to then be able to think about the entirety of everything else.

It is also the most practical entry point; before taking a flyer and risking hard-earned value, take the time to understand bitcoin and then use that knowledge to evaluate the field. There is no promise that you will come to the same conclusions, but more often than not, those who take the time to intuitively understand how and why bitcoin works more easily recognize the flaws inherent in the field. And even if not, starting with bitcoin remains your best hope of making an informed and independent assessment. Ultimately, bitcoin is not about making money and it's not a get-rich-quick scheme; it is fundamentally about storing the value you have already created, and no one should risk that without a requisite knowledge base. Within the world of digital currencies, bitcoin has the longest track record to assess and the greatest amount of resources to educate, which is why bitcoin is the best tool to learn.

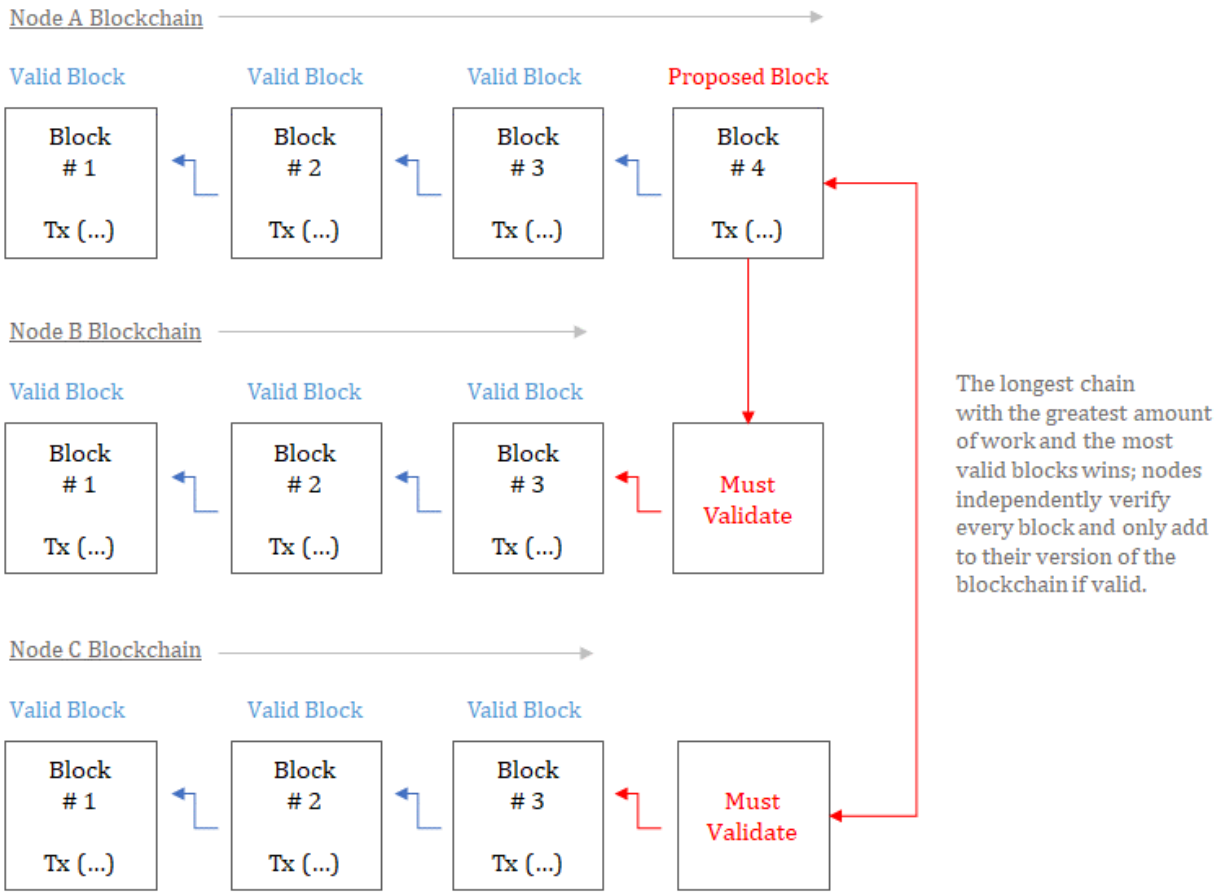
To start on this journey, first realize that bitcoin was created to specifically address a problem that exists with modern money. The founder of bitcoin set out to create a peer-to-peer digital cash system without the need for a trusted third-party, and a blockchain was one critical part of the solution. In practice, bitcoin (the currency) and its blockchain are interdependent. One does not exist without the other; bitcoin needs its blockchain to function and there would not be a functioning blockchain without a native currency (bitcoin) to properly incentivize resources to protect it. That native currency must be viable as a form of money because it is exclusively what pays for security, and it must have credible monetary properties in order to be viable.

Without the money, there is no security and without the security, the value of the currency and the integrity of the chain both break down. It is for this reason that a blockchain is only useful within the application of money, and money does not magically grow on trees. Yep, it is that simple. A blockchain is only good for one thing, removing the need for a trusted third-party which only works in the context of money. A blockchain cannot enforce anything that exists outside the network. While a blockchain would seem to be able to track ownership outside the network, it can only enforce ownership of the currency that is native to its network. Bitcoin tracks ownership and enforces ownership. If a blockchain cannot do both, any records it keeps will be inherently insecure and ultimately subject to change. In this sense, immutability is not an inherent trait of a blockchain but instead, an emergent property. And if a blockchain is not immutable, its currency will never be viable as a form of money because transfer and final settlement will never be reliably possible. Without reliable final settlement, a monetary system is not functional and will not attract liquidity.

Ultimately, monetary systems converge on one medium because their utility is liquidity rather than consumption or production. And liquidity consolidates around **the most secure**, long-term store of value; it would be irrational to store wealth in a less secure, less liquid monetary network if a more secure, more liquid network existed as an attainable option. The aggregate implication is that only one blockchain is viable and ultimately necessary. Every other cryptocurrency is competing for the identical use case as bitcoin, that of money; some realize it while others do not but value continues to consolidate around *bitcoin* because it is the **most secure** blockchain by orders of magnitude and all are competing for the same use case. Understanding these concepts is fundamental to bitcoin and it also provides a basic foundation to then consider and evaluate the noise beyond bitcoin. With basic knowledge of how bitcoin actually works, it becomes clear why there is no blockchain without bitcoin.

There is no blockchain

Often, bitcoin's transaction ledger is thought of as a public blockchain that lives somewhere in the cloud like a digital public square where all transactions are aggregated. However, there is no central source of truth; there are no oracles and there is no central public blockchain to which everyone independently commits transactions. Instead, every participant within the network constructs and maintains its own independent version of the blockchain based on a common set of rules; no one trusts anyone and everyone validates everything. Everyone is able to come to the same version of the truth without having to trust any other party. This is core to how bitcoin solves the problem of removing third-party intermediaries from a digital cash system.



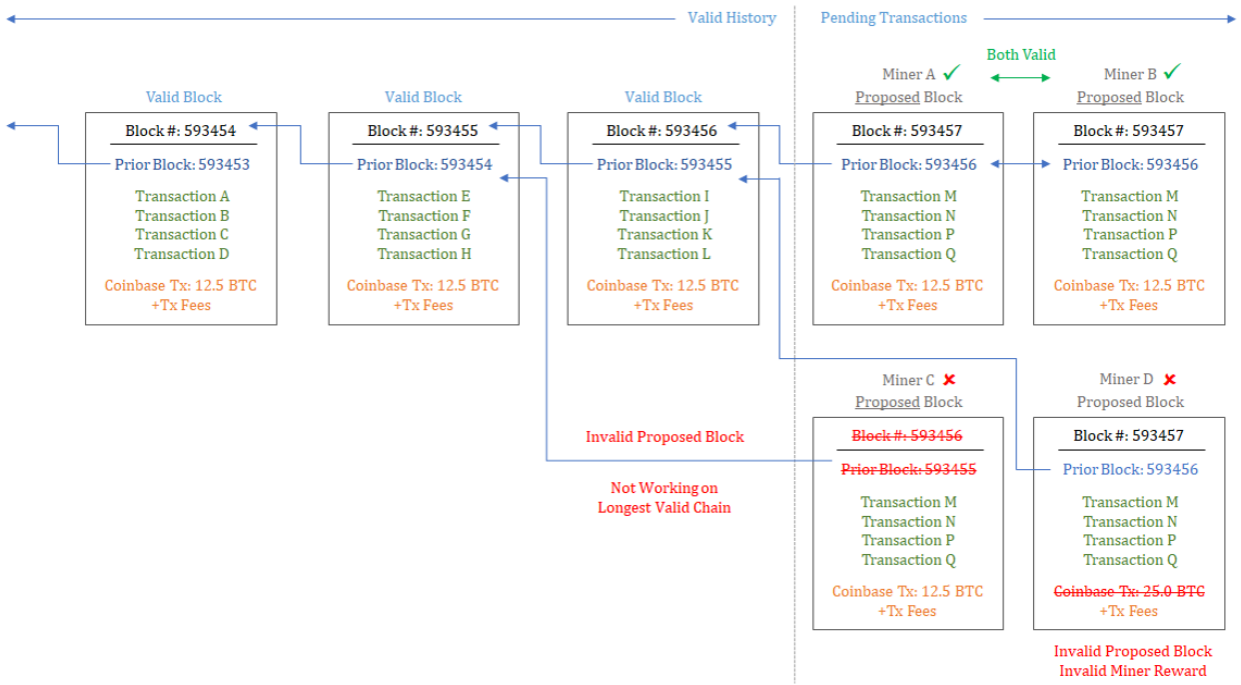
Every participant running a node within the bitcoin network independently verifies every transaction and every block; by doing so, each node aggregates its own independent version of the blockchain. Consensus is reached across the network because each node validates every transaction (and each block) based on a core set of rules (and the longest chain wins). If a node broadcasts a transaction or block that does not follow consensus rules, other nodes will reject it as invalid. It is through this function that bitcoin is able to dispose

with the need for a central third-party; the network converges on the same consistent state of the chain without anyone trusting any other party. However, the currency plays an integral role in coordinating bitcoin's consensus mechanism and ordering blocks which ultimately represents bitcoin's full and valid transaction history (or its blockchain).

The basics of bitcoin: blocks and mining

Think of a block as a dataset that links the past to the present. Technically, individual blocks record changes to the overall state of bitcoin ownership within a given time interval. In aggregate, blocks record the entire history of bitcoin transactions as well as ownership of all bitcoin at any point in time. Only changes to the state are recorded in each passing block. How blocks are constructed, solved and validated is critical to the process of network consensus, and it also ensures that bitcoin maintains a fixed supply (21 million). Miners compete to construct and solve blocks that are then proposed to the rest of the network for acceptance. To simplify, think of the mining function as a continual process of validating history and clearing pending bitcoin transactions; with each block, miners add new transaction history to the blockchain and validate the entire history of the chain. It is through this process that miners secure the network; however, all network nodes then check the work performed by miners for validity, ensuring network consensus is enforced. More technically, miners construct blocks that represent data sets which include three critical elements (again simplifying):

1. Reference to prior block → validate entire history of chain
2. Bitcoin transactions → clear pending transactions (changes to the state of ownership)
3. Coinbase transaction + fees → compensation to miners for securing the network

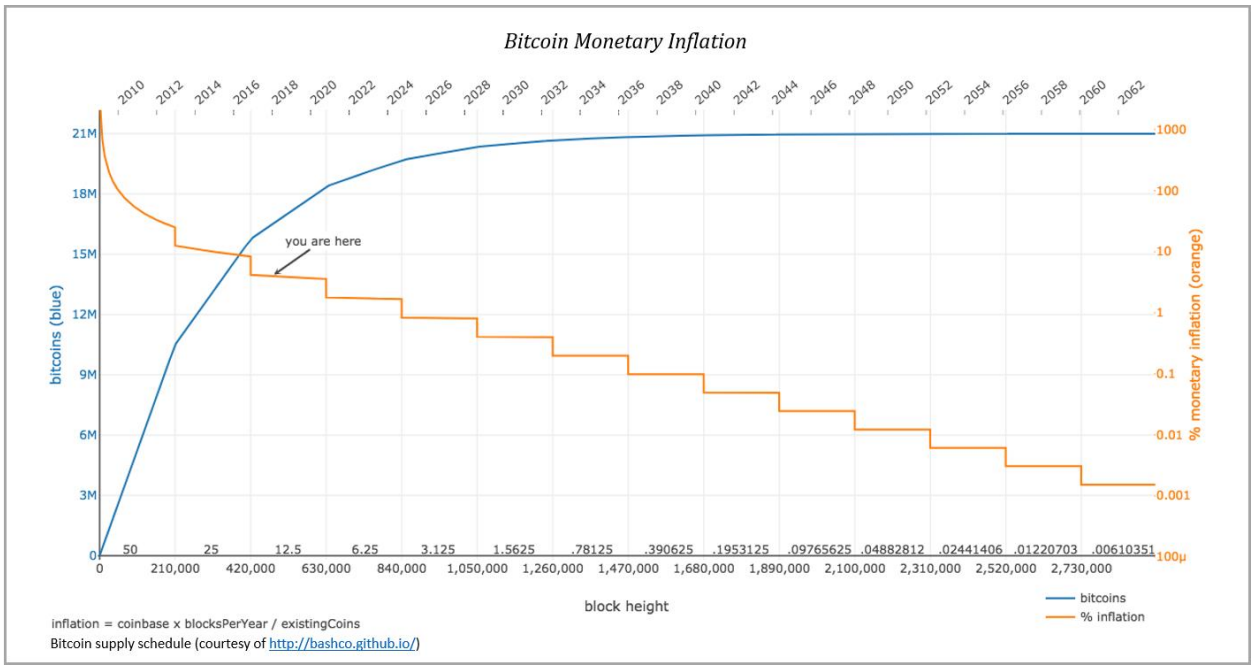


To solve blocks, miners perform what is known as a proof of work function by expending energy resources. In order for blocks to be valid, all inputs must be valid and each block must satisfy the current network difficulty. To satisfy the network difficulty, a random value (referred to as a nonce) is added to each block and then the combined data set is run through bitcoin's cryptographic hashing algorithm (SHA-256); the resulting output (or hash) must achieve the network's difficulty in order to be valid. Think of this as a simple guess and check function, but probabilistically, trillions of random values must be guessed and checked in order to create a valid proof for each proposed block. The addition of a random nonce may seem extraneous. But, it is this function that forces miners to expend significant energy resources in order to solve a block, which ultimately makes the network more secure by making it extremely costly to attack.

Adding a random nonce to a proposed block, which is an otherwise static data set, causes each resulting output (or hash) to be unique; with each different nonce checked, the resulting output has an equally small chance of achieving the network difficulty (i.e. representing a valid proof). While it is often referred to as a highly complicated mathematical problem, in reality, it is difficult only because a valid proof requires guessing and checking trillions of possible solutions. There are no shortcuts; energy must be expended. A valid proof is easy to verify by other nodes but impossible to solve without expending massive amount of resources; as more mining resources are added to the network, the network difficulty increases, requiring more inputs to be checked and more energy resources to be expended to solve each

block. Essentially, there is material cost to miners in solving blocks but all other nodes can then validate the work very easily at practically no cost.

In aggregate, the incentive structure allows the network to reach consensus. Miners must incur significant upfront cost to secure the network but are only paid if valid work is produced; and the rest of the network can immediately determine whether work is valid or not based on consensus rules without incurring cost. While there are a number of consensus rules, if any pending transaction in a block is invalid, the entire block is invalid. For a transaction to be valid, it must have originated from a previous, valid bitcoin block and it cannot be a duplicate of a previously spent transaction; separately, each block must build off the most up to date version of history in order to be valid and it must also include a valid coinbase transaction. A coinbase transaction rewards miners with newly issued bitcoin in return for securing the network but it is only valid if the work is valid.



Coinbase rewards are governed by a predetermined supply schedule and currently, 12.5 new bitcoin are issued in each valid block; in approximately eight months, the reward will be cut in half to 6.25 new bitcoin, and every 210,000 blocks (or approximately every four years), the reward will continue to be halved until it ultimately reaches zero. If miners include an invalid reward in a proposed block, the rest of the network will reject it as invalid which is the base mechanism that governs a capped total supply of 21 million bitcoin. However, software alone is insufficient to ensure either a fixed supply or an accurate transaction ledger; economic incentives hold everything together.

Consensus on a decentralized basis

Why is this so important? Within one integrated function, miners validate history, clear transactions and get paid for security on a trustless basis; the integrity of bitcoin's fixed supply is embedded in its security function, and because the rest of the network independently validates the work, consensus can be reached on a decentralized basis. If a miner completes valid work, it can rely on the fact that it will be paid on a trustless basis. Conversely, if a miner completes invalid work, the rest of the network enforces the rules, essentially withholding payment until valid work is completed. And supply of the currency is baked into validity; if a miner wants to be paid, it must also enforce the fixed supply of the currency, further aligning the entire network. The incentive structure of the currency is so strong that everyone is forced to adhere to the rules, which is the chief facilitator of decentralized consensus.

If a miner solves and proposes an invalid block, specifically one that either includes invalid transactions or an invalid coinbase reward, the rest of the network will reject it as invalid. Separately, if a miner builds off a version of history that does not represent the longest chain with the greatest proof of work, any proposed block would also be considered invalid. Essentially, as soon as a miner sees a new valid block proposed in the network, it must immediately begin to work on top of that block or risk falling behind and performing invalid work at a sunk cost. As a consequence, in either scenario, if a miner were to produce invalid work, it would incur real cost but would be compensated nothing in return.

Through this mechanism, miners are maximally incentivized to produce honest, valid work and to work within the consensus of the chain at all times; it is either be paid or receive nothing. It is also why the higher the cost to perform the work, the more secure the network becomes. The more energy required to write or rewrite bitcoin's transaction history, the lower the probability that any single miner could (or would) undermine the network. The incentive to cooperate increases as it becomes more costly to produce work which would otherwise be considered invalid by the rest of the network. As network security increases, bitcoin becomes more valuable. As the value of

bitcoin rises and as the costs to solve blocks increases, the incentive to produce valid work increases (more revenue but more cost) and the penalty for invalid work becomes more punitive (no revenue and more cost).

Why don't the miners collude? First, they can't. Second, they tried. But third, the fundamental reason is that as the network grows, the network becomes more fragmented and the economic value compensated to miners in aggregate increases; from a game theory perspective, more competition and greater opportunity cost makes it harder to collude and all network nodes validate the work performed by miners which is a constant check and balance. Miners are merely paid to perform a service and the more miners there are, the greater the incentive to cooperate because the probability that a miner is penalized for invalid work increases as more competition exists. And recall that random nonce value; it seemed extraneous at the time but it is core to the function that requires energy resources be expended. It is this tangible cost (skin in the game) combined with the value of the currency which incentivizes valid work and which allows the network to reach consensus.

Because all network nodes independently validate blocks and because miners are maximally penalized for invalid work, the network is able to form a consensus as to the accurate state of the chain without relying on any single source of knowledge or truth. None of this decentralized coordination would be possible without bitcoin, the currency; all the bitcoin network has to compensate miners in return for security is its native currency, whether that is largely in the form of newly issued bitcoin today or exclusively in the form of transaction fees in the future. If the compensation paid to miners were not reasonably considered to be a reliable form of money, the incentive to make the investments to perform the work would not exist.

The role of money in a blockchain

Recall from Bitcoin Can't Be Copied, if an asset's primary (if not sole) utility is the exchange for other goods and services, and if it does not have a claim on the income stream of a productive asset (such as a stock or bond), it must compete as a form of money and will only store value if it possesses credible monetary properties. Bitcoin is a bearer asset, and it has no utility other than the exchange for other goods or services. It also has no claim on the income stream of a productive asset. As such, bitcoin is only valuable as a form of money and it only holds value because it has credible monetary properties (read The Bitcoin Standard, chapter 1). By definition, this is true of any blockchain; all any blockchain can offer in return for security is a monetary asset native to the network, without any enforceable claims outside the network, which is why a blockchain can only be useful in connection to the

application of money. The chart below from The Bitcoin Standard articulates this point:

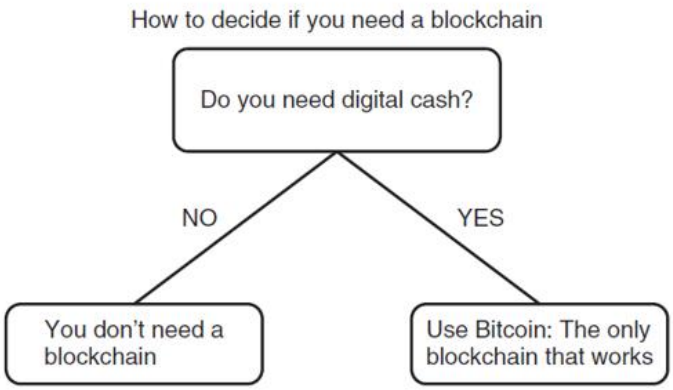


Figure 22 Blockchain decision chart.

Without a native currency, a blockchain must rely on trust for security which eliminates the need for a blockchain in the first place. In practice, the security function of bitcoin (mining), which protects the validity of the chain on a trustless basis, requires significant upfront capital investment in addition to high marginal cost (energy consumption). In order to recoup that investment and a rate of return in the future, the payment in the form of bitcoin must more than offset the aggregate costs, otherwise the investments would not be made. Essentially, what the miners are paid to protect (bitcoin) must be a reliable form of money in order to incentivize security investments in the first place.

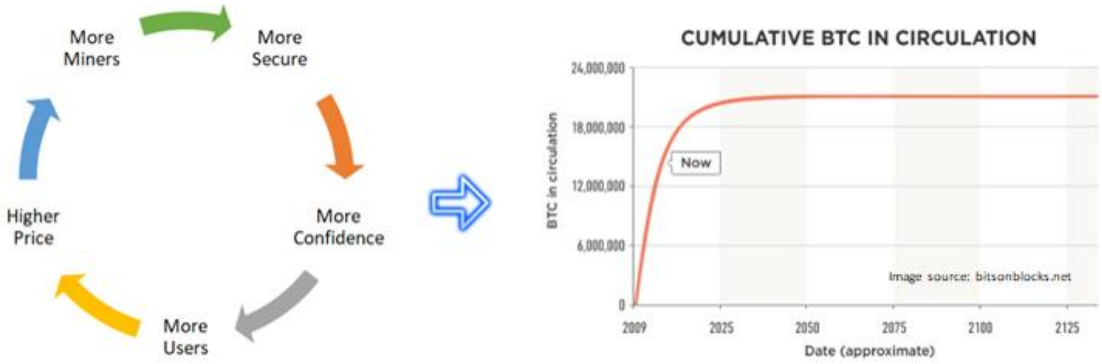
This is also fundamental to the incentive structure that aligns the network; miners have an embedded incentive to not undermine the network because it would directly undermine the value of the currency in which miners are compensated. If bitcoin were not valued as money, there would be no miners, and without miners, there would be no chain worth protecting. The validity of the chain is ultimately what miners are paid to protect; if the network could not reasonably come to a consensus and if ownership were subject to change, no one could reasonably rely on bitcoin as a value transfer mechanism. The value of the currency ultimately protects the chain, and the immutability of the chain is foundational to the currency having value. It's an inherently self-reinforcing relationship.

Immutability is an emergent property

Immutability is an emergent property in bitcoin, not a trait of a blockchain. A global, decentralized monetary network with no central authority could not function without an immutable ledger (i.e. if the history of the blockchain were insecure and subject to change). If settlement of the unit of value (bitcoin) could not reliably be considered final, no one would reasonably trade real world value in return. As an example, consider a scenario in which one party purchased a car from another in return for bitcoin. Assume the title for the car transfers, and the individual that purchased the car takes physical possession. If bitcoin's record of ownership could easily be re-written or altered (i.e. changing the history of the blockchain), the party that originally

transferred the bitcoin in return for the car could wind up in possession of both the bitcoin and the car, while the other party could end up with neither. This is why immutability and final settlement is critical to bitcoin's function.

Remember that bitcoin has no knowledge of the outside world; all bitcoin knows how to do is issue and validate currency (whether a bitcoin is a bitcoin). Bitcoin is not capable of enforcing anything that exists outside the network (nor is any blockchain); it is an entirely self-contained system and the bitcoin network can only ever validate one side of a two-sided value transfer. If bitcoin transfers could not reliably be considered final, it would be functionally impossible to ever trade anything of value in return for bitcoin. This is why the immutability of bitcoin's blockchain is inextricably linked to the value of bitcoin as a currency. Final settlement in bitcoin is possible but only because its ledger is reliably immutable. And its ledger is only reliably immutable because its currency is valuable. The more valuable bitcoin becomes, the more security it can afford; the greater the security, the more reliable and trusted the ledger.



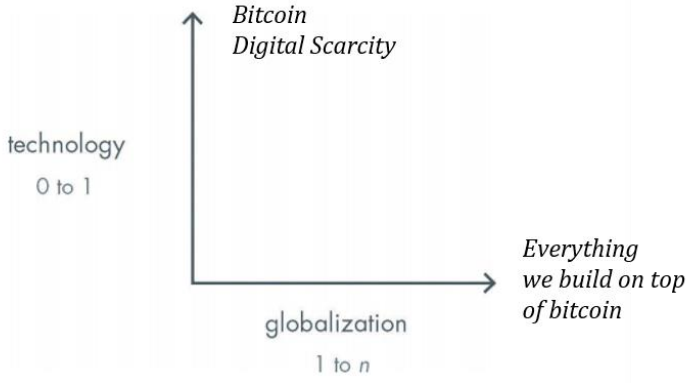
Ultimately, immutability is an emergent property, but it is dependent on other emergent network properties. As bitcoin becomes more decentralized, it becomes increasingly difficult to alter the network's consensus rules and increasingly difficult to invalidate or prevent otherwise valid transactions (often referred to as censorship-resistance). As bitcoin proves to be increasingly censorship-resistant, confidence in the network grows, which fuels adoption, which further decentralizes the network, including its mining function. In essence, bitcoin becomes more decentralized and more censorship-resistant as it grows, which reinforces the immutability of its blockchain. It becomes increasingly difficult to change the history of the blockchain because each participant gradually represents a smaller and smaller share of the network; regardless of how concentrated ownership of the network and mining may be at any point in time, both decentralize over time so long as value increases, which causes bitcoin to become more and more immutable.

Bitcoin, not blockchain

This multi-dimensional incentive structure is complicated but it is critical to understanding how bitcoin works and why bitcoin and its blockchain are dependent on each other. Why each is a tool that relies on the other. Without one, the other is effectively meaningless. And this symbiotic relationship only works for money. Bitcoin as an economic good is only valuable as a form of money because it has no other utility. This is true of any asset native to a blockchain. The only value bitcoin can ultimately provide is through present or future exchange. And the network is only capable of a single aggregate function: validating whether a bitcoin is a bitcoin and recording ownership.

The bitcoin network is a closed loop and an entirely independent system; its only connection to the physical world is through its security and clearing function. The blockchain maintains a record of ownership and the currency is used to pay for the security of those records. It is through the function of its currency that the network can afford a level of security to ensure immutability of the blockchain, which allows network participants to more easily and consistently reach consensus without the need for trust in any third-parties. The cumulative effect is a decentralized and trustless monetary system with a fixed supply that is global in reach and accessible on a permissionless basis.

Every other fiat currency, commodity money or cryptocurrency is competing for the **exact same use case as bitcoin** whether it is understood or not, and monetary systems tend to a single medium because their utility is liquidity rather than consumption or production. When evaluating monetary networks, it would be irrational to store value in a smaller, less liquid and less secure network if a larger, more liquid and more secure network existed as an attainable option. Bitcoin is valuable, not because of a particular feature, but instead, because it achieved finite, digital scarcity. This is the backbone of why bitcoin is secure as a monetary network and it is a property that is dependent on many other emergent properties.



A blockchain on the other hand is simply an invention native to bitcoin that enables the removal of trusted third parties. It serves no other purpose. It is only valuable in bitcoin as a piece to a larger puzzle and it would be useless if not functioning in concert with the currency. The integrity of bitcoin's scarcity and the immutability of its blockchain are ultimately dependent on the value of the currency itself. Confidence in the aggregate function drives incremental adoption and

liquidity which reinforces and strengthens the value of the bitcoin network as a whole. As individuals opt in to bitcoin, they are at the same time, opting out of inferior monetary networks. This is fundamentally why the emergent properties in bitcoin are next to impossible to replicate and why its monetary properties become stronger over time (and with greater scale), while also at the direct expense of inferior monetary networks.

"I don't believe we shall ever have a good money again before we take the thing out of the hands of government, that is, we can't take them violently out of the hands of government, all we can do is by some sly roundabout way introduce something that they can't stop." -F. A. Hayek

Ultimately, a blockchain is only useful in the application of money because it is dependent on a native currency for security. Bitcoin represents the most secure blockchain by orders of magnitude. Because all other blockchains are competing for the same fundamental use case of money and because bitcoin's network effects only continue to increase its security and liquidity advantage over the field, no other digital currency can compete with bitcoin. Liquidity begets liquidity and monetary systems tend to one medium as a derivative function. Bitcoin's security and liquidity obsoleted any other cryptocurrencies before they left the proverbial gates. Find me a cryptocurrency that comes close to bitcoin relative to security, liquidity or the credibility of its monetary properties, and I will find you a unicorn.

The real competition for bitcoin has and will remain the legacy monetary networks, principally the dollar, euro, yen and gold. Think about bitcoin relative to these legacy monetary assets as part of your education. Bitcoin does not exist in a vacuum; it represents a choice relative to other forms of money. Evaluate it based on the relative strengths of its monetary properties and once a baseline is established between bitcoin and the legacy systems, this will then provide a strong foundation to more easily evaluate any other blockchain related project.

To learn more, I suggest reading, The Bitcoin Standard (Saifedean Ammous), Inventing Bitcoin (Yan Pritzker) and Mastering Bitcoin (Andreas Antonopolous), probably in that order.

Next week: to be determined...

Thanks to Will Cole, Phil Geiger and Adam Tzagournis for reviewing and providing valuable feedback. Also thanks to Saif, Yan and Andreas for their books which are incredible resources.

Views presented are expressly my own and not those of Unchained Capital or my colleagues; if you would like to subscribe to weekly releases, please click here.

Mainstream Media of Exchange

By Knut Svanholm

Posted September 6, 2019

What is a Medium of Exchange? A monetary good is often described as a Store of Value, a Medium of Exchange and a Unit of Account. But what do these mean and in what order are they important for a monetary good to succeed, short term and long term? It all depends on the depth of one's analysis.

Let's rewind to the dawn of civilized society. Money hasn't really been invented yet and good old barter is the only means of trading there is. I will give you my three goats if you give me your cow. If the receiver of this proposal values three goats more than one cow, an exchange occurs. This is at the very core of all human interaction that isn't violent. Both parties believe that they stand to gain something from the interaction. If this wasn't the case, no interaction would have taken place. But how can I know that one or more of my three goats won't be used as barter in another exchange of which I'm not a participant? I can't and neither can anyone else, except the new owner of these bearded omnivores. They are by definition a Medium of Exchange. So is everything else. Every physical thing that anyone has ever claimed ownership of can be used as a Medium of Exchange. The good's usefulness as such however, is another matter.

A goat is hardly considered to be a very effective form of value bearing asset by anyone. Let's examine why. In order for a good to be a useful Medium of Exchange it needs to be portable, divisible, fungible and not easily confiscatable but it also needs to be able to store value, at least short term. Storing value is the trickiest part since what anyone finds valuable is entirely subjective. This is easy to forget. In what order the other monetary properties are important depends on how, where, why and when the supposed exchange takes place. A car, for instance, can be considered relatively portable if it works and the potential buyer is within an acceptable range but

it's not very divisible and quite easy to confiscate. In-game gold or Monopoly money on the other hand is very divisible and portable but not very fungible since it's almost exclusively attractive to those playing a very specific game at a very specific point in time. These examples might seem arbitrary and insignificant to any real world economy, but the truth is that the only thing separating money from other goods as media of exchange is its usefulness as such.

In order for anyone to accept something as payment for another thing they need to be confident that this something will not lose its value anytime soon. This is the one key property that any method of payment must hold. An apple can be bought for a certain amount of money but no one would accept apples as payment for a new car since the apples would rot and lose their value well before he could exchange them for something else. What everyone seems to have forgotten is that the same is true for fiat money. Your Dollars or Euros won't rot overnight but they will rot over a couple of decades. No one stacks money in their mattress anymore because of this. Inflation deprives us of the ability to store value long term. Because of this, every decision made by every politician, every merchant and every entrepreneur is corroded by short term thinking. Human progress is equipped with a damper and we're not as progressive, effective or innovative as we could be. All because of our inability to resist the urge to dilute our money supply. The temptation to counterfeit has existed as long as money has and no civilization has ever been able to stop it. On the contrary, we've been very inventive when it comes to inventing excuses for this behavior.

Enter Bitcoin. A monetary entity that no human can alter or even influence at this point. A very divisible token directly linked to the most fundamental thing of value the universe has to offer — energy. A means of converting energy into a part of the worlds only digital pie, of which no more than 21 million (times a hundred million) slices can ever be cut. A portable, divisible, fungible and not easily confiscatable form of money that exists and proves its superiority to the existing system every day. So why isn't Bitcoin particularly popular as a Medium of Exchange? Will it ever be and, more importantly, does it really matter? To answer this, we must dive a little deeper into the subject. Bitcoin is a very good Store of Value from a personal perspective. You acquire an amount and that amount stays the same no matter how long you keep it. More importantly, that amount will represent the same part of the whole sum of bitcoins that can ever exist no matter how long you keep it. If you want your specific amount of bitcoins to buy you a "lambo", all you have to do is wait for someone to be willing to sell you a "lambo" for that amount. This might take a while (or it might not) but if Bitcoin just manages to keep on doing what it does, this day will happen. It is only a matter of time because, unlike "lambos", bitcoins are scarce. Very scarce. Even absolutely scarce, which is a property of an asset that mankind has never encountered

before. More and more people realize this which is why they're reluctant to sell their bitcoins. The newly minted bitcoins that are mined every day need to be sold in order for the miner's business models to work but the ones that are already in circulation tend to stay where they are because people value them a lot higher than what the current price in dollars or euros happen to be.

A good Medium of Exchange needs to be able to store value. The better it stores value however, the less likely people are to exchange it for something that isn't likely to store value as well. Bitcoin's value has such a large potential upside that people refuse to exchange it for frivolous things such as coffee or even mass produced cars. Contrary to what one might think, this doesn't make it a bad Medium of Exchange. Quite the opposite. How often a Medium of Exchange is used is not the correct metric to look at when trying to measure its usefulness as such a medium. This misses the point. What should be measured is said medium's ability to buy you as much or more than you bought it for at some point in time. Bitcoin is the only tool available that practically guarantees this. Fiat money, inflation and the ideas of John Maynard Keynes have distorted our perception of what money ought to be so much that we believe that how convenient it is to buy coffee with it, is the most important thing about it.

Looking only at the merchant adoption and spread of acceptance metrics, Bitcoin still seems to be struggling quite a lot. In reality, this is a non sequitur and has little to do with the actual success and functionality of the network. The price of a bitcoin, as shown by ticker widgets and market cap websites, represents the lowest current price that anyone is willing to accept on an exchange market. Only a very few bitcoin owners are willing to accept this price and most of them are waiting for a better opportunity. Bitcoin is indeed a currency, but it behaves very differently in comparison to all other currencies that preceded it. The fact that people are reluctant to use bitcoin for everything but a few, very important transactions is a proof of bitcoin's monetary superiority rather than anything else. So forget about coffee, forget about whether you franchise burger joint accepts bitcoin and start focusing on what you can use this tool for. Bitcoin is a true grassroots revolution and it grows from the ground up, not the other way around.

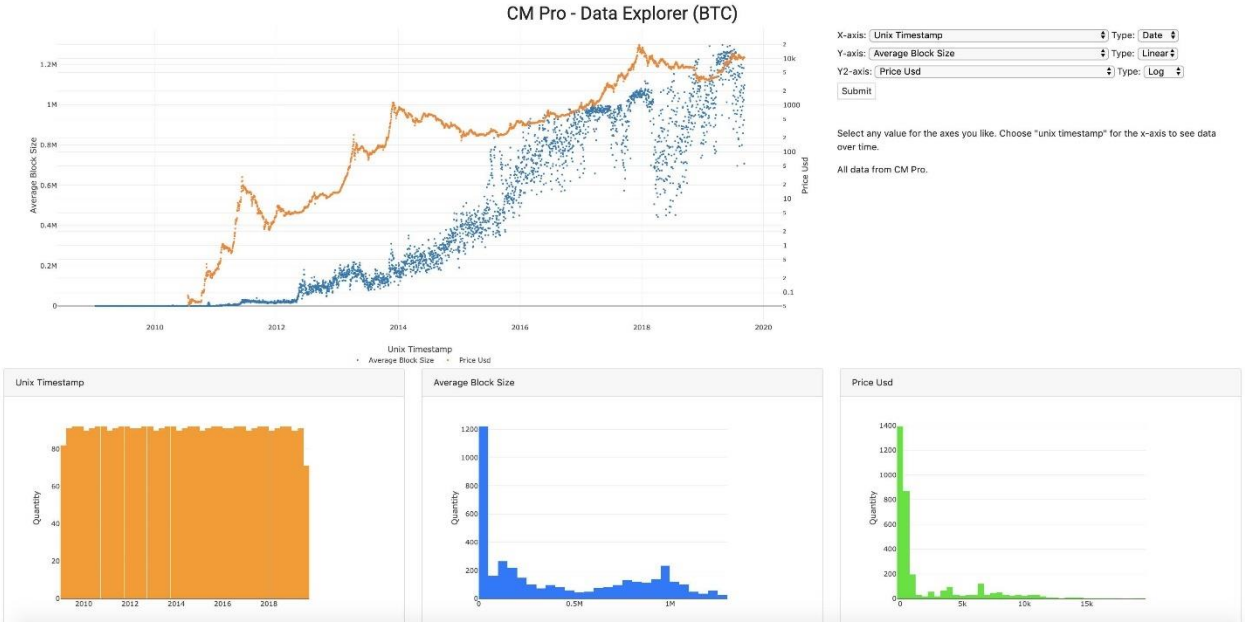
Tweetstorm: 21 Charts

By Hans Hauge

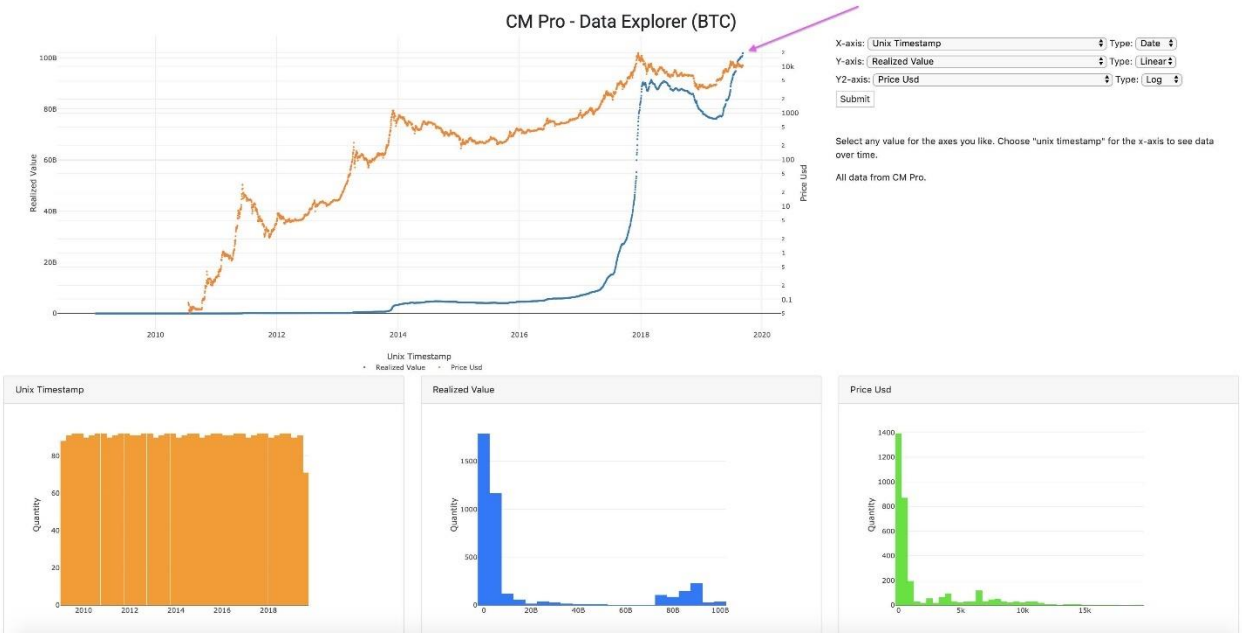
Posted September 10, 2019

I've heard people say that being involved in Bitcoin is a game of speculation. Some say it's all about FUD, FOMO, Fear and Greed or following the crowd. I call BS. Let's look at the data! Here are 21 Bitcoin charts from @coinmetrics that tell a different story.

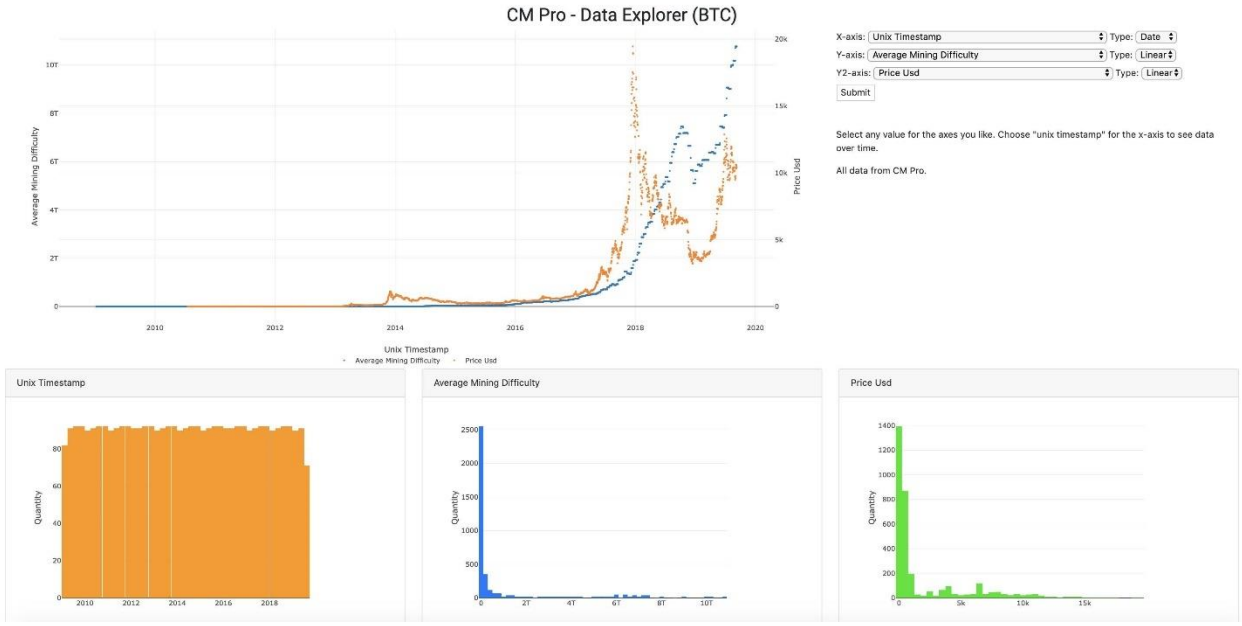
The amount of data being stored on the blockchain has been increasing constantly, regardless of the price. Why do people want to transmit data on the Bitcoin blockchain? It's all about trust and the ability to transfer value without asking permission!



Realized value is at an all-time high. This is the amount the coins are worth the last time they were moved. Look at that momentum...

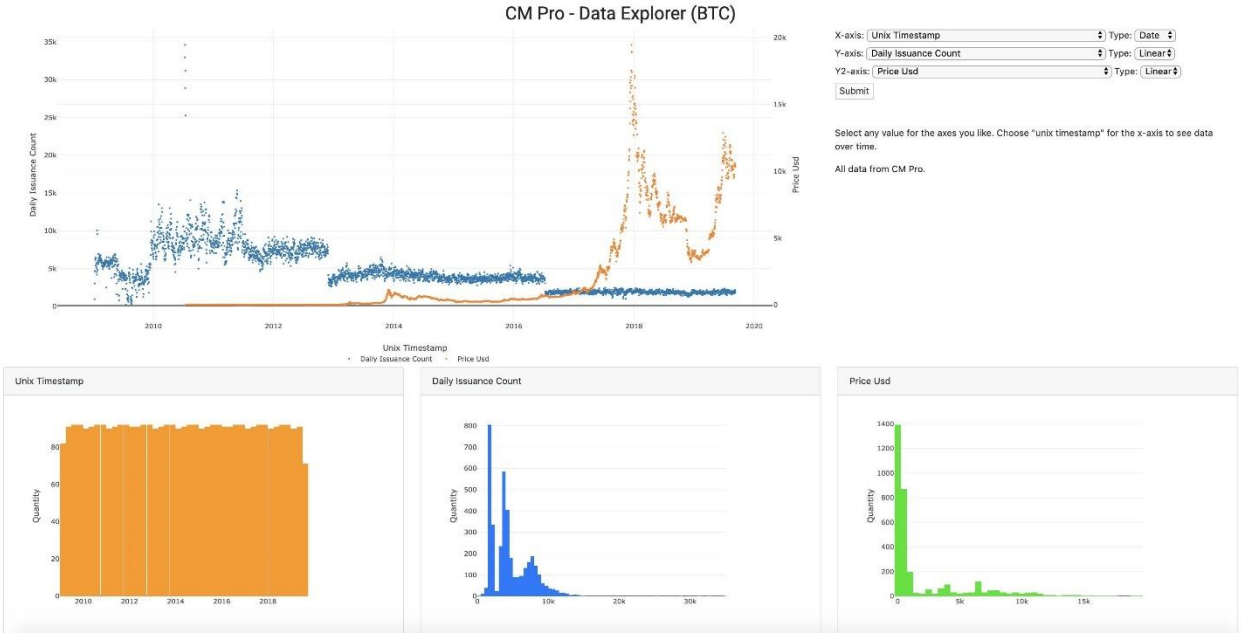


Look at the current mining difficulty. This represents an immense investment in infrastructure for the future of Bitcoin. Do the miners look worried to you? I estimate this represents at least a $10B investment in CAPEX and look at the growth...

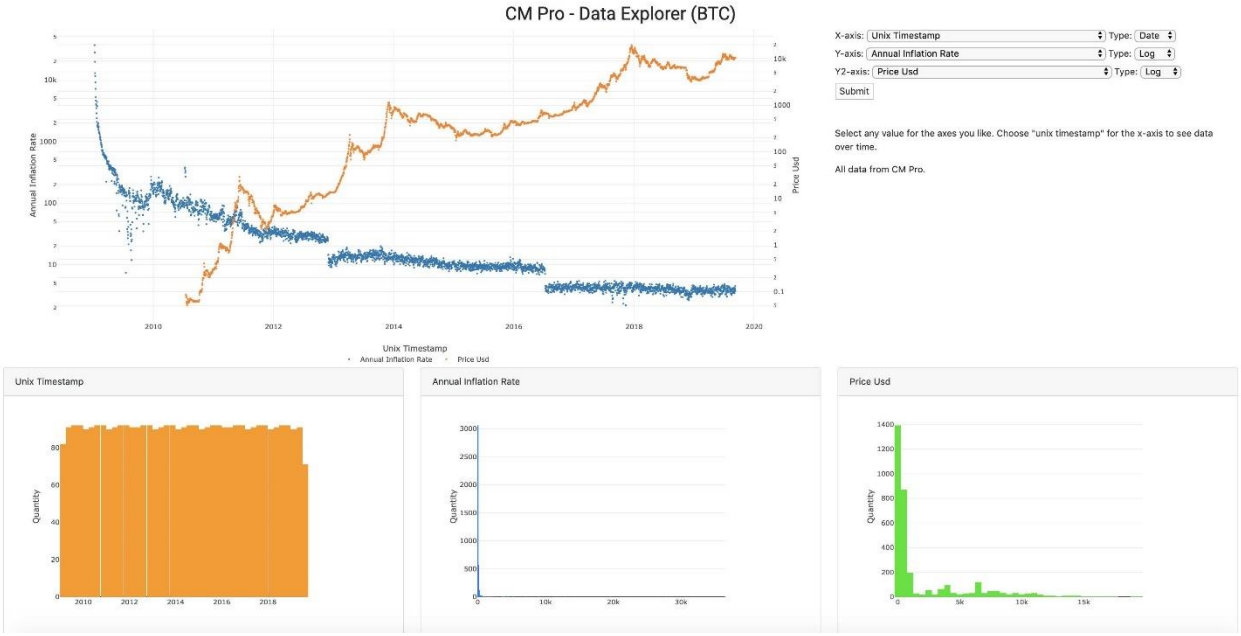


Check out the median transaction fee pull-back. The same thing happened in the last bubble. The price at those arrows on the left was $1k and $2.6k, which seemed high at the time. In retrospect, de nada.

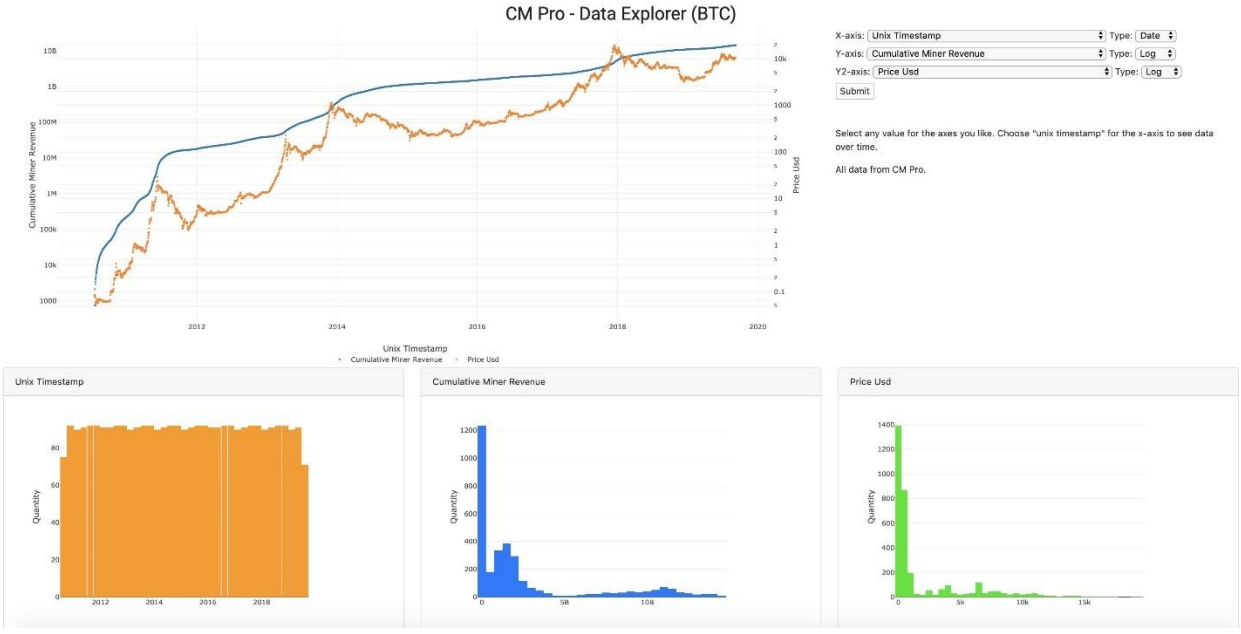
Daily issuance count, look at the decline. This reduction in new supply fuels one of the most basic laws of economics, which most commonly applies to commodities, Supply and Demand. If the supply gets squeezed and the demand keeps increasing, well...



Here's another view that takes into account the circulating supply. This is the Annual Inflation Rate. Who's ready for the next halving?

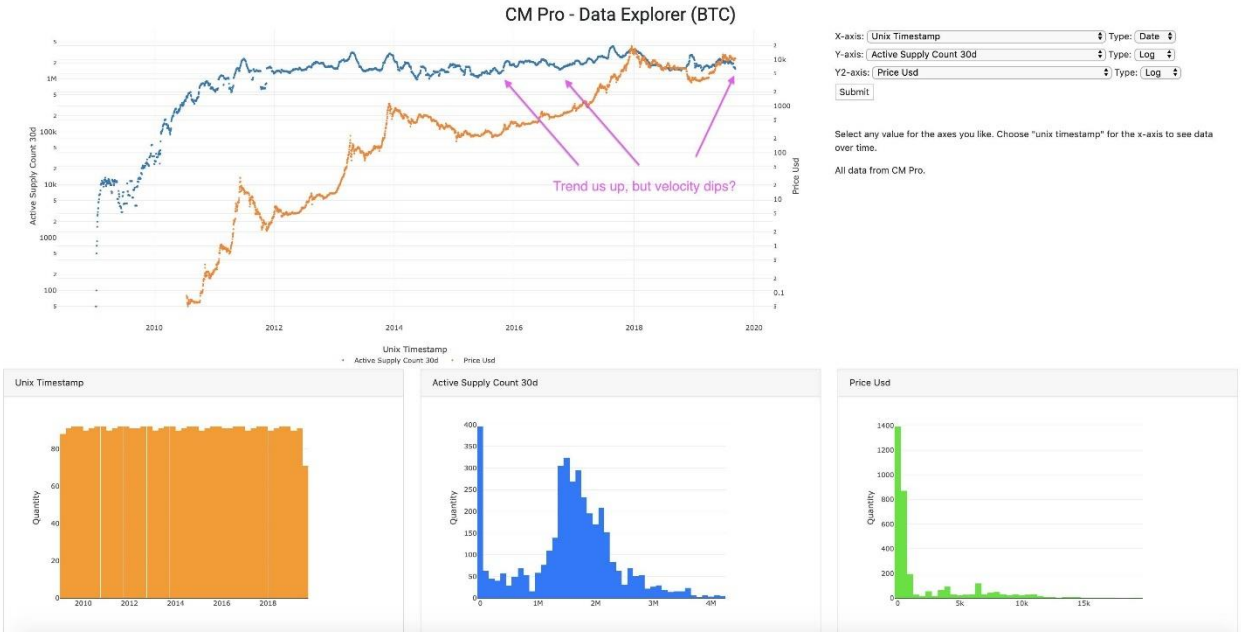


We talked about the miners earlier. What's driving that increase in difficulty? If you answered "Revenue growth for the industry in Log(Log()) scale" you get a gold star!

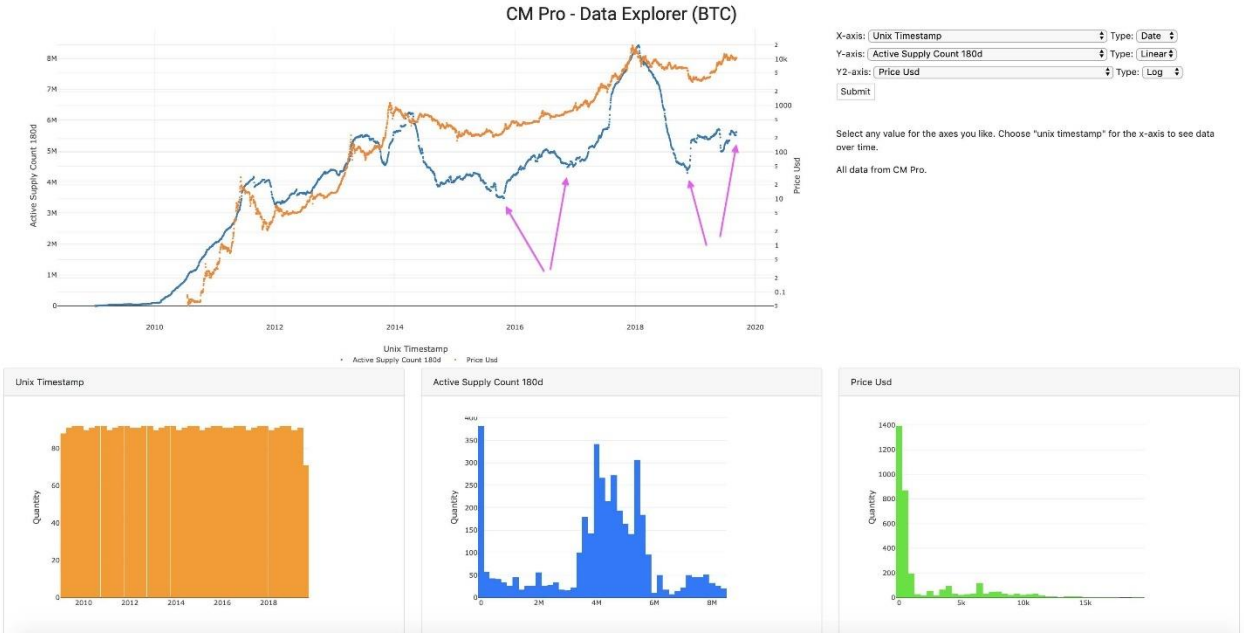


Let's turn our attention to the active supply over the last seven days. This gives us unique insight into the behavior of Bitcoiners, specifically if they're holding or trading. When the blue line touches the red line, there's more HODLing going on, bullish in a bull market.

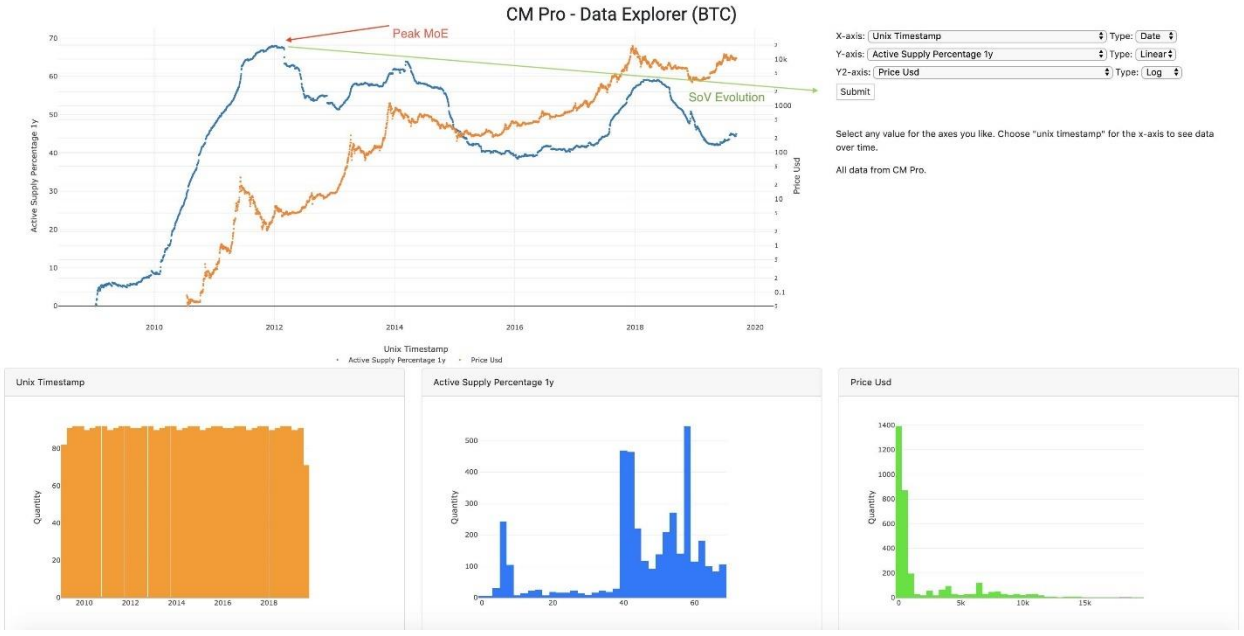
If we substitute the 30 day count for the 7 day, we get an even better picture. In the middle of a bull market, we see velocity drop. Why? This is the calm before the storm...



Now look at this, expanding to 180 days. One - Bottom of the cycle, Two - Second chance to buy in, Three - Moon. 2017 - the price in floor two fell from the $700 range to the $500 range; 2019 the price fell from about $14k to where we are now, near $10k. Same Bitcoin, 20x bigger.

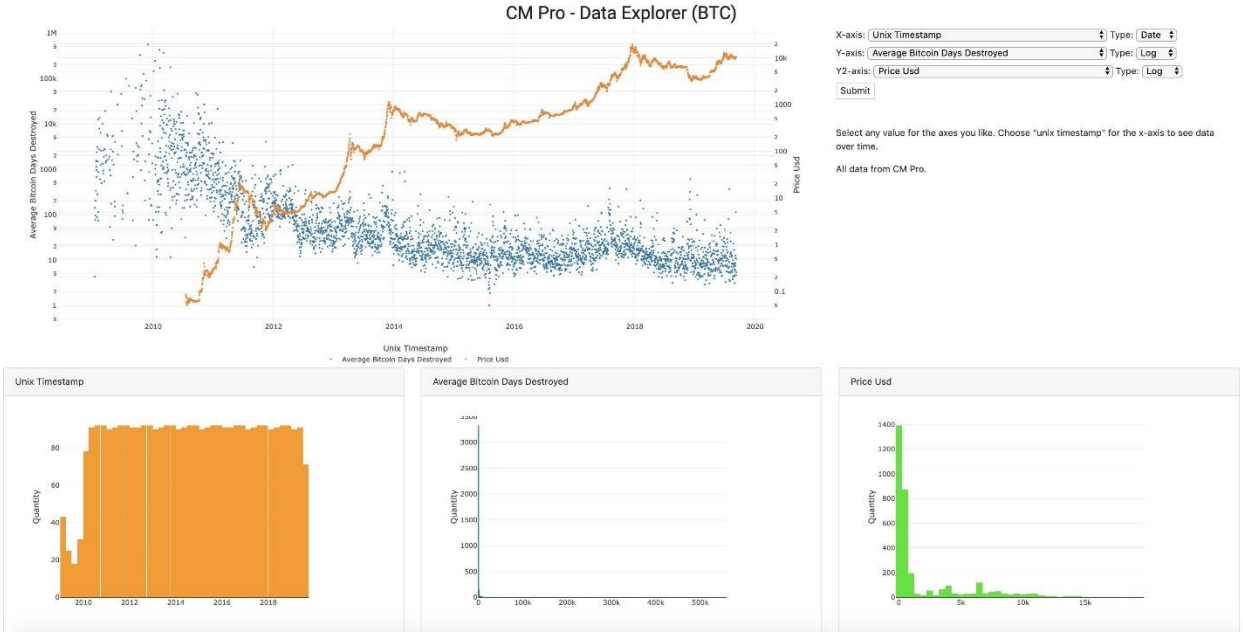


Waxing philosophical for a moment, I suggest Bitcoin is evolving from a Method of Exchange that can store value to a SoV that can be exchanged. As the market value increases, look at the change in the active supply percentage over the trailing 1y.

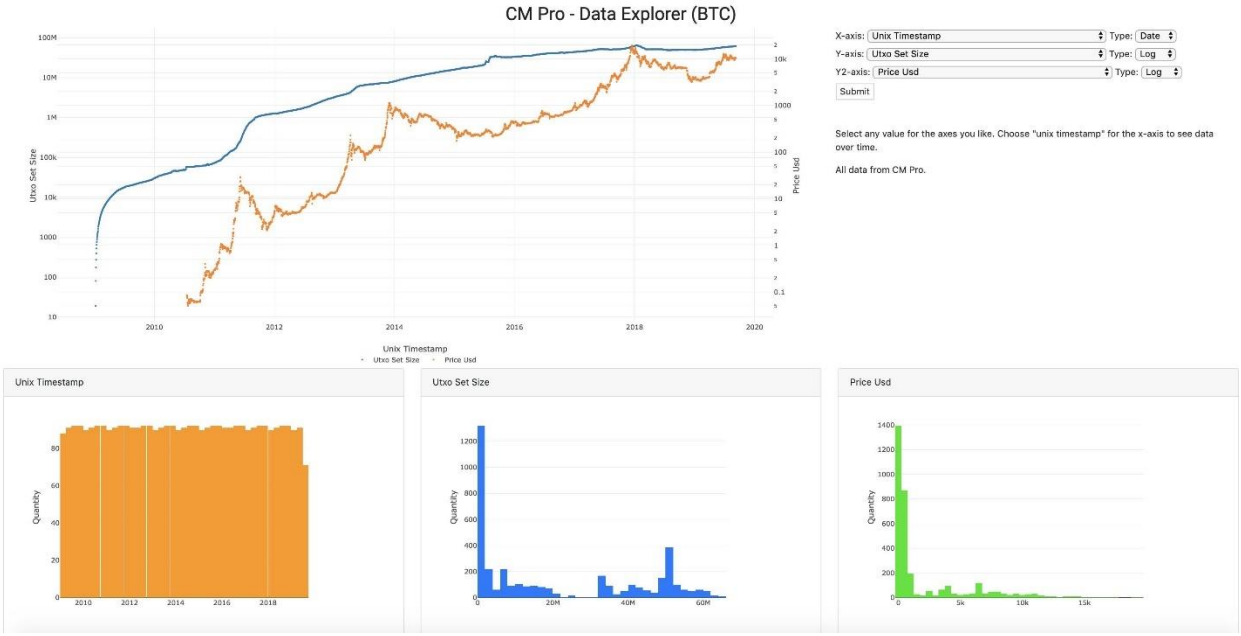


Coming back to the “two chances to enter” model for a moment, isn’t it a bit spooky how history looks like it’s repeating itself? Check out the value per byte transferred below. Got your ticket to the moon yet?

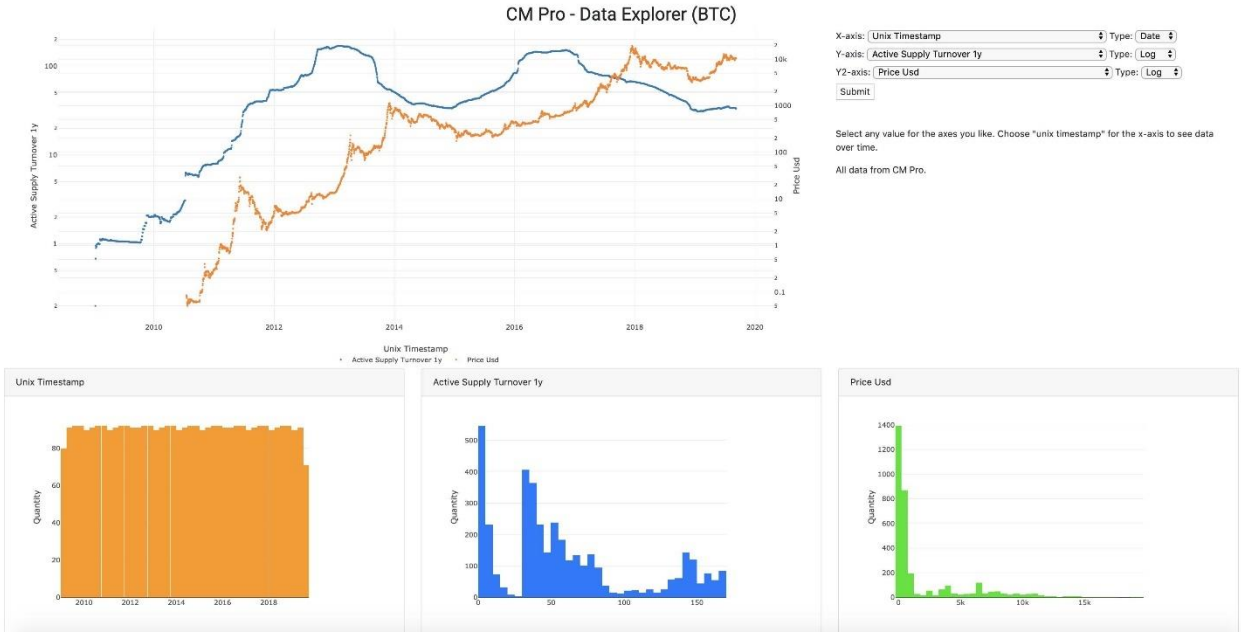
I normally talk about Bitcoin Days Destroyed in the sense of the TOTAL number or the adjusted figure (total / circulating supply). But, if we look at the average there is a constant decline. The longer you HOLD, the less you want to FODL paradoxically. Bitcoin Singularity?



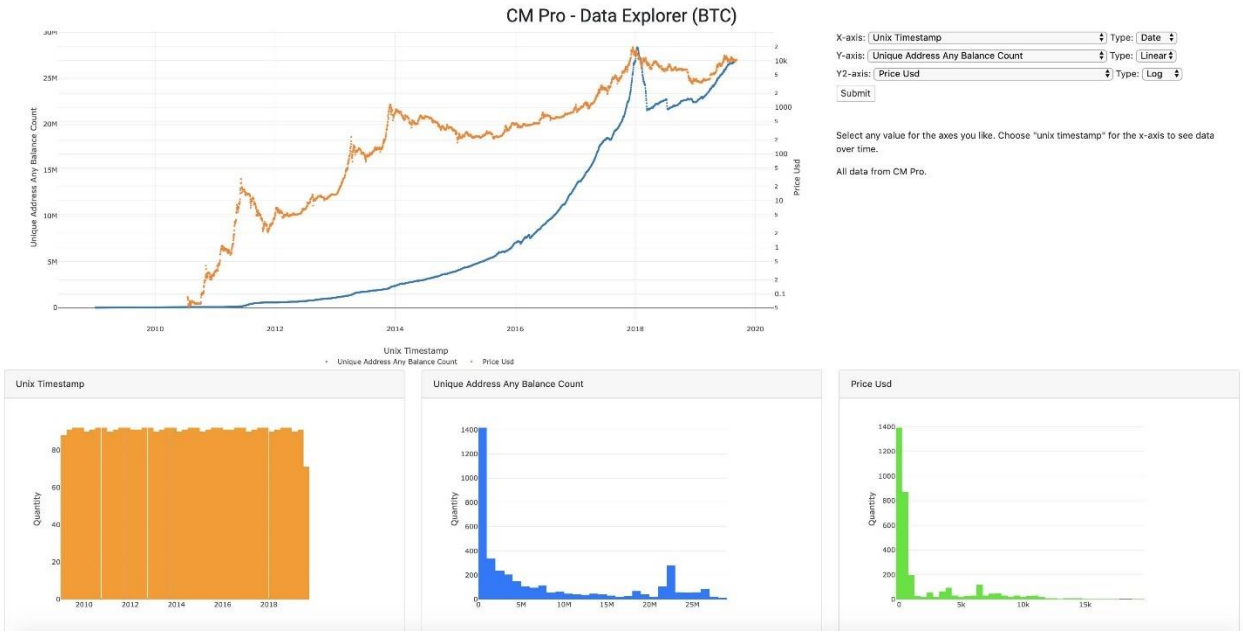
We talked about supply, now let's look at demand using the UTXO set size as another way to conceptualize the participants in the Bitcoin network. Look at the growth here. This is getting very close to an all-time high as well.



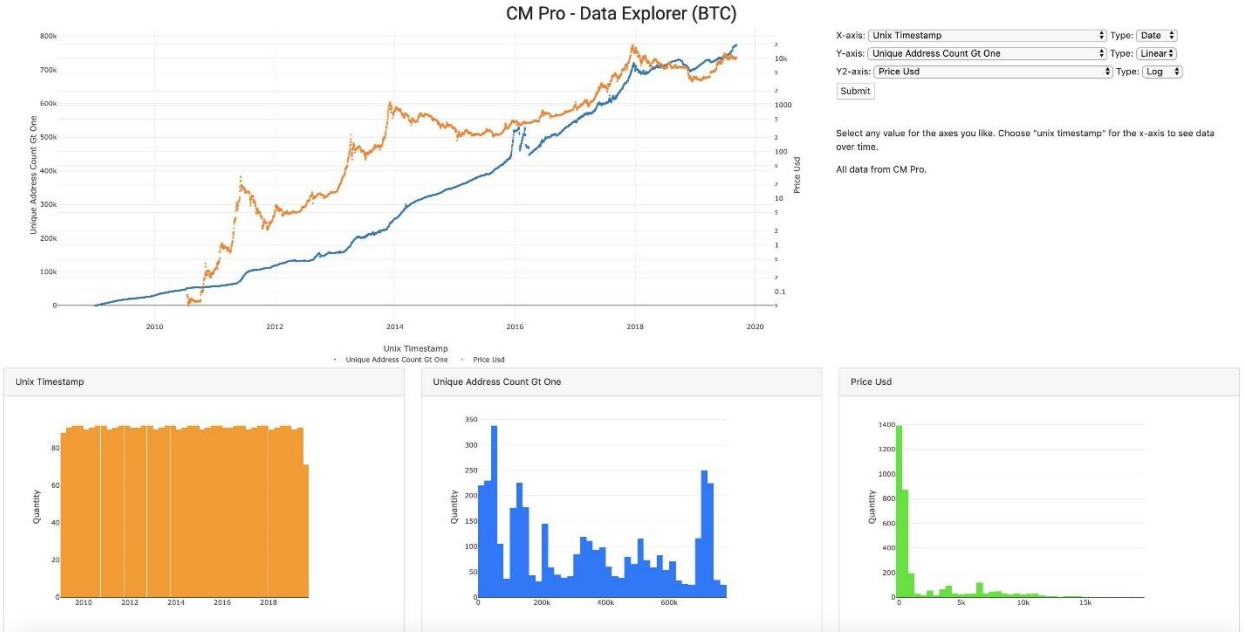
In inventory management, turnover is a good thing because it shows you're moving your product. But with Bitcoin, we have to consider that an increase in HODLing means Bitcoin is transitioning into a Store of Value as I mentioned before. Inventory turnover also supports this view.



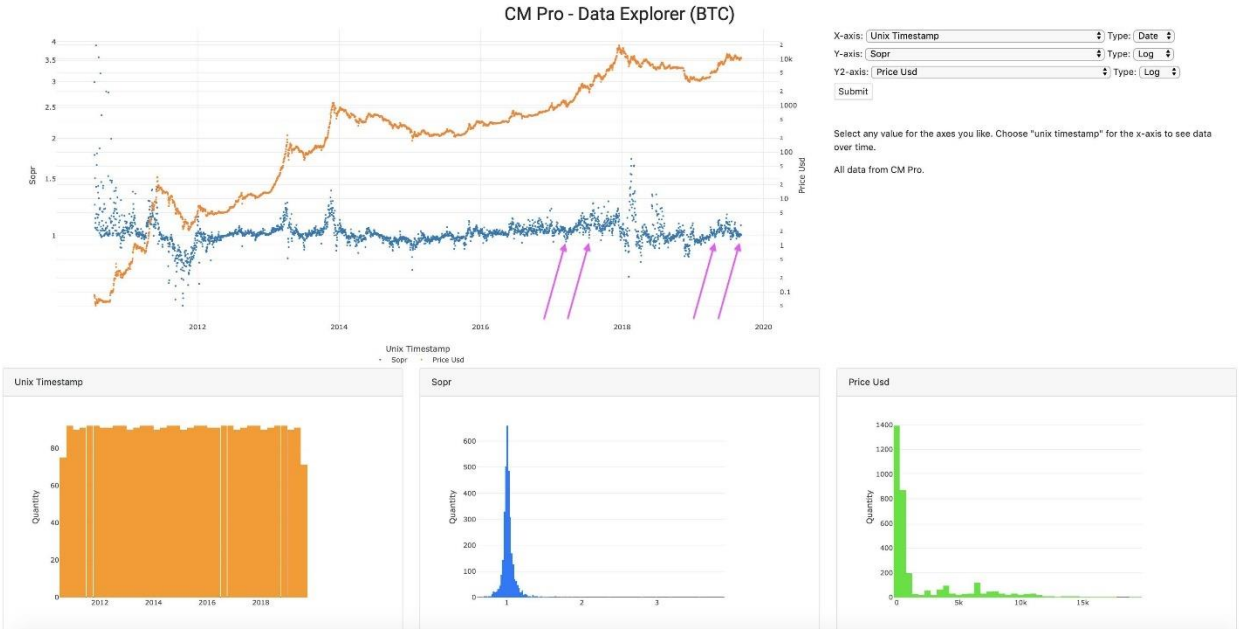
Back on the demand side again for you Econ nerds, we can also look at the number of unique addresses that hold ANY balance of Bitcoin. Also, this is near an ATH.



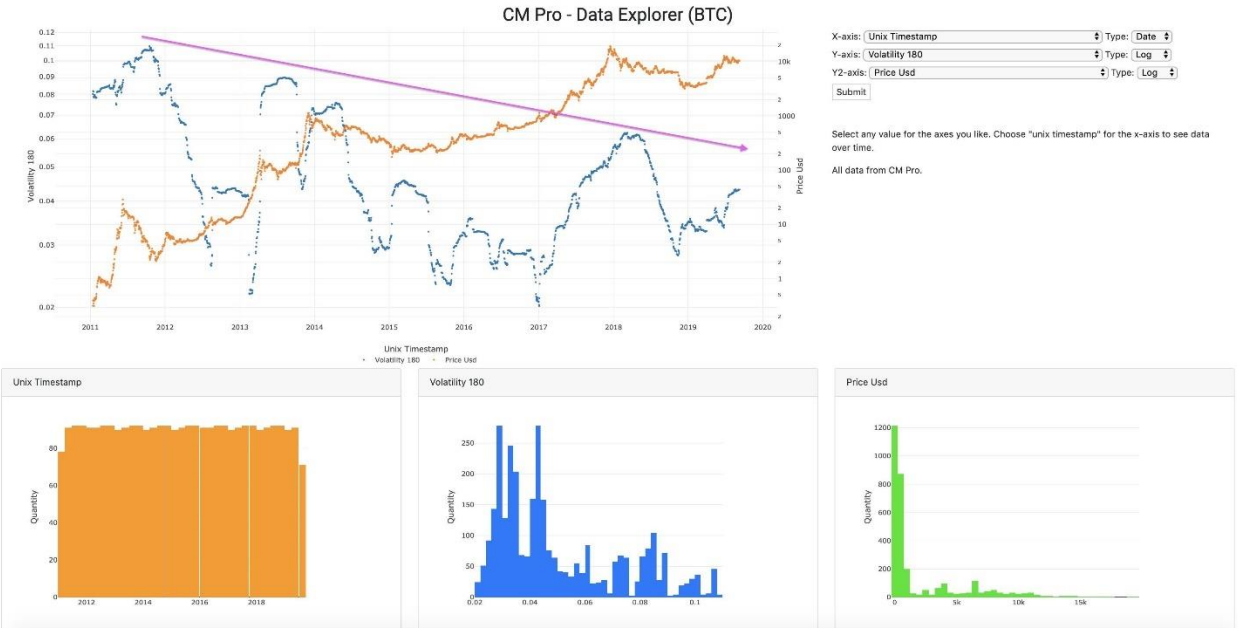
If we ask “How many addresses have at least 1 BTC” the answer would be in the blue line below. This figure IS at an all-time high (as of yesterday). The virus is spreading!



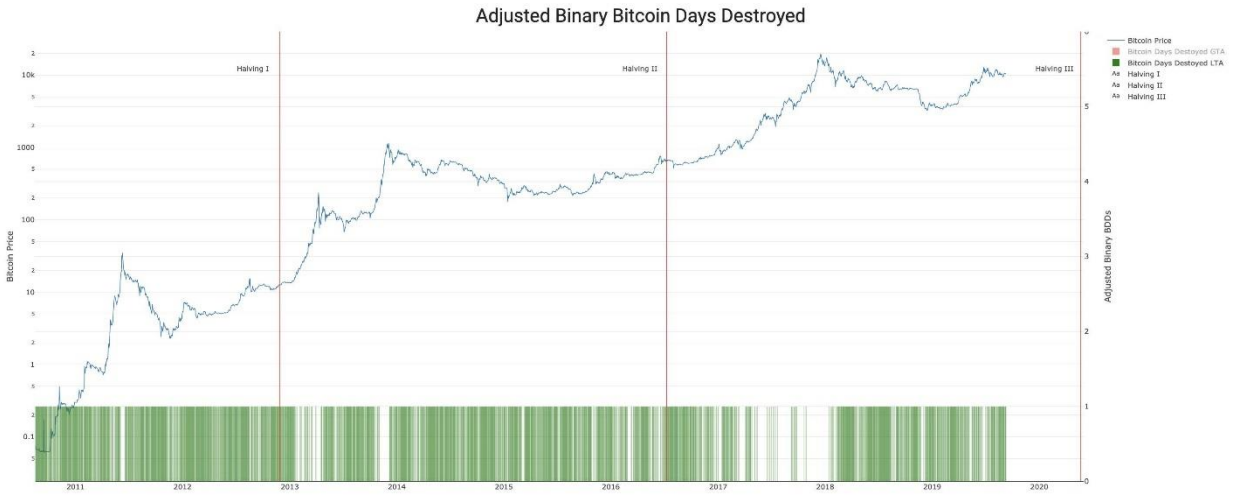
SOPR has reset to the “around 1” level. Last time we saw this the price was around $5k. Now we have SOPR around 1 at $10k. To me this speaks of the lower risk to entry. @renato_shira can correct me if I misunderstand.



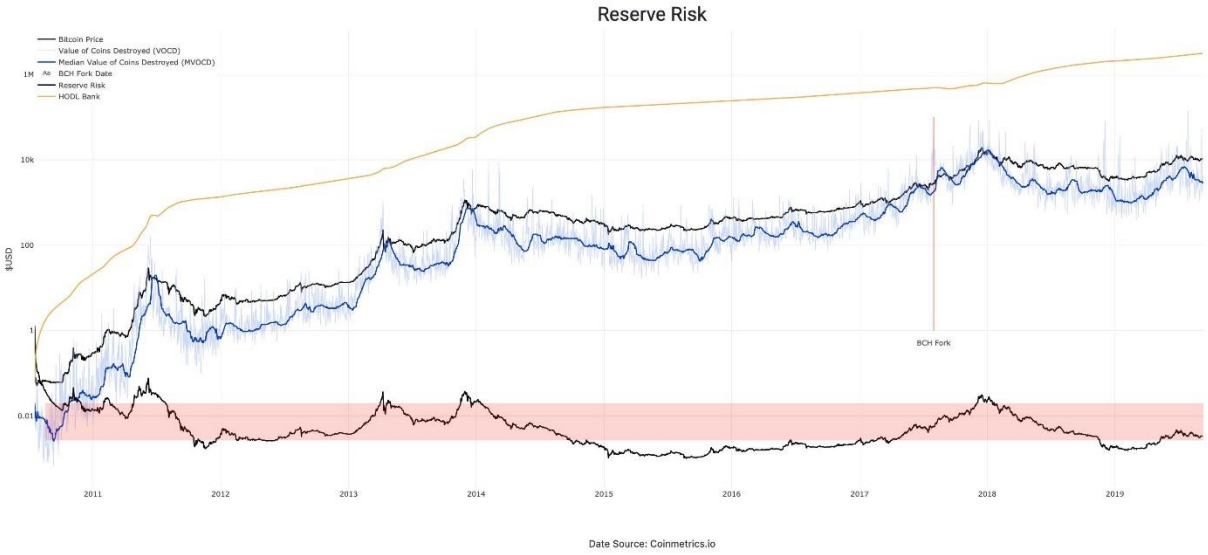
And of course volatility is decreasing over time in log scale. NBD. Majority of the volatility to the upside but let's not mention that.



Another view of Bitcoin Days Destroyed, Adjusted Binary BDD. Green bars are LESS than average on an adjusted basis. Unless you see a white gap, we're not at the top of a bubble. It's just data.



And lastly, Reserve Risk which answers the question “how much risk to I take on by entering now?” I rest my case.



Floor on Bitcoin's risk less interest rate

By Tamas Blummer

Posted September 11, 2019

There is a floor to Bitcoin's risk less interest rate determined by its mining schedule.

Risk less interest is an income one gets paid in a deal that can not go wrong. This sounds like investors' wet dream, but there is a real world example of it in the fiat money world, the treasury bonds.

Since the government may print any amount, it will never default on a loan denominated in its own currency. The interest may not have the expected purchasing power, but it is certain that both interest and nominal amount will be paid.

A rational investor would not lend money for less interest than what can be received risk less, hence this rate builds a floor for interest rates for loans of comparable term.

Is it possible to earn risk-less interest in Bitcoins? Yes, e.g. with products that implement the side memory pattern, that I described on the Bitcoin developer list. If someone pays you to lock your Bitcoins to a contract for a time period, then you earn risk less interest. Locking means you forgo the opportunity of spending them until a later time point. The income is risk less since you certainly regain control of the Bitcoins in the future.

What rate of risk less interest should an investor demand in Bitcoin?

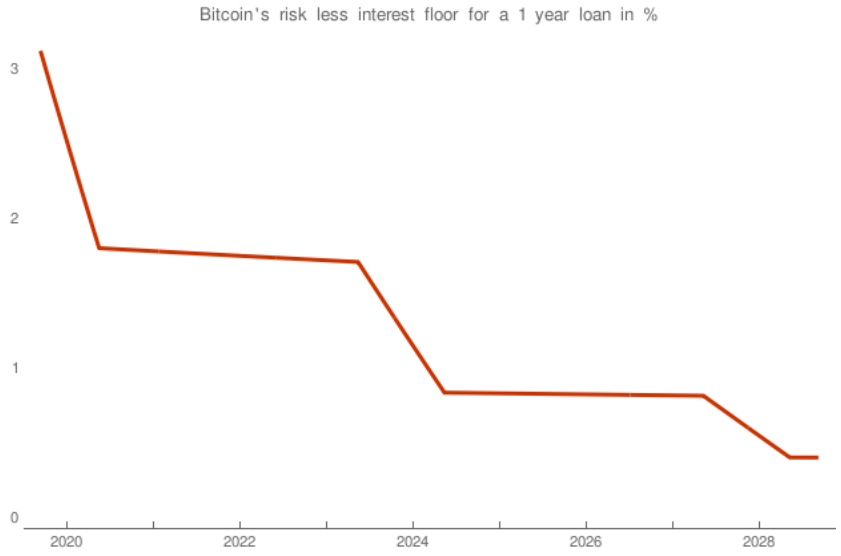
Interest generally is expected to compensate for diminishing purchasing power while you are not in control of the funds, if it would not, why doing it? Many take it for granted that Bitcoin's purchasing power will increase with time, and there is a good chance for that, but only a chance. Certain is that the number of Bitcoins in circulation is increasing. This means if everything else would stay the same then Bitcoin's purchasing power would diminish with the rate of the dilution through mining.

Dilution is not insignificant and is compute able thanks to Bitcoin's deterministic issue schedule. Miners currently earn 12.5 Bitcoins for a block and 6 blocks are expected to be produced in an hour. This means 1,800 Bitcoins are produced every day. These new Bitcoins dilute the value of those already in circulation, 17,929,350 at this moment.

This means a current dilution rate of 1,800/17,929,350 = 0.01004% per day that would be roughly 3.6% p.a. if we would ignore the halving, which we should not. See a precise calculation of forward rates below.

A rational investor should require at least a compensation for this dilution when negotiating an interest rate. Therefore the dilution rate acts as a floor to risk less interest.

Since dilution is deterministic, we may calculate the floor to forward risk less interest rates in the future. I did the work for you for the next ten years.

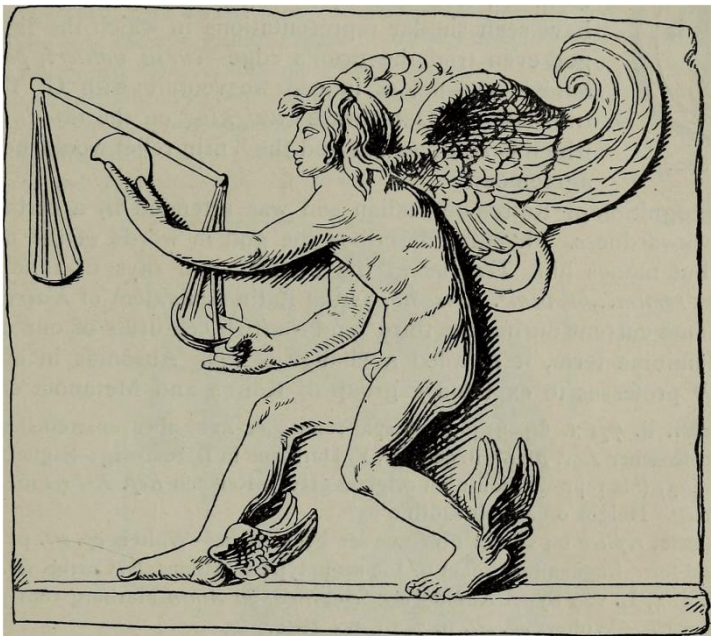


The Encrypted Meaning of Crypto

A very short etymology of the semantic hell that is 'crypto'

By Erik Cason

Posted September 11, 2019



Kairos — the personification of opportunity, luck and favorable moments. Also presented as a favorable opportunity opposing the fate of Man.

The term crypto has a complex and deep history that reaches much father back then the recent development of the science of cryptography. The written word itself goes back for at least two and a half millennia, though its existence has been much longer. Through the use and abuse of the word over this time, crypto has shrouded and concealed its meaning to all except for the most astute observers. Personally I am the most guilty of this robbery of language; having continued the legacy of bankrupting the term, widely referring to everything in the crypto-currencies ecosystem, asset, token, DeFi, DLT, etc. as simply 'crypto'. Why? Because I love that it further encrypts the meaning of the word itself, leaving it deeper in obscurity. This leaves the individual to wrestle with the question of what 'crypto' really means, and if they are to try to decipher it, or allow for its true name to remain hidden to them. Either way, in the words of Satoshi Nakamoto,

"If you don't believe me or don't get it, I don't have time to try to convince you, sorry."

However, I'll take a shot at trying to convince folks because I believe this technology is messianic, and all seekers should have an opportunity to discover the truth. To understand what crypto is, and to take it seriously; there must be a deep hermeneutical process that is undertaken to allow for a sincere engagement of what crypto-graphy means in order to allow for a new form of value-ability to come into view. The real ontological discover that lies hidden at the core of this technique of power goes beyond any law, and

allows for any person to use this power to protect them when nothing else can.

The origins of 'crypto'

Coming from the ancient greek word κρυπτός (krúptō), roughly meaning, 'I conceal', crypto in the last century has been generally understood as being a prefix for a concealed political motive such as a crypto-facist, or crypto-communist. However, it also is a prefix for 'of relating to cryptography', such as crypto-suite or crypto-currency. The linguistic obfuscation here is of particular interest to us, because it allows for a much more radical form of power to lay hidden at the center of 'crypto-assets' through its encrypted meaning. What is particular about bitcoin, and crypto-currencies in general, is that they have given rise to a new kind of political character: crypto-anarchists. Crypto-anarchists are not of the same linguistic character that 'crypto-facist' or 'cryptography'. Crypto in crypto-anarchy is referring to using cryptography as the base tool for organizing an anarchist (i.e. no laws) society. Crypto-anarchism is not attempting to the concealment of its objectives of creating anarchism; at least not initially. And to be clear, I'm not speaking of the childish 'destroy & enjoy' kind of false anarchism portrayed in the media, but that of the linage of Prodhorn, Bakuin, Goldman, Rocker, and so many others. Anarchism is the radical freedom of individuals through the decentralization and the diffusion of power through various non-state organizations. Through the total empowerment of individuals against the state, anarchism is the third way between communism and fascism that we must demand, and is our only hope for a future free against tyranny, despotism, and panopticism we live under today.

The concealment of crypto

Tim May knew of this linguistic pun when he coined the term crypto-anarchist, and had the following to say about it:

I devised the term crypto anarchy as a pun on crypto, meaning "hidden," on the use of "crypto" in combination with political views (as in Gore Vidal's famous charge to William F. Buckley: "You're crypto fascist!") and of course because the technology of crypto makes this form of anarchy possible. The first presentation of this term was in a 1988 "Manifesto," whimsically patterned after another famous Crypto Anarchy and Virtual Communities manifesto. Perhaps a more popularly understandable term, such as "cyber liberty," might have some advantages, but crypto anarchy has its own charm, I think.

Charming indeed. However, because of the semantic hell that is crypto (as in the crypto-currency ecosystem), the very meaning of what crypto-anarchy is has transmuted it into something not well-understood by most involved in the field of crypto-currencies. Over the last thirty years we have lost the key to this scripture which has created the nonsense vacancy of the term 'crypto' as we see it today. The metaphysical meaning of crypto has encrypted its meaning to shitcoiners, nocoiners and everyone in between for greedy, high-time preference bullshit tokens that are devoid of real value. Funny enough, these are the very people who are crypto-anarchist in the deepest sense of the word. They help propel this ecosystem deep into the heart of financial Troy, sincerely believing the gigantic horse of blockchain was a gift from the Gods. And it is. They just don't realize that crypto is a gift from the New Gods, not the old ones. They don't understand that this technology is uses cryptography *as a tactic* to organize people on anarchist lines, using cryptography to directly shield the bodies of any involved. They simply see 'blockchain' (a semantic hell in its own right) as another iteration of state power — of finding new laws, and 'better' regulation with more panoptic violations. They lack the fundamental understanding of why the explosive power of cryptography is at the heart of these systems. They lack the understand that cryptography's fundamental objective is to protect one from **ANY** advisory at any cost — including all law, militaries, and tax agencies. They fail to see that the fixed supply cap of bitcoin, the proof-of-work scheme, and pseudo-anonymity are not technical issues, but politcal ones. Adversarial thinking is inherently anarchist, and cryptography has always bared the signature of this at its heart. This is why cryptography has always been a military tactic first, as it has always existed outside of the bounds of law, and existed in only the field of war long before the word cryptography was even produced. It is important to remember that anarchism has always influenced and served the original ideas of those who would later become the cypherpunks. Chaum's 1985 paper Security Without Identity: Transaction Systems to Make Big Brother Obsolete points directly to this. It was one of the first papers that understood and connected governmental control of money with the security state, and how the technology of encryption could make big brother obsolete. Later in 1992, Tim May distilled these values into the 'Crypto-anarchist Manifesto', which opens with the following:

A specter is haunting the modern world, the specter of crypto anarchy. Computer technology is on the verge of providing the ability for individuals and groups to communicate and interact with each other in a totally anonymous manner. Two persons may exchange messages, conduct business, and negotiate electronic contracts without ever knowing the true name, or legal identity, of the other. Interactions over networks will be untraceable, via extensive rerouting of encrypted packets and tamper-proof boxes which implement cryptographic protocols with nearly perfect

assurance against any tampering. Reputations will be of central importance, far more important in dealings than even the credit ratings of today. These developments will alter completely the nature of government regulation, the ability to tax and control economic interactions, the ability to keep information secret, and will even alter the nature of trust and reputation.

Shortly after this was written, the first of the Crypto Wars started and the struggle to break cryptography out of its militarized cage was initiated. Through the valiant and heroic efforts of these great men (of whom, many are still contributing today), and their personal direct struggle against agents of the state, they managed to expropriated the greatest and most powerful technology of defensive asymmetrical warfare in the history of mankind from the military-industrial complex and let it out into the world to complete its messianic task.

The meaning of Crypto without the decryption key

Flash forward 30 years, now 'crypto' has completely broken out of its militarized cage, and there is no power on earth which can stop it. However, with the spectacular number of 'crypto' projects out there, so much noise has been created that the meaning of crypto itself has been lost, and has encrypted the actual meaning of crypto to itself. The apex of this kind of insanity has to be the Facebook's shitcoin Libera project. Those who are responsible for the most systematic violations of privacy that have ever been conceived or could even be imagined, now want to take those steps further; this under the idiotic guise of 'crypto' once again. This is of the greatest ironies because while society may now have all of the radical tools that May theorized about 30 years ago to liberate ourselves from the camps of the state, we have been made blind to the real power that we have access to because of the semantic abyss we have fallen into. Our lack of class consciousness and the historical context that has got us here, has every blockchain bro proudly patting each other on the back, chained to their blocks of oppression in the darkness of Plato's Cave. As I warned in The Poverty of Tokens, crypto-assets can become a panoptic nightmare of privacy violations when blockchains becomes mutable, pre-mined, non-anonymous. They no longer have any of the majesty, consanguinity, or consensuality of real crypto assets like bitcoin, nor could they ever offer such assurances. Bitcoin can offer these kinds of assurances because it is not asking one to stake proof on trusting the system. Bitcoin demands that everyone check the work and not to trust, but to verify. Satoshi took the hermeneutics of value in the digital age very seriously, and bitcoin is what was produced from that angst. If we are to reclaim the term crypto from its inane semantic dribble (which I am not convinced we should — I think it is better this way), then we must have a deep understanding of the etymology of the word crypto, and how it has been used historically. Crypto has always been about the form of

power which is now enshrined within the modren science of cryptography. It has always been about the capacity to conceal, and to hold secrets for oneself, and how such a secret generates power. Crypto is about the whole historical ark of the last 2,500 years in which this written term κρυπτός has been utilized as a tactic of self-protection *through* concealment. From steganography and the first shift ciphers of Cesar in ancient Rome, to the ciphers devised by Francis Bacon and Vigenère in the middle ages, to crypto's premier as a full science with Kerckhoffs's principle in *La Cryptographie Militaire;* crypto *has always been about power!* It is a form of power that is created through the concealment of information. It is only in the last century and a half that it has become an explicit material science lobotomized of its origins, purpose, and mysticism to serve only the state, and its great machines of death. Crypto is about the power of privacy, and the form of power that is decrypted when the concealment of information is verified and guaranteed beyond the law of any and all men. But so long as 'crypto' remains a vacuous slogan used by every piece of shit blockchain thought up, crypto will continue to be a nascent term concealing its true meaning and its messianic potential.

Tweetstorm: How do you know it's not too late to buy Bitcoin now?

By Hasu

Posted September 12, 2019

A common question that precoiners have is, "How do you know it's not too late to buy bitcoin now?"

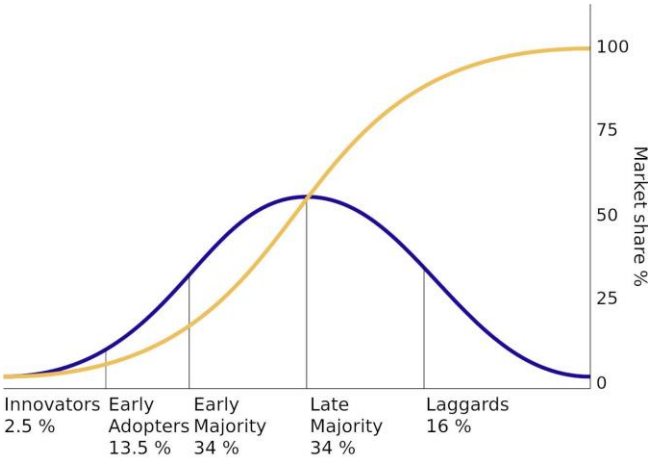
They still assume Bitcoin follows the value/adoption curve of a pyramid scheme - a system that needs to sustain itself with new buyers and collapses if those ever run out.

The question seems reasonable: Once Bitcoin is widely adopted, the future value from speculation will indeed be zero. But that ignores half the picture - where has that speculative value gone? And does it mean that earlier buyer now have an incentive to sell?

The EV of a pyramid scheme decreases the later we are in the adoption cycle. But the EV of a network good like money increases, as it becomes more useful the more people own it.

What was seen as speculative value during the earlier adoption stages was merely the discounted use-value of later stages. In the beginning, Bitcoin had no use-value. In the end, Bitcoin has only use-value.

Because Bitcoin becomes more useful the later in the adoption cycle we are, there is never a point where the marginal buyer can lose from adopting it. Only the value for the marginal buyer will come less from people finding it useful later than from himself finding it useful now.



To wrap around to the initial question, a potential investor should ask himself whether a mature Bitcoin system is genuinely useful to him and others.

If the answer to that is positive, there's no reason to expect the system to unwind as more people join.

Bitcoin Astronomy

By Dhruv Bansal

Posted September 13, 2019

The desire to travel far away and start a new currency will become a powerful driver of human expansion into space.

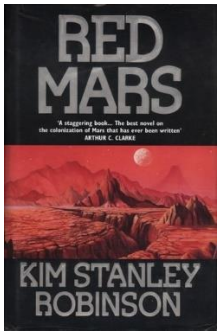
Earth will run on bitcoin, but colonies on Mars, the outer planets, and distant stars will not. Though faraway colonies will value and trade bitcoin, they will choose to launch, defend and use their own local blockchains. This pattern of replication is an inevitable consequence of hyperbitcoinization and the physical limitations inherent to any blockchain that respects the finite speed of light.

Speculating about the future is always indulgent and never a science, but speculation about tomorrow helps us better understand today. There is a fascinating and rich history of speculation about bitcoin astronomy that we extend and explore in this series. Our aim is to present blockchains and the social, political, & economic structures they produce, as fundamental forces in the universe, on par with evolution, the production of entropy, and the passage of time.

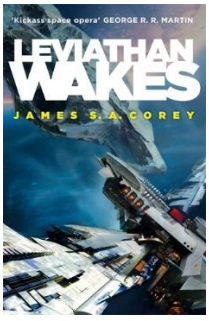
This article focuses on Mars, the Red Planet, and speculates about the economic revolution we foresee occurring there. What happens on Mars will eventually be replicated across the solar system and beyond. But we begin with Earth, in the not-too-distant future, in a post-hyperbitcoinization era.

Hyperbitcoinization on Earth

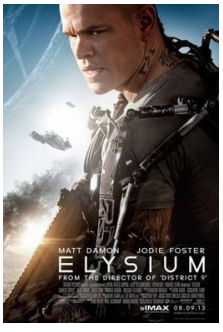
What does a hyperbitcoinized future Earth settling nearby planets look like? It's probably a mix of works such as these, but with more bitcoin:



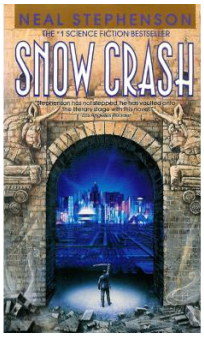
Settlement, terraforming, and revolution on Mars



Conflict between Earth, Mars, and minor powers of Sol.



Rich people will definitely move to space.



A world without nations but a powerful belief in digital reality.

Imagine it: 100 years from now, bitcoin is a global currency used by all people. Individuals mostly transact on one of several second layer lightning networks. Large transactions still occur on the chain, though usually through aggregation mechanisms. Third and fourth layers also exist: the Internet becomes a bootstrapped mesh network with nodes settling on the lightning network as they store data and push bandwidth. Many powerful global corporations are replaced by inter-operating protocols, all distributed and market-driven, settling to BTC. In a hyperbitcoinized world, bitcoin is not just the foundation of the world economy; it's the unit of account for new distributed infrastructures of computing, telecommunications, identity, etc.

Hyperbitcoinization is not limited to affecting financial, computer, and social networks. Many other industries will change both in relation to, and independently from, this trend. 20% of world energy production will go to SHA256 hashing because the industries of bitcoin mining and power generation will have merged. The environment is significantly degraded in the future, but it's not because of bitcoin. Bitcoin mining in 2019 is already utilizing greener energy sources than other industries, and the continued rapaciousness of bitcoin miners for energy will turn out to be the reason fusion power is successfully commercialized, a delicious irony.

In parallel with technological and cultural change will be political revolution. Climate, refugee, and other crises combined with new politics born from new distributed technologies will have transformed the squabbling cathedrals of today's nations and corporations into a chaotic global bazaar of local polities and loose-knit federations. Empires may still exist, in places, but this is an age of city states.

Humanity started reaching out into space in the 20th century and is doing so again in the 21st. If Elon Musk is successful, we will begin to colonize Mars in the next 20 years. Fast-forward another century: how large could Musk's Mars colony be?

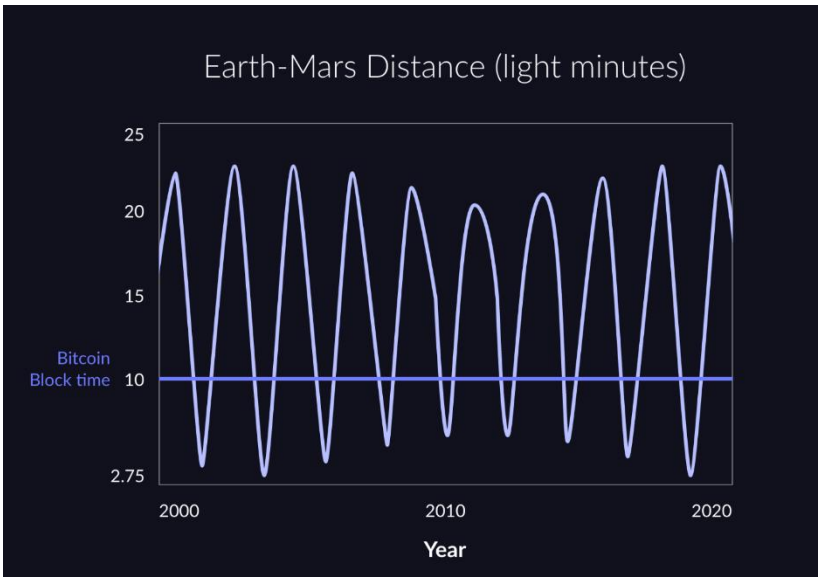
A century is a very long time, enough to master fusion and deploy macroengineering marvels such as space elevators (and not by nation-states, but by distributed, public corporations chartered through bitcoin). These advances will enable waves of settlers to flee environmental degradation on Earth in search of a better life on Mars. The population of Mars sometime in the 22nd century could easily number in the tens or hundreds of millions.

Will these Martian millions be using bitcoin?

Bitcoin on Mars

Mars will be the first large human colony sufficiently far away for significant light-lag to occur in communications with Earth. This lag will begin as a

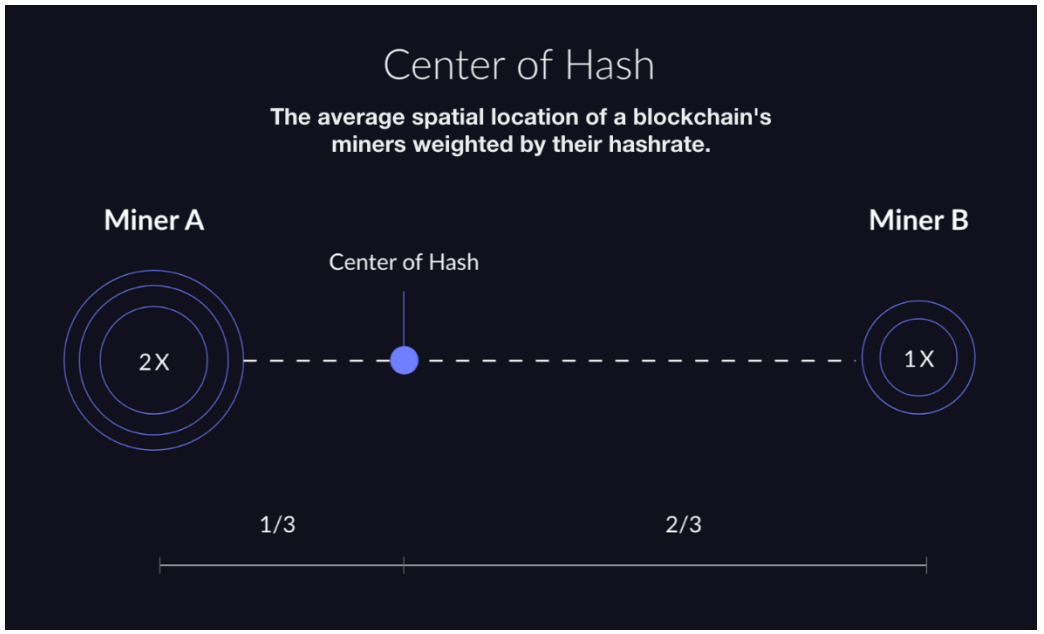
challenge for explorers, grow into an inconvenience for colonists, and, finally, become a membrane separating two cultures.



Mars is between 3 & 22 light-minutes away (12.5 light-minutes on average), meaning a round-trip signal time of between 6 and 44 minutes (25 minutes on average). The bitcoin block time is only 10 minutes. (Source)

Communication between Earth and Mars will certainly still be possible, though networking primitives will be very different than those of today's Internet (or even the Internet of the then-Earth). A laser-powered, market-driven telecommunications network of relayers and amplifiers will crisscross the inner solar system, trading bandwidth over time and distance for BTC. But there will still be challenges caused by the unavoidable delay inherent to all Earth-Mars communication. Bitcoin users and miners in particular will be affected because of their great distance from Earth and its *center of hash*:

Imagine two miners A & B separated a distance apart. Miner A has twice the hashrate of miner B. Their center of hash will be located at a point in space 1/3 of the distance between them, closer to miner A. A similar calculation can obtain the center of hash for many miners at various hashrates distributed over a large volume of space. Compare to center of mass.



Bitcoin's center of hash today is somewhere near the center of the

Earth, perhaps a bit closer to China. This may change as humanity expands and bitcoin miners set up in orbit or on Luna. But bitcoin's center of hash is likely to always remain within a few light-seconds distance of the center of the Earth. This will have deep consequences for the future expansion of human civilization.

Screenshot of a Bloomberg terminal in 2130. Bitcoin's center of hash is near the Earth's center, slightly shifted towards the location of Moon which hosts 15% of all bitcoin miners. (Source)

Martians will be able to use bitcoin

A Mariner Valley feed store, circa 2130. All prices are in $atoshis per kilogram. The economy of Mars will initially run on bitcoin. Martians can hold and transact in bitcoin as well as on the higher layer lightning networks.

Martians will be able to use bitcoin, lightning networks, and higher layers of the bitcoin ecosystem, but Martians will suffer various small disadvantages compared to Terrans because of their distance from bitcoin's center of hash.

Firstly, hodling is using: anyone can use bitcoin just by owning some BTC. The first hodler to step on Mars will bring bitcoin to that rusty world. In this way, even though bitcoin's center of hash is bound to Earth, its reach encompasses the universe.

But Martians can do more than silently hodl. They can run full nodes to help sustain local copies of the blockchain on Mars. They can also transact in bitcoin with each other or with Terrans simply by transmitting signed bitcoin transactions, though they'll have to wait up to 22 additional minutes for their signals to arrive at the center of hash on Earth.

Most transactions in this era aren't occurring on the blockchain, but on lightning networks. Martians will be able to use lightning networks, but as Clark Moody points out, they have to take particular care to guard against fraud because of their distance from the center of hash. One tactic might be to choose long lock times for the channels they create and use to route. This may sound like a lot of work, but in a hyperbitcoinized future, the lightning network is old technology; software will handle this constraint behind the scenes.

As Mars grows, so will its lightning network, its third and fourth layers, and their connections to Earth. Martian lightning nodes will earn fees from routing transactions, and Martian disk and server farms will locally cache all the best content from meshflix and apps from the dapp store for Martian use. Yes, there will be constant inefficiency due to Mars' distance from the center

of hash, but for the most part, Martians users will feel as well-integrated into bitcoin and its higher layers as Terrans do.

What about Martian miners?

Bitcoin mining will not be possible on Mars

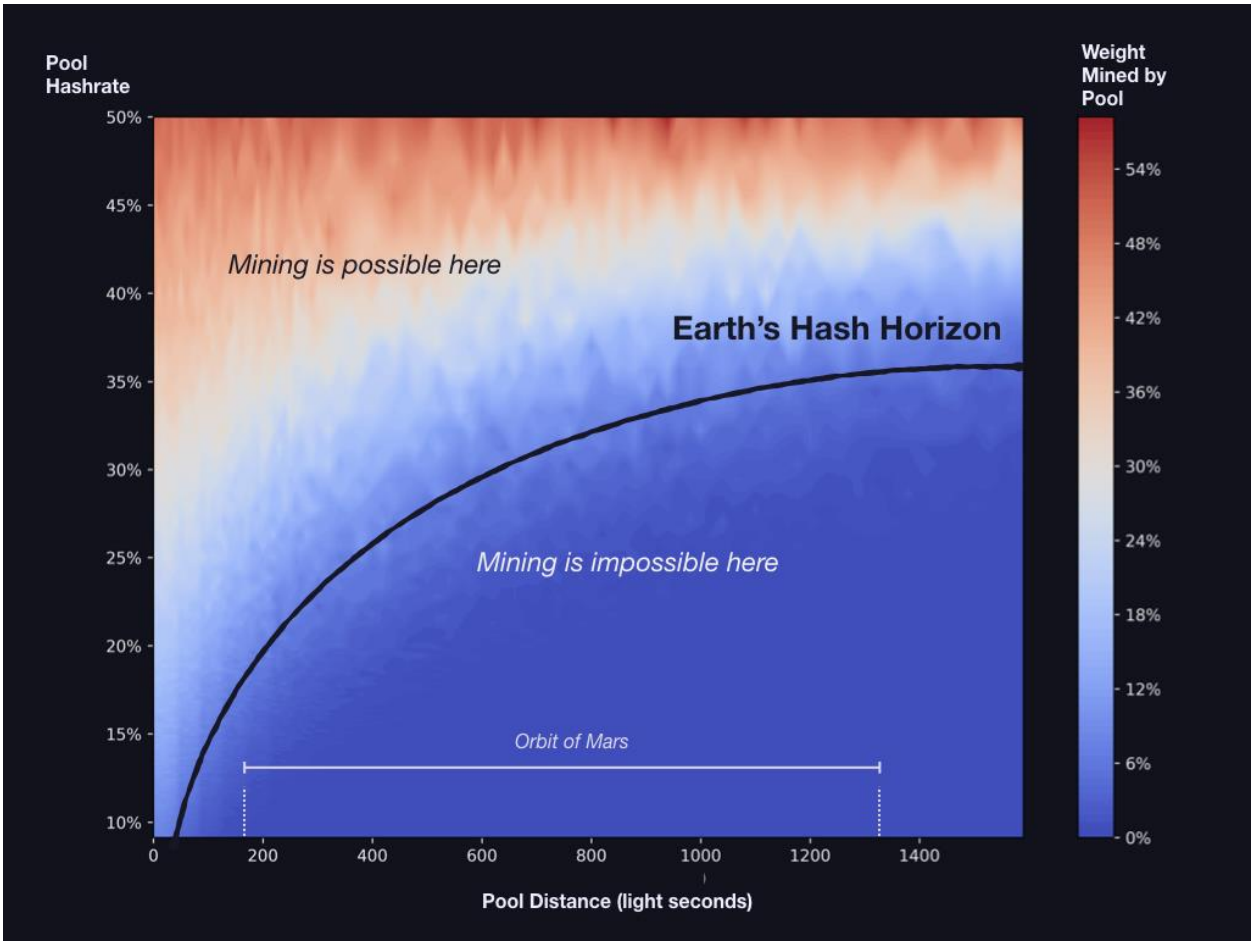
It will not be possible to mine bitcoin on Mars. The issue is too little hashrate at too far a distance:

Mining Bitcoin on Mars would be unprofitable because of the propagation delay, assuming Earth maintains hash power dominance. The Martian miners would have a view of the blockchain up to 22 minutes out of date, so by the time their latest mined block reaches the majority of hash power on Earth, on average there would be four new blocks added to the chain. — Clark Moody, Bitcoin and the Interplanetary Frontier

The bitcoin network is something like a clock (more on this in Part 3), and it relies on all of its nodes being "in sync" by sharing the same set of blocks and pending transactions. Great distance between miners results in great communication times, difficulty syncing, and the impossibility of mining. A less exotic illustration of this syncing problem exists today and provides an analogy for long communication times in space: If a miner has a poor connection and very limited bandwidth (or blocks are very much larger) then it can take significantly longer for that miner to see the same blocks and transactions as other miners in the network.

Let's consider an example: A pool of bitcoin miners with, say, 10% of hashrate is located on Earth, near the center of hash. This pool will mine its corresponding fraction of hashrate in blocks: 10% of all blocks. If the pool moves into space very far away, and its distance to the center of hash increases, the pool will find itself winning less than 10% of blocks because of syncing problems caused by communication delays. The further away from the center of hash the pool travels, the lower their fraction of winning blocks. At some distance — some *horizon* — the pool will no longer win any blocks at all, despite still representing 10% of the hashrate.

We wanted to be more quantitative about the relationships between a miner's distance from the center of hash, their relative hashrate, the delays they experience in communication, and the resulting weight of blocks they can mine, so we wrote a program called hashwars to simulate these sorts of scenarios. You can find it on GitHub and use it to produce plots such as this one:



A plot of the relative success of a minority pool of miners at different distances from the center of hash and different relative hashrates compared to the majority. The color plotted shows the fraction (by weight) of blocks mined by a pool at the corresponding distance and relative hashrate. Each point represents the average of many simulations of a bitcoin-like blockchain with a block time of 10 minutes.

This plot shows that as a pool of bitcoin miners retreats from the center of hash at Earth, the effectiveness of their hashrate at winning blocks diminishes greatly. Distance protects bitcoin miners on Earth from hashrate that is too far away. This leads us to formulate the following law:

First Law of Bitcoin Astronomy (or "The Law of Hash Horizons"): Given constant hashrate, as a miner moves away from the center of hash of a blockchain, the number of blocks won by that miner statistically trends towards zero.

Vitalik Buterin has written about the Defender's Advantage conferred by cryptography. The existence of hash horizons confers a similar Hometown Advantage for bitcoin miners. Bitcoin's block time of 10 minutes was presumably chosen by Satoshi as a compromise between minimizing 1st-

confirmation time and chain splits. In making this choice, Satoshi also set the scale of Earth's hash horizon.

In particular, Mars is outside the hash horizon of Earth. Martians cannot compete in protecting the money they use. This situation is not unique to Mars. Prospective bitcoin miners at any great distance from Earth would be similarly suppressed (and this would have been differently true for other choices of the block time as well). Indeed, in the article above, Clark concludes: *Extreme luck aside, the dominant mining planet will remain dominant across the solar system.*

The Muskcoin Revolution of 2140

In our view, Clark is partially right. Earth will remain the dominant *bitcoin* mining planet. But one day Martians will stage a revolution in support of their own token: **Muskcoin**. If they succeed, then Mars will become the dominant Muskcoin mining planet. The Muskcoin Revolution of 2140 will become a template for other colonies of Earth to follow, just like the American Revolution of 1776 was in its age.

Why Martians will want Muskcoin

Transaction without settlement is tyranny. — Martian revolutionary slogan, 2138

Why would Martians, happily using bitcoin and all its layers, desire to launch their own token? And why would anyone, Martian or Terran, even value such a thing?

In a hyperbitcoinized world, bitcoin has outcompeted all other fiat and cryptocurrencies. Bitcoin is both sound money and substrate for the entire economy. To people of the future, new tokens will seem like foolish scams as no token could have features not already provided by the bitcoin ecosystem, and no token could amass sufficient hashrate to defend against even casual attacks by small bitcoin miners/pools. For people of the future, words like *altcoin* or *staking* will sound as silly as *nephrology* and *laserdisc* do to us today.

The cynical explanations, preferred by future Terrans and Tories on Mars, will be greed and stupidity. If Muskcoin copied bitcoin, and it succeeded, its early adopters would be rewarded the way early bitcoin miners were rewarded back on Earth in the (now mythical) early years of the 21st century. But Muskcoin supporters will dodge these criticisms and argue that Muskcoin is **necessary**. Many revolutionaries of this era are second and third generation Martians who have never been to Earth, whose frail bodies could never withstand the harsh pull of Earth's gravity well. They feel they are their own

people, yet Terran control over which bitcoin transactions can settle means they are part of the dominion of bitcoin and, therefore, Earth. Their desire for Muskcoin is the universal desire of all people for self-determination.

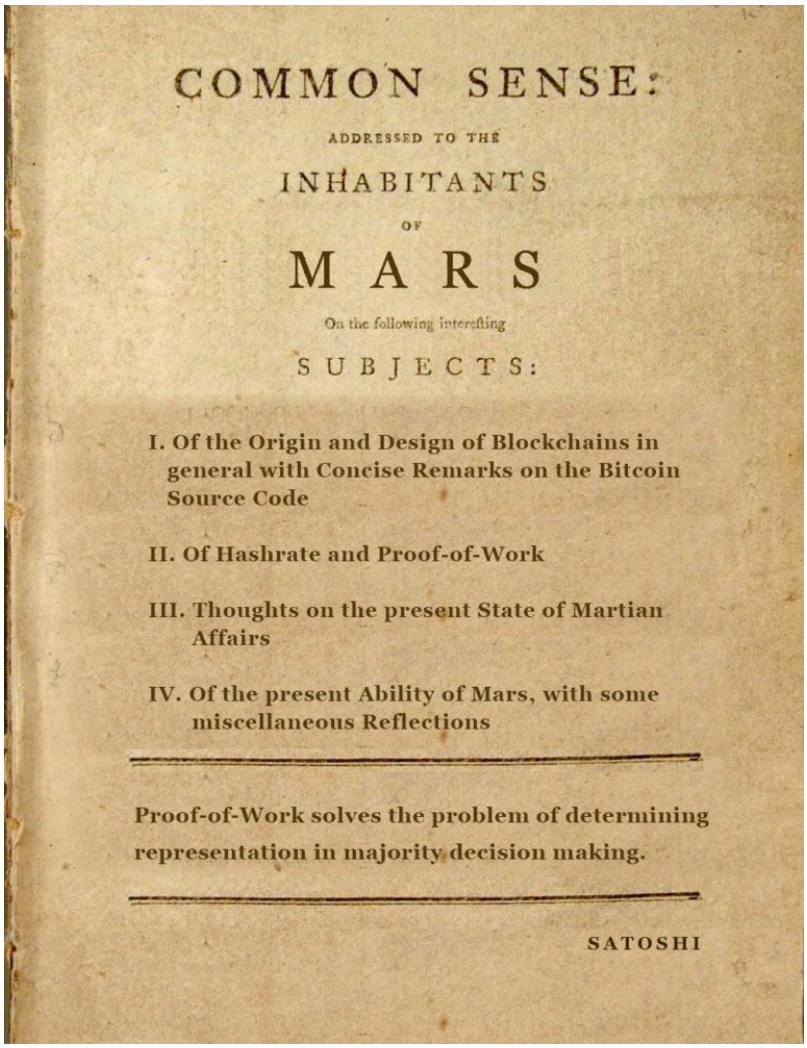
Muskcoin will be modeled on bitcoin and will have many of the same properties. If bitcoin became sound money on Earth, then Muskcoin may become sound money on Mars, and for similar reasons: an intolerant minority of Martians who desire an independent Mars will support its growth.

Muskcoin also has one distinguishing feature not present in bitcoin or in any of its historical altcoins, justifying Martians' support: Muskcoin will have *a center of hash located on Mars*.

A center of hash on Mars would allow Martians to develop a Muskcoin mining industry with all its positive effects. In a hyperbitcoinized world, being able to mine on a local blockchain may be a killer feature. As in, a feature worth literally dying for. A feature worth fighting a revolution over.

What will be the revolutionaries' arguments? Imagine some Martian Thomas Paine's future version of *Common Sense*:

- **Settlement:** Mars is a self-sufficient world full of cashflows generated by our industrious people. Martians run all the shops, factories, and services we rely on ourselves. And Martian reality VR is the most popular content streamed back on Earth! Yes, we manage to keep a few scraps of routing fees, but all the settlement fees from our labors accumulate back in the already full coffers of greedy Terran miners. Keep Martian settlement fees for Martians!
- **Energy:** Terrans claim Mars is well-supplied through



COMMON SENSE:

ADDRESSED TO THE

INHABITANTS

OF

MARS

On the following interesting

SUBJECTS:

I. Of the Origin and Design of Blockchains in general with Concise Remarks on the Bitcoin Source Code

II. Of Hashrate and Proof-of-Work

III. Thoughts on the present State of Martian Affairs

IV. Of the present Ability of Mars, with some miscellaneous Reflections

Proof-of-Work solves the problem of determining representation in majority decision making.

SATOSHI

existing trade channels yet we have all seen the lights flicker under the Great Dome of Elon during power crunches. Our heavy metals mining industry is anemic,1` and we are unable to build the power capacity we need. The positive feedback loop between mining and energy production and investment that has been showering Earth with prosperity since the early 21st century must be started here on Mars!

- **Fairness:** All our settlement transactions must be transmitted through a small number of high-powered comms lasers all of which are owned by perfidious Terran corporations. Native Martian transactions always seem to be enqueued for broadcast behind those of Terrans.
- **Censorship:** Censoring transactions delays our commerce and endangers our republic. How long before Martian leadership's transactions are not broadcast at all? By willingly using bitcoin we tie a Terran yoke around our own necks. Are we just serfs in some fiefdom of Earth? Or are we the Children of Mars!?

The narrative of Muskcoin revolutionaries will be part political identity and economic liberation. Intertwined with these themes is the seductive opportunity for those who support the revolution to become a population of "First Miners", those who win a significant fraction of Muskcoin, the future currency of the Red Planet.

There will be many attempts at Muskcoin

Like any revolution, Muskcoin's will be chaotic. It may start in fits and bursts and fizzle out again, as Muskcoin efforts fail and are abandoned and renewed again. But eventually some critical mass of supporters and infrastructure will be present and, in a short time, a gaggle of competing Muskcoin contenders will launch, each promoted by various factions on Mars and on Earth with their own interests, all vying for the title of Muskcoin. It will be an age of speculation and charlatanism not seen since the ICO boom of 2017.

Balkanization of Muskcoin into many competing chains will be in the interests of Terran bitcoin maximalists, and some may encourage it. Could Mars unite around some single version of Muskcoin? The fairness of bitcoin's launch (its immaculate conception) contributed greatly to its success on Earth. Will any Muskcoin be able to replicate these feats on Mars? It's possible that Satoshi's disappearance is a one-time trick. But maybe, in this distributed future, successful, open-source anonymous projects with unknown creators are commonplace. There may be established platforms and methodologies for fair launches of all kinds of distributed services with economic incentives to reach stable Schelling points. Operationalized game theory for adversarial systems.

Most Terrans will be indifferent to Muskcoin

Say some Muskcoin contender does emerge from the fray and starts making news on Earth. What would be the reaction of Terrans to Muskcoin? Bitcoin is not government or corporate money; it is money from voluntary consensus forged by users. Muskcoin is, therefore, not a revolution against a government or corporation, but against a voluntary consensus. It is a new political and economic choice, a new Schelling point, in a higher orbit around the Sun.

The future analogues of governments and corporations may have vested interests in bitcoin's continued use, success, and stability, but the rise of Muskcoin on Mars won't threaten bitcoin on Earth. Bitcoin will continue to be used by Terrans and Martians alike, even those who support Muskcoin.

As a result, most Terrans will just not care about Muskcoin. They will happily mine and use bitcoin, dismissing reports of a growing Muskcoin user base and hashrate as idle chatter about some duster scam. Some will acquire it as a joke or just to say they have some. As Muskcoin appreciates (relative to bitcoin), it will probably do so in waves, shocking most Terrans. Some will become radicalized against Muskcoin and deliver screeds against it, claiming it has no value or isn't based on anything or doesn't work as well as bitcoin or is only used by criminals.

But some Terrans will be Muskcoin enthusiasts. They will recognize the advantages brought to Earth by bitcoin and feel it's only fair that Muskcoin do the same for Martians. These sympathizers may view a risky new Muskcoin as having potentially outsized returns compared to a mature and stable bitcoin ecosystem with predictable, low yields. Some may invest in Muskcoin, driving its price up relative to bitcoin, or even begin mining it themselves through subsidiaries on Mars.

Finally, some Terrans will be adversely affected by Muskcoin and willing to oppose it. Miners and others close to the energy production & settlement layers of Earth's bitcoin infrastructure may wish to preserve their transaction fees and control over Martian infrastructure. Some power blocs on Earth may not want Mars to gain further political autonomy. These actors will try and attack Muskcoin.

The Empire Will Strike Back

Could the rise of Muskcoin lead to a shooting war between political blocs on Earth and Mars? Some argue that a bitcoin standard would be a disincentive to large-scale conflict because states would have to resort to direct taxation to pay for their war machines. But history has demonstrated that destructive technologies become cheaper and easier to wield over time. Humans of the future may be just as tribal and easy to incite to stupidity and violence as

those of today. A century from now, nuclear technology will be commonplace and some burly faction on Earth could launch a few H-bombs at Mars and obliterate the entirety of its young civilization. This would be effective, but immoral and unwise. Destroying Martian infrastructure would do more collateral damage to the closely linked economy of Earth than the success of Muskcoin ever could have. This is a counter-productive response to the economic threat posed by Muskcoin.

Strong cryptography prevents anyone from stealing Muskcoin, but coordinated factions of Terran bitcoin miners antagonistic towards Muskcoin may have vastly more pooled hashrate than Muskcoin supporters on Mars. This makes it possible for them to launch 51% attacks and attempt to create double-spends on the Muskcoin blockchain. Such an attack might be the analogue of a special forces op against a rogue nation. A precise demonstration of power designed to serve as both temporary setback and warning.

The people of Mars may not be swayed by such displays. Disproportionate, violent responses from empires tend to legitimize the claims of revolutionaries and strengthen their zeal. In this case, antagonistic factions on Earth may have to resort to the ultimate weapon of hash war, the cryptographic analogue of a traditional H-bomb: the **hash bomb**. A hash bomb is a sequence of empty blocks of tremendous weight mined directly on the genesis block of some blockchain to be destroyed. When a hash bomb arrives at the target blockchain's center of hash, it immediately triggers a reorg, orphaning all locally mined blocks, and creating a huge upward difficulty adjustment. A hydrogen bomb can reduce a city to its foundations, and fallout makes rebuilding difficult. A hash bomb eradicates the target blockchain's history, replacing it with a nullscape of empty blocks. The attackers own all the coins and the defenders' hashrate can only produce a trickle of new blocks at the greatly increased difficulty. Complete and utter economic ruination.

Defenders can't ignore a hash bomb as its blocks are valid (you may argue that block timestamps would be horribly out of date coming from Earth, but block timestamps are user-defined — Terran miners can always fake them). Defenders could always start a new blockchain but attackers, especially if they have vastly greater hashrate, can just send another hash bomb as soon as they receive the new blockchain's genesis block.

The Art of Hash War

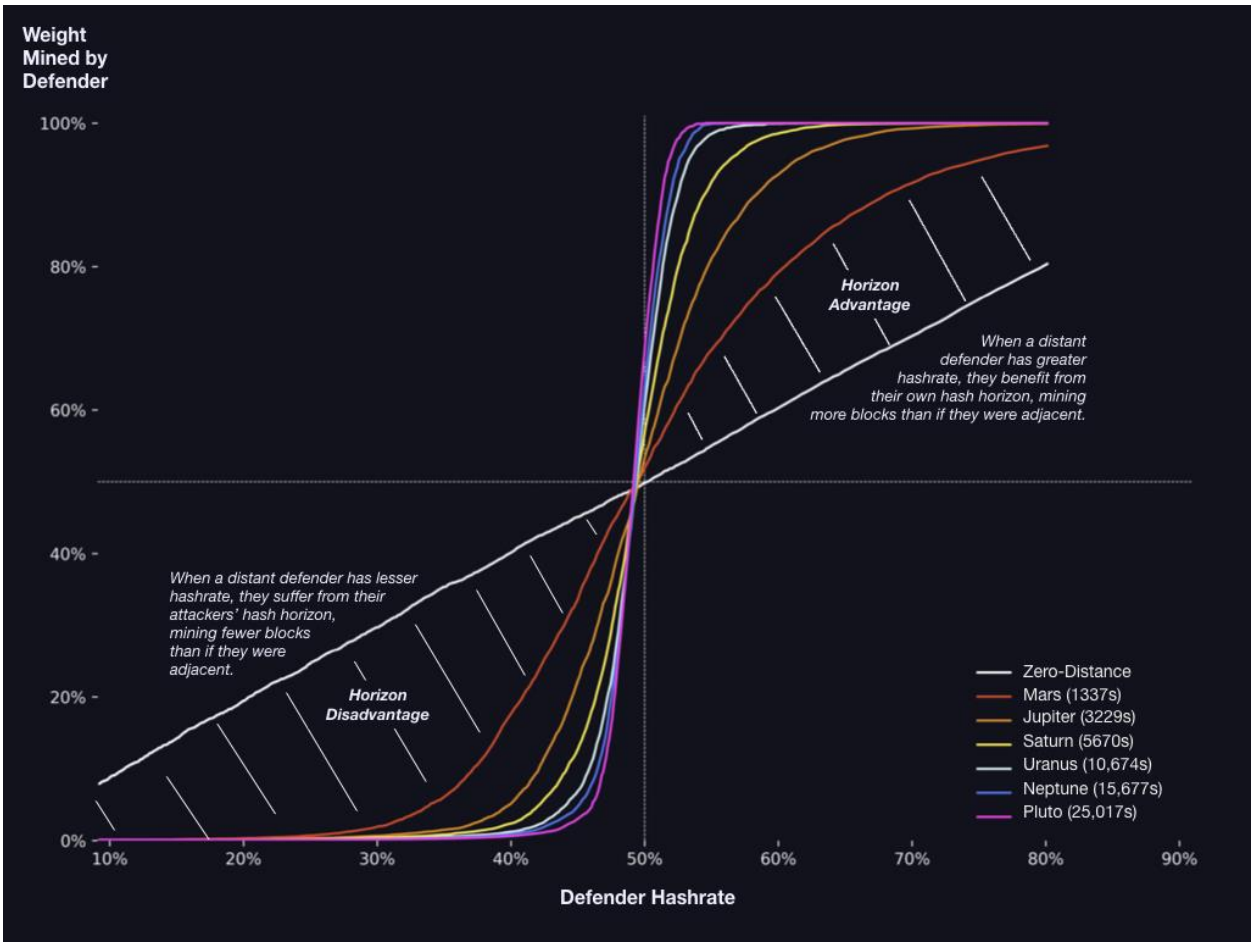
The art of war teaches us to rely not on the likelihood of the enemy's not coming, but on our own readiness to receive him; not on the chance of his

not attacking, but rather on the fact that we have made our position unassailable. — Sun Tzu

Martian revolutionaries have two significant advantages that they will seek to maximize before they engage in hash war:

- *The First Law of Bitcoin Astronomy* cuts both ways. As Earth's hash horizon prevented Martian miners from mining bitcoin, Mars' own hash horizon is a bulwark against attacks from Terran miners.
- In the future, the bitcoin mining industry is extremely efficient. Most Terran miners will prefer to mine bitcoin and earn settlement fees in bitcoin rather than use their hashrate to attack Muskcoin. Only some fraction of Terran miners will feel sufficiently antagonistic towards Muskcoin to spend hashrate attacking it.

This suggests that the timing of the Muskcoin launch is extremely important. Launch too early, and small pools of antagonistic Terran miners will be able to hash bomb Muskcoin just for the lulz. Long before actually launching Muskcoin, smart Martian revolutionaries will perform simulations to determine whether or not they have sufficient relative hashrate against their Terran adversaries to support a Muskcoin launch. They will produce analyses like the one below (produced with the hashwars program):



The plot shows the fraction (by block weight) of a new blockchain mined (y-axis) by a defender at a given distance (each line) from an attacker as a function of the relative hashrate between attacker and defender (x-axis). Deviation of the plotted lines from the white line (representing zero distance) shows the (dis)advantage conferred by the hash horizon at that distance.

This plot shows the defensibility of a new blockchain given various distances between that blockchain's defenders and attackers as well as their relative hashrate. At zero distance (the white line) and with 50% relative hashrate, the defenders should win exactly 50% of the blocks by weight (this is the dead center of the plot). Following the white, zero-distance line to the left, as the relative hashrate of defenders decreases, they mine fewer blocks. Following this white line to the right, as their relative hashrate increases, they mine more blocks. At zero-distance, the relationship between hashrate and block weight mined is linear, as expected.

But now look at the red-orange curve for Mars' distance. At 50% relative hashrate, this curve predicts Martians should mine slightly more than 50% of all blocks. This makes sense because this simulation assumes the blockchain starts at the location of the defender, giving them a small initial advantage.

Even though attacker/defender hashrate is evenly split, the Martian's hash horizon maintains this initial advantage.

Following the red-orange curve for Mars' distance to the left, when Martian' defenders have less relative hashrate than attackers, the curve drops **faster** than the white, zero-distance line. This is a direct consequence of the Law of Hash Horizons — being in the minority at a distance confers a mining disadvantage. Conversely, following the red-orange Mars curve to the right, it rises **faster** than the white, zero-distance line. This is the Law of Hash Horizons again, but this time the disadvantage is the attackers' because they have the smaller hashrate. This effect is even more dramatic for the outer planets at greater distances. The further a new blockchain launches from its potential attackers, the less relative hashrate is needed to defend it.

Martians will perform more realistic simulations than those presented here. They will try to plot their own hashrate curve, predicting their chances for success given their hashrate estimates. But are there any other techniques which can adjust the odds in their favor?

Advanced Blockchain Defense Strategies

There are also other techniques Martians can use to boost their resistance against Terran hashrate that require Muskcoin to make some changes to bitcoin's consensus rules:

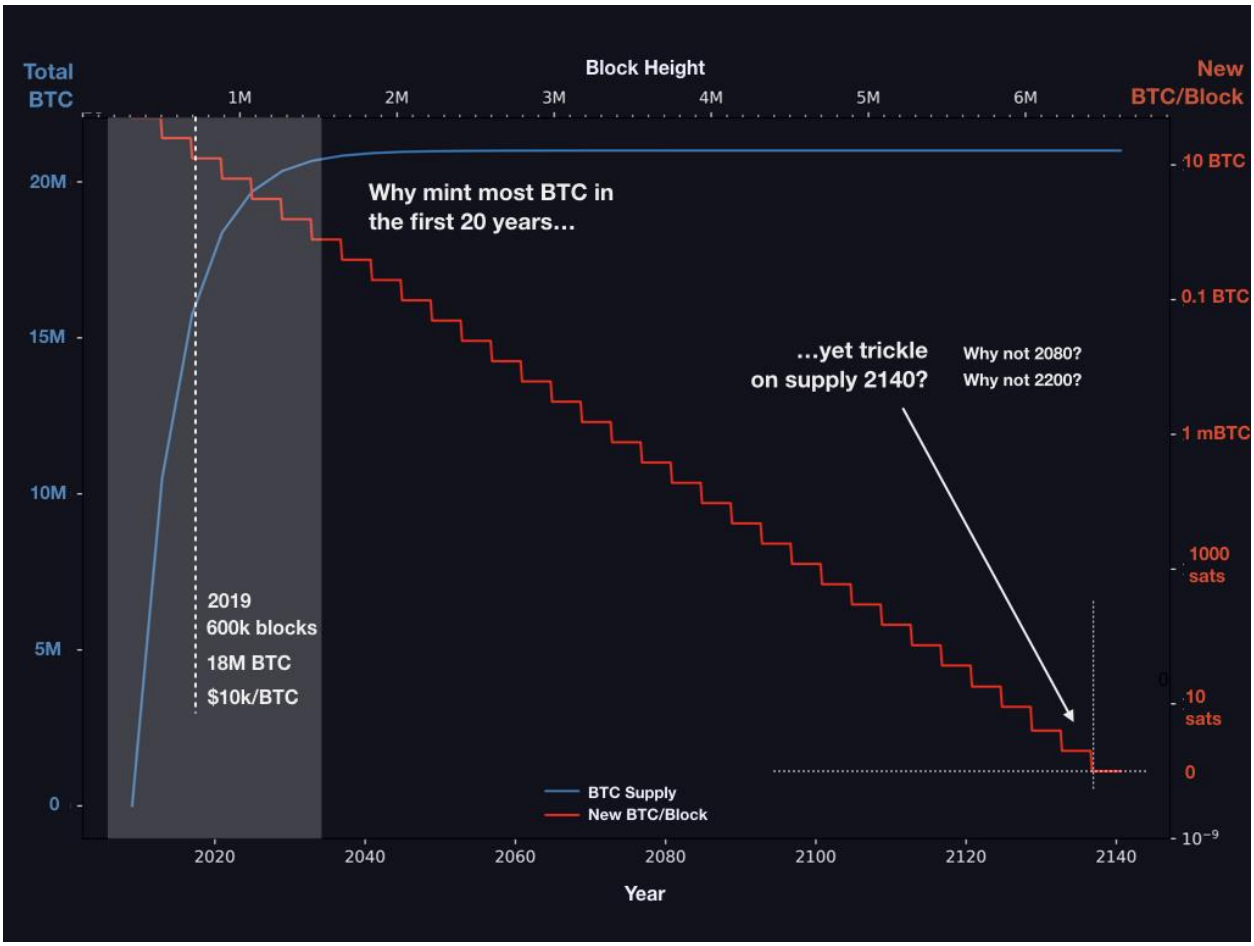
- Muskcoin could adopt a different hashing algorithm than bitcoin. Whether this would provide much defense against Terran adversaries depends upon how easily hashrate can be reconfigured or produced in the future. Computing technology could potentially be faster AND more flexible in the future, making specificity/performance trade-offs such as those made by current generation ASICs less relevant: There may be less design space to "get ahead of the current generation of bitcoin miners." It's also possible that manufacturing in the future is extremely fast & automated, and that once an ASIC design is known, it's easy to mass produce in 3d-printing industrial fabricators.
- Muskcoin could merge mine with bitcoin, inserting bitcoin block headers into muskcoin blocks and having muskcoin clients also be bitcoin clients. The weight of a muskcoin block could be defined as including the weight of the bitcoin blocks behind it. This lets Muskcoin piggyback from bitcoin's existing hashrate and security at the cost of being integrated with it.
- Perhaps in combination with the above strategy, Muskcoin could prohibit long reorgs, dramatically increasing resistance to distance hashrate.

- If a robust, trustless proof-of-location algorithm can be created, it's possible that new blockchains seeking to resist distance hashrate might demand proof of proximity to a certain location (the core of Mars) before accepting candidate blocks from miners.

In our early era, it's hard to know what the impacts of the proposals above would be on the consensus behavior and viability of Muskcoin. But in the future, blockchain engineering will be much better understood, a science rather than a dark art. Martians may have other consensus-based defenses which we cannot fathom today.

When Phobos?

When the time is right, Martians will have tools and strategies to help them launch and defend Muskcoin. But when will this be? How long exactly before Muskcoin goes to the Moons? The answer to that question may be also be the answer to another: why is bitcoin's issuance schedule so long and drawn out?



Bitcoin's supply is mostly produced in its first 20 years. Yet new BTC will

continue to be mined (at an ever-diminishing rate) for another 120 years, till 2140. Why did Satoshi pick this timeframe and not, say, 2080 or 2200?

It makes sense that most BTC are minted in the first 20 years of bitcoin's history — early adopters need to be incentivized to evangelize and build on the network. But why continue to trickle out tiny amounts of BTC per block for another 120 years? Why not 60, or 240? What if Satoshi was trying to estimate something...

Martian Satoshi Conjecture: What if Satoshi designed bitcoin's block reward schedule to continue minting BTC until the year 2140 when sufficient hashrate is developed on Mars to launch a new blockchain?

Even if this conjecture is false, at some date in the future, the Muskcoin Revolution will succeed. Bitcoin will continue to dominate trade near Earth, but Muskcoin will be used near Mars. Trade between the worlds will rely on cross-chain atomic swaps. The BTC/Muskcoin price, once volatile, will settle to reflect humanity's collective views on the future of the two civilizations, much as fiat currencies do today but without the ability to manipulate supply.

Bitcoin beyond Mars

Near Sol

The cynicism of Terran nocoiners during the Muskcoin Revolution will be understood as a reasonable stance to have taken given the total hegemony of bitcoin in their lives. After the revolution, everyone will understand that successful human colonies near locations with abundant natural resources that are able to attract settlers and build industry will launch their own blockchains once they have sufficient political will and hashrate. Indeed, becoming a peer in the Solchain network will become the definition of what it means to be a successful colony.

Future econobiologists will see the Muskcoin Revolution as not exceptional but natural. An expanding civilization, limited by light lag, must necessarily become more distributed.

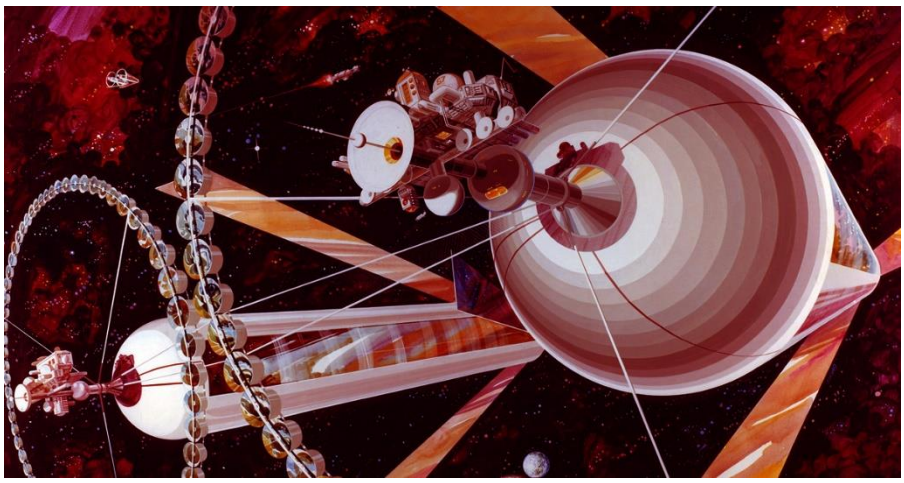
A blockchain makes a strong body for an economy, but it is anchored to its center of hash. When a spore of humanity lands in a far off place, it relies on tenuous connections back to its parent blockchain body. If the location is rich in resources, the spore multiplies and becomes capable of extracting more energy from its environment. Eventually a new blockchain body springs forth, reliant on its own mining metabolism, carrying the genetic imprint of the original chain but now independent. A child body, a daughter chain.

In this way blockchains will seep across the solar system, attracted by energy and resources. Flocks of mobile transport/miners will migrate among the

worlds looking for the best way to arbitrage fuel & time across interplanetary hashrate and shipping markets. Humanity will grow like a fungus or slime mold, comfortable in our warm and dark corner of the Milky Way.

(This section was inspired by conversations with and the excellent work of Brandon Quittem.)

Beyond Sol



An Embarrassment of Riches

Why would we travel all the way to another star system if we can build anything we need right here at home? (Source)

What will it take to extend the tendrils of our civilization across the gaps between the stars? Science fiction often presents interstellar colonization as an inevitability of future progress. The more realistic scenario is that humanity will reach some point where interstellar colonization becomes theoretically possible but practically unachievable due to costs. While it may be practical to send small probes quickly, sending thousands of humans and equipment on a years-long journey to another star will be one of biggest investments humanity ever makes. What would be the return?

Consider that there is sufficient matter and energy right here in the solar system to support indefinite growth in human population. Feedstocks of metals, water, and gases are all abundant in asteroids, comets, moons, and the gas & ice giants. We know how to create spin gravity, and the asteroid belt alone has enough raw matter to fashion many thousands of Earths worth of living space in artificial habitats. Fusion powered by water would let us ignite miniature suns for ourselves wherever we choose to live. And we can begin to harvest the enormous power output by the Sun each second, currently lost to space, uncollected by anyone. Why would there be demand to settle new star if our own solar system has infinite supply?

Distance makes the hash grow stronger

Why settle Alpha Centauri? Because it's far away.

The answer again lies in blockchains, distance, and artificial scarcity. While the first Martian settlers were easily able to use bitcoin on Earth, the first settlers of Alpha Centauri would be operating with a 4 year light lag to Earth. This would make bitcoin and any other Solchain unusable by Centaurans far before they even arrived at their destination, while they were still in deep space. Once they arrived at their destination, this light lag would give them a tremendous advantage defending against antagonistic hashrate on Earth. They would be able to start their own blockchain far sooner after their founding than any Solchain in history. In this way, the first settlers of Alpha Centauri would be given two unique opportunities. First, they get to make history by being the first humans to settle another star system. Second, they make fortunes by quickly being able to start and mine their own blockchain. As the Sol system grows more crowded, the perceived return on the investment of a colonization mission will grow. The timeframe for this investment may be a century or more, but the hyperbitcoinized future is one of sound money, low-time preference, and correspondingly long investment horizons.

Mallory was asked "Why climb Mt. Everest?" and his stoic response has become famous, the slogan of explorers and adventurers ever since: *Because it's there.* Some future Mallory, head of the first Alpha Centauri settlement mission, will be asked "Why settle Alpha Centauri?" and their response will similarly become famous, an inspiration to countless new colonists: *Because it's far away.*

Blockchains incentivize our species to spread far apart, so that great distances may intervene, casting their hash horizons over colonial outposts like dark wings, protecting new, fledgling coins. If this hypothesis is true, it means that bitcoin is more than merely new money.

It is a new driver in the expansion of civilization and will play a bigger role in the future story of humanity than any of us now realize. HODL on.

Beyond Humanity

Stay tuned for Part 2 of this series in which we examine the more universal consequences of these speculations and Part 3 in which we dig into how blockchains will transform our understanding of space and time.

Postscript

A great many people helped make this article possible. Foremost among these are my brilliant and understanding colleagues at Unchained Capital who have my gratitude for participating in and tolerating many wonderful conversations and Slack threads. Ryan Gentry, Taylor Pearson, Tuur Demeester, Buck Perley, Marty Bent, and Brandon Quittem gave me excellent feedback on early drafts. Dan Held, Clark Moody, Grisha Trubetskoy, Murch, David Harding and many others laid the foundation for all this speculation. Thanks to all of you!

Discovering Bitcoin: A Brief Overview From Cavemen to the Lightning Network

By Giacomo Zucco

Posted September 2019

Welcome to the introduction to a series of seven articles, entitled "Discovering Bitcoin: A Brief Overview From Cavemen to the Lightning Network."

"Did You Just Say *Seven*?"

I know what you are thinking, dear reader: Seven articles outlining the history of Bitcoin is too much for your busy schedule and too little to do justice to such an ambitious subtitle. As for your schedule, just relax: Today is Monday and, before next Sunday, you have exactly seven days, one for each article. *Bitcoin Magazine* suggested that I keep each article at around 1,200 words: Based on the average reading speed of an adult (265 words per minute), that's less than five minutes per day! You can find them, believe me. Also, by the end of this introduction, you will have already read 1,200 words, which aren't even included in the total count, since this is just the introduction. Yes, I scammed you. SFYL. As for the pretentious subtitle, I believe that these seven brief articles will be enough to develop — if not a deep knowledge of Bitcoin (an intricate maze of distributed systems engineering, open source development, applied cryptography, Austrian economics, information security and more) — at least a very high-level overview of the purposes it was designed to fulfill and of the reasons why it is structured the way it is. I chose this title not only because I intend to present the subject as a process of discovery but also because many of the best Bitcoin books and conferences are titled with a gerund (*Mastering Bitcoin*, *Programming Bitcoin*, *Grokking Bitcoin*, *Inventing Bitcoin*, *Understanding Bitcoin*, *Scaling Bitcoin*, *Breaking Bitcoin*, etc), so I wanted to respect the tradition.

Original Vision: The "Five Ws"

One of the challenges in trying to explain Bitcoin — its purpose, its structure and how the former conditions the latter — is deciding where to start. Allow me to bore you with some personal background here to justify my choice. The first few times I had to select some conceptual map, back in 2014, I opted for the famous "Five Ws," an established information-structuring technique that Wikipedia tells me dates back to Aristotle himself!

When?

I decided to put the "When?" part first, to frame the actual necessity for a so-called "blockchain" (the ugly but also popular word sometimes used to label Bitcoin's "timechain"): Basically just a time-related tool needed to establish a canonical ordering and to enforce a unique history in the absence of any central coordinator. Since the term had, by then, already become an abused buzzword, I considered it important to stress that everything a "blockchain" does is to answer questions based on "when" (specifically: "When can I reasonably consider this transaction as practically irreversible?" and "When was this unit of value added to the ledger relative to others?"). Bitcoin only needs a "blockchain" to prevent double-spending of valid transactions and to keep the supply growth rate under control in a decentralized setting.

Who?

But what are those "valid transactions"? In order to explain the ownership scheme in Bitcoin and the role of digital signatures, I introduced the "Who?" part, trying to provide my clients with an introduction to public key cryptography and to some general cybersecurity practices.

What?

In order to clarify concepts like "proof of work," algorithmic difficulty adjustment and finite total supply of virtual "units," I introduced the "What?" part, trying to deliver a basic introduction to client-puzzle functions and to some theory of value, as well as to answer questions like how the supply growth could be algorithmically controlled?

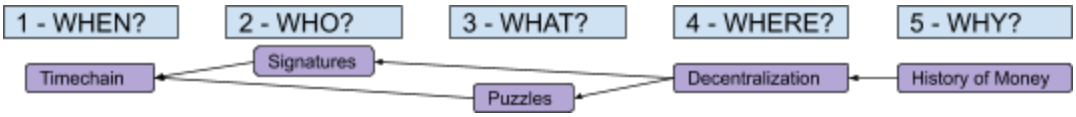
Where?

But why bother with "decentralized settings" anyway? Since there are central "coordinators" in most architectures, it would be reasonable to leverage them to provide a relative and unique chronology (no inefficient "blockchain" needed), to manage identities (no need for digital signatures, with all of their

UX and security challenges), or to issue digital receipts for physically scarce goods (no need for a slow and painful price-discovery process to assign some value to intrinsically digital scarcity). The "Where?" part was used to clarify that our assumption was a system with no single point of failure, designed to avoid the fate of political censorship which affected centralized predecessors of Bitcoin, like E-gold.

Why?

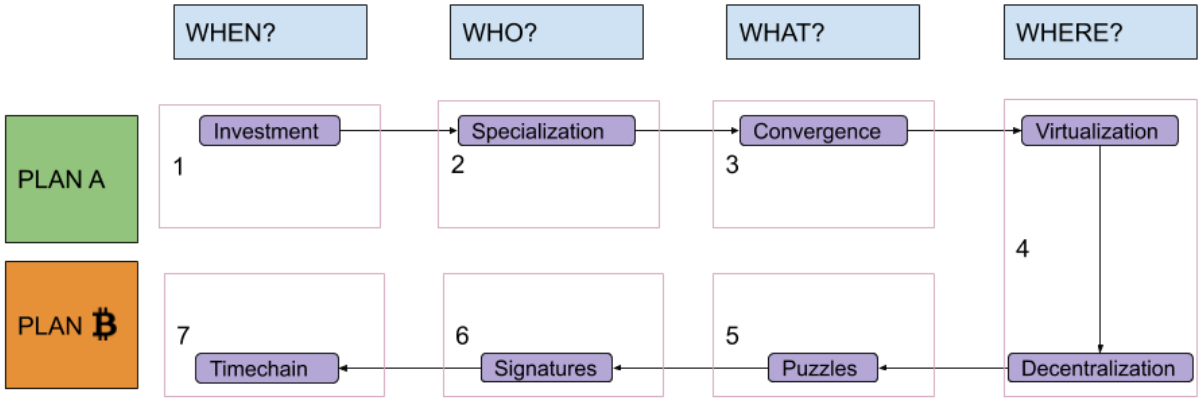
And what about the reasons for such political censorship? I moved then to the "Why?" part, where I tried to give a quick overview (more logical than historical) of the evolution of money: from stored consumption goods, to barter, to commodity-money, to free-banking representative money to monopolistic "fiat" money. The lessons were usually arranged more or less like this (the arrows represent a logical dependency, "We need the thing on the left because of the right"):



Upgrade: Four Ws, Two Plans

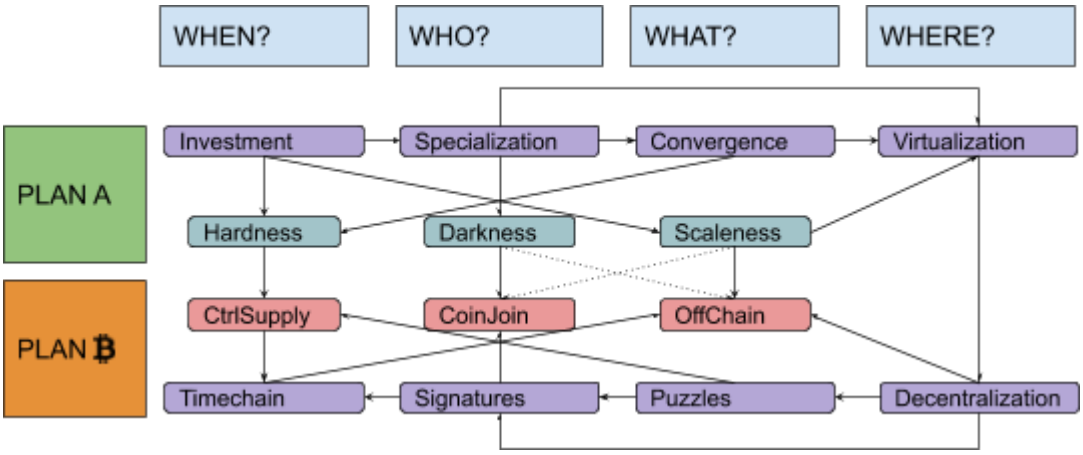
There were two problems with this model, the first being ordering: Each step was presented as necessary to "fix" the next one, in a sort of reversed causal chain, but the full picture became clear only at the end. It would have been more natural to flip it, starting from some monetary history in "Why?," going through failed attempts at building centralized alternatives to fiat money in "Where?," introducing decentralized value issuance in "What?" and decentralized ownership transfer in "Who?," and finally ending with decentralized unique chronology in "When?" The second problem was the amount of information packed inside the "Why?" part. A lot of possible subsections, ironically, fitted quite well in the four remaining "Ws": discussions about saving and investment fit pretty well in a "When?" section, discussions about exchange and specialization in a "Who?" section, discussions about convergence and liquidity in a "What?" section and discussions about virtualization of value by trusted central parties in a "Where?" section. Solving these problems would have required my audience to remain open-minded and focused while I ranged from cavemen to central banks. I couldn't afford, back then, to keep them waiting for the "blockchain" meme for so long. But now I can. I guess that means, dear reader, that you will endure four (pseudo)historical articles before I even introduce the very first bit of cryptography! Stay strong! I labeled the first part of this series, ranging from fish-eating cavemen to modern monetary systems, "Plan A,"

since it represents the first attempt at developing a monetary technology, characterized by a progressive centralization and by a very unhappy ending: fiat money. The second part is labeled “Plan ₿” (yes, you guessed it: the “₿” stands for Bitcoin): It starts from the messy situation that Plan A got us stuck in, approaching state-of-the-art Bitcoin development. The “Where?” part is the conjunction (and turning point) between the two plans. Something like this:



Trigger Warning!

In this series, I will often prioritize conceptual symmetry over economic rigor and technical accuracy. I will privilege logical connections over real-world chronological sequences, both in relation to monetary history and to technological development. I will commit terminological abuses that would make most economists and developers cringe, particularly when I discuss money attributes (where I will use an almost-made-up word: “scaleness”) and implementation paradigms (where I will abuse the term “CoinJoin” to address Bitcoin’s UTXO-model in general). No spoilers, but the overall map of logical connections should look something like this:



All the articles will include beautiful illustrations by @CryptoScamHub, of Bitcoin Twitter fame, in his signature "toxic" style. So, are you ready? Cancel all of your appointments for the next week. Or, at least, remove five minutes from one of them, each day. See you next time, for "Discovering Bitcoin Part 1: About Time." ***Continue reading the "Discovering Bitcoin" series here:*** "Discovering Bitcoin Part 1: About Time" "Discovering Bitcoin Part 2: About People" "Discovering Bitcoin Part 3: Introducing Money" "Discovering Bitcoin Part 4: A Wrong Turn (New Plan Needed)!" "Discovering Bitcoin Part 5: Digital Scarcity" "Discovering Bitcoin Part 6: Digital Contracts" "Discovering Bitcoin Part 7: The Missing Pieces"

Discovering Bitcoin Part 1: About Time

As anticipated in the introduction to this series, we will start exploring the period of monetary (pseudo)history prior to fiat money, which we call "Plan A," focusing on the topic of time and on the question "When?" There won't be much cryptography or computer science in what follows: It will all sound very simple, even … primitive! Indeed, I would ask you, dear reader, to try to forget your advanced education and your civilized manners, and pretend, just for a few minutes, to be a fish-eating caveman. *This is the first installment of bitcoiner Giacomo Zucco's series "**Discovering Bitcoin: A Brief Overview From Cavemen to the Lightning Network**." Read the Introduction to his series here.*

From Immediate Consumption … to Storage …

Image courtesy of CryptoScamHub

Your caveman life is based on immediate consumption: You use your bare hands

and a pointy stick to catch two fish every day, then you go back to the cave and you eat them immediately. One fish would be enough to survive, two are enough to feel "Thanksgiving full." Every day you catch and eat two. You don't save. It's always the same. Your "utility function" (this is what a fancy economist would call it) is constant with respect to time.

Image courtesy of CryptoScamHub

But let's try to think about the future for a bit! What if, instead of eating both fish, you eat just one and save the second (alive in a jar, for example)? Do it for two days in a row, and on the third day you will be able to eat your fill without even going out to fish! I will admit this is not a great improvement yet: You just give up some pleasure today and tomorrow, in order to get some rest on the third day. Not impressed.

… to Investment!

But what about spending that third day building a fishing rod ("capital good"), which would enable you to catch four fish instead of two, every day, forever? That's called investment: You give up some pleasure for a while, but in return you get some productive and durable results. Congratulations, dear reader: You are a "low-time-preference capitalist caveman" now! With your brand new fishing rod, you can eat two fish every day *and* rest every two days!

But why stop here? You could invest some of your day off in building a large fishing net, which you could use to get eight fish a day! By saving and investing, you can get more fish, thus have more time to build something more efficient, as long as there are improvements to achieve. The more time you spend saving and investing, the wealthier you get. The growth is not even linear: Every improvement can build on top of the previous one! Soon enough, you will be "Captain Caveman": commanding a huge fleet of wonderful fishing boats, getting 1,000 fish a day!

It's easy to underestimate the deep implications of this process. Predisposition to invest (after having saved, delaying consumption) is linked to something economists call "low temporal preference," which is, in turn, connected to very important effects on the well-being of people and of entire civilizations! A very good account of the significance of these topics and of their relationship with monetary technologies and practices is given in the book *The Bitcoin Standard* by Saifedean Ammous. Read it, if you haven't. Another great reference is the essay "Money, Bitcoin and Time" by Robert Breedlove.

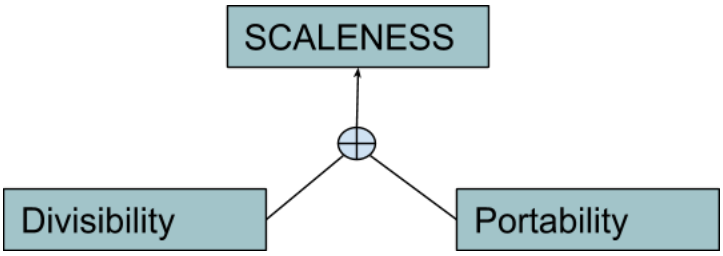
Physical "Hardness"

In order to be useful for this kind of process, a good must possess a good "hardness": Any unit of said good should not significantly lose its ability to provide utility if stored over some period of time. (This means the good does not easily decompose, deteriorate or degrade, or it does so comparatively less than other goods.) Other common terms for this attribute are "durability" and "salability across time." (In the context of your currently solitary condition, you should interpret the "sale" part as "you selling something to your future self.") In all of the cases above, the expressions are often used beyond the physical scope to include the social and institutional attributes of goods as well. Since you are a lonely caveman, and there is no society or institution around you yet, we employ the term "hardness" only in the narrower sense of physical resistance to deterioration of the units of good, delegating other aspects to Part 3 (coming soon).

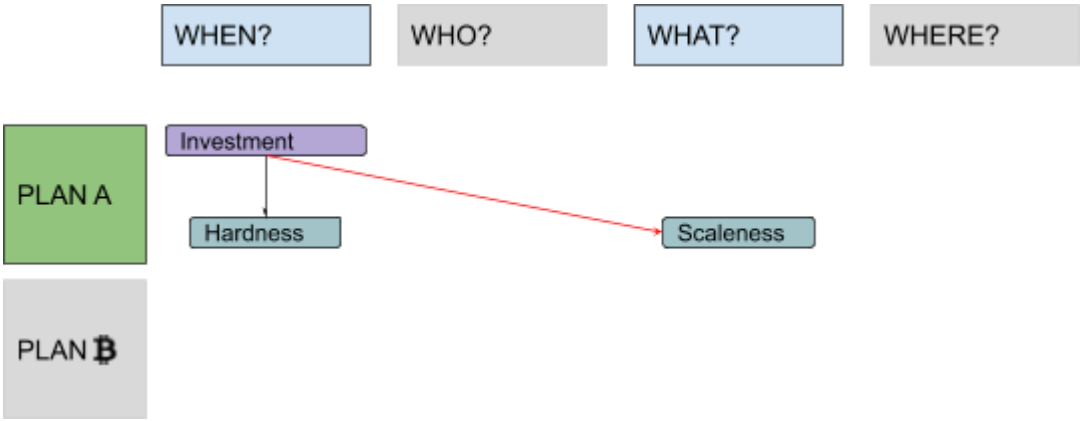
The good we chose as our first example, fish, is not very "hard," comparatively, at least not if you don't perform some specific actions as soon as you bring it back to your cave. A trivial action would be to keep it alive in a jar, as mentioned. Without additional treatments, a fish kept alive is more durable than a dead one. A smoked or salted fish, though, would be even more durable than one kept alive.

A New Attribute: "Scaleness"

Even dismissing social considerations, there is another reason for which unitary physical durability doesn't really cover, alone, the broader concept of scalability across time. The fact is that the ability to store arbitrary quantities of a good is not dependant only on its unitary attributes! At the beginning of your virtuous cycle of saving and investment, you decided to eat one fish and to store the other alive. How convenient that, in order to survive, you needed to eat exactly *one fish* and not, for example, one and a half fish, leaving you with half a fish to store! Indeed, a live fish isn't great for divisibility. Smoked, salted or refrigerated fish would fare way better. On the other hand, considering that by the time you appointed yourself "Captain Caveman" you started storing 1,000 fish every day, keeping them alive in jars must be quite challenging. Again: Conserved fish would be way easier to store than living specimens. In these examples, the discriminant is not how well any unit of good maintains its value across time, but rather how well the overall good maintains it across "scale": when you store smaller fractions of it vs. when you store larger multiples. The former case is usually addressed in monetary theory with the term "divisibility," the latter with the term "portability" (which often carries some movement-across-space connotations, but ultimately boils down to the fact that a portable good must possess high value in small bulk).



The composite attribute is sometimes called "salability across scale," which, just like "salability across time," is actually pretty neat. Since I like shorter terms, I will use the (almost made-up) word "scaleness" instead (I guess this is a case of terminology choice which would deserve a Trigger Warning as I described in my introduction). This attribute has more to do with the "What?" column than with the "When?" one, to be fair.



It's interesting to note the nice link with the word "scalability," which usually means something else entirely (it refers to the property of a system to handle a growing amount of work by means of additional resources). Within the context of Bitcoin, however, it has been used to address the technical limitations on the number of settlement transactions per unit of time and cost (related to the fact that blocks are limited in size and frequency). In this very specific meaning, the "salability problem" could be reduced to a divisibility one (basically, it doesn't make economic sense to transfer amounts that are less valuable than the transfer costs), thus the conceptual link is justified. So far, you've learned:

- to store your wealth, sacrificing immediate consumption
- to invest your stored wealth, increasing your productivity
- to focus on goods that show good physical "hardness" and good "scaleness."

But what can you do with all of the fish you catch every day? Not much, actually, if you are still able to consume just two and you can't exchange them, which is something you will learn about tomorrow, in Part 2.

Discovering Bitcoin Part 2: About People

This is the second installment of bitcoiner Giacomo Zucco's series "Discovering Bitcoin: A Brief Overview From Cavemen to the Lightning Network." Read the Introduction to his series and Discovering Bitcoin Part 1: About Time. In this installment, we will build on the previously acquired strategies of storing wealth, investing that stored wealth, and increasing productivity and focusing on goods with physical "hardness" and good "scaleness," to explore the concepts of exchange, specialization and "darkness."

From Solitary Consumption … to Exchange …

Welcome back, dear reader. Let's further explore the period of monetary (pseudo)history prior to fiat money, which we call "Plan A," this time focusing on the topic of people and on the question "Who?" As we established in Part 1 you are now a very successful caveman: You own and manage a huge fleet of fishing boats, catching more fish than you could eat in a lifetime.

Image courtesy of CryptoScamHub

While you managed to leave immediate consumption behind, learning the art of saving and investing, you are still practicing solitary consumption. Not that you are necessarily alone: There might be someone around you, but you are not exchanging with anyone, so it doesn't really matter if there is just one caveman or hundreds of cavemen (or cavewomen, or cave-nonbinary-people; you have to forgive the lack of politically correct sensibility in these articles — we are discussing primitive times). Every day, you catch 1,000 fish, eat two and store the rest. After a short while, your utility function gets flat with respect to the amount of fish you catch and the number of people around you. Consider this scenario: Apart from fishing, each caveperson can also

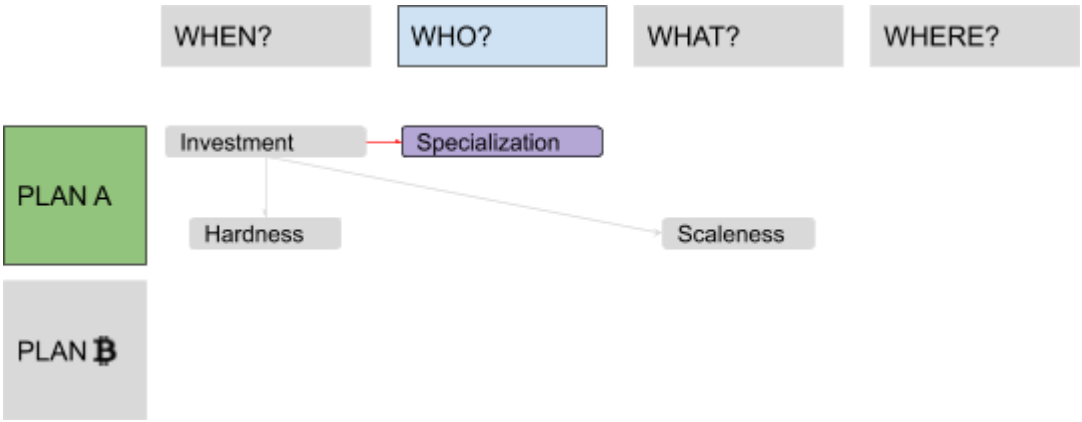
draw two jars of water from the local spring every day and survive on drinking just one. What if, instead of eating two fish and storing 998, you start storing just 997 and *exchanging* one with Alice, a nice cavewoman who can give you an extra jar of water in return? In this way your utility increases, and after two days Alice could start working on her own fishing rod! Clearly, the number of possible exchanges can grow with the number of cavepeople in your local cave-economy.

Image courtesy of CryptoScamHub

But not that much, admittedly. First of all, it's not all that hard for you to draw some water by yourself. Furthermore, Alice is also able to fish and save one fish per day, like you did: Why should she even exchange with you? Not impressed.

… to Specialization!

But why should every process of saving and investing deal with fish? The important insight is that you cavepeople are not all the same! You each have different skills, inclinations, beliefs, preferences, priorities and experience. Alice could become a great industrialist in the water sector, for example, producing tons and tons of jarred water a day. Bob, a talented cave-artist, could specialize in nice rock paintings! So, you suggest to your cave-friends that they should adopt this new, incredible strategy: specialization! Now everybody can focus on some specific skill, and every utility function can keep growing and growing, both with time and with the number of diverse people involved in the trade. This is what we call "division of labour": the very cornerstone of civilization!



Specialization also improves investment and innovation, since even very simple tools needed for industry would be prohibitively hard to build without any help from people in other industries. (As you may know, even building just a pencil requires cooperation between thousands of different people from all over the world.) And many complex tools are needed, even just to create other tools! It's a virtuous cycle: Specialization sparks innovation, encouraging cavepeople to invest time in creating tools (tool-making tools included), increasing productivity and freeing up more time, which in turn can be used to specialize even further or to reach an even greater number and variety of cavepeople to exchange with, thereby increasing the division of labor even further, and so on!

Hardness and Scaleness Strike Again

Of course, not every kind of good can be easily passed along many different hands. The main attributes that turned out to be useful to efficiently store some arbitrary quantity of a good also help to transfer it. A good with good physical hardness — which preserves its physical features at a unitary level when stored for a certain period of time — will typically also preserve the same features when transferred over a certain number of people, and vice versa. You would have a hard time naming a kind of good that is resistant to storage but not to transfer, or to transfer but not to storage. A good with good scaleness — which is efficiently stored in small fractions (divisibility) or in large aggregates (portability) — will also show the same features when passed from hand to hand instead of stored. What we are trying to express now is not exactly what economists would call "salability across space" (possibly redundant with the concept of portability); it's actually closer to the concept of "salability across people."

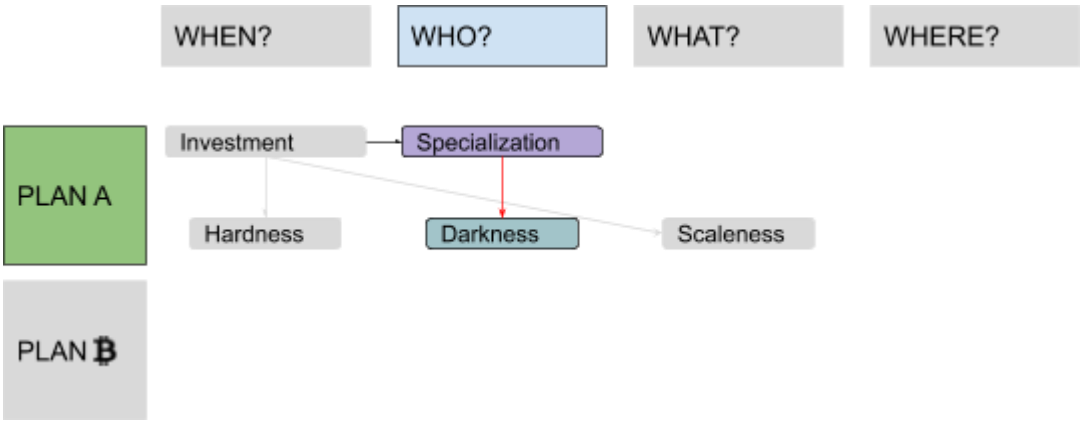
A New Attribute: "Darkness"

A good that's durable enough to maintain its unitary physical properties over many exchanges, and with enough scaleness to be exchanged in huge multiples or in small fractions, is comparatively better, as far as salability

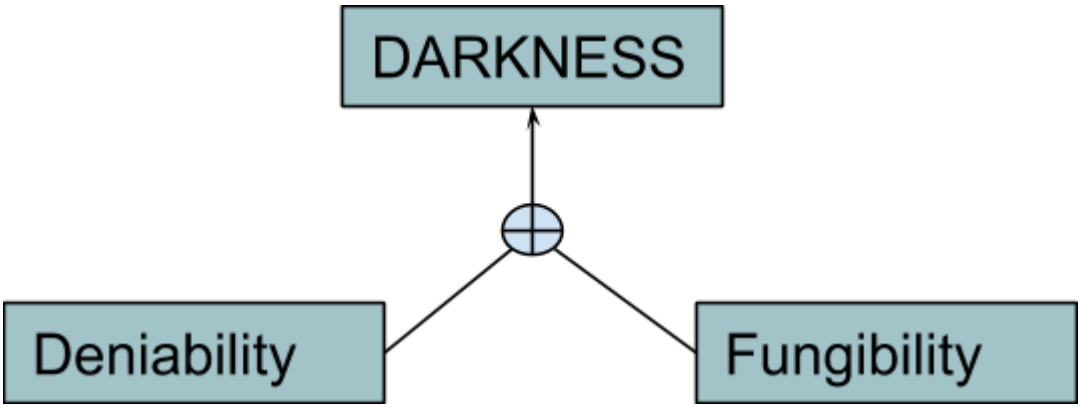
across people is concerned. But these two attributes alone still don't entirely cover that broader concept. You and your cave-friends want to exchange with a growing number of different people: the more different, the better, since diversity increases the chances of specialization. But diversity can also increase the chances of conflict and distrust: You know and like Alice and Bob, but you don't really know, let alone like, all of these new people! You want to exchange goods that don't carry the personal "mark" of previous owners and aren't connected with a specific person or tribe; otherwise, it would be difficult for them to be accepted across large scopes of trade. Furthermore, the more people exchange, the more they draw the attention of caveman Mallory: a local bully who doesn't want to increase his wealth by providing value, but by tracking, controlling, censoring and taxing exchanges. When Mallory's lust for control arrives at the point that he tries to ban exchanges between cavemen not "registered" with him, a lot of cavepeople are excluded from the scope of trade: This is the phenomenon known as "financial exclusion" and it reduces utility for everybody.

Image courtesy of CryptoScamHub

Some goods are ideal for mitigating such problems — for example, "bearer instruments," which don't carry the personal information of previous owners, making it easy for everyone to deny having been involved in any specific transaction. When you deal with such goods, Mallory could at most ban you from the market because of who you are and what you are doing now (or not doing, such as not paying him a bribe), but not because of who the previous owners were (yourself included) and what they did. This isn't an ideological problem, but a functional one: A good cannot easily be traded if the receiver has to verify the entire history of the previous owners in order to know how much political risk (including persecution, censorship, taxation, debt) he is actually inheriting. But it clearly involves moral, political and ethical aspects, like the importance of privacy as a human right. I will use the term "darkness" to address this attribute.



In the context of Bitcoin, many terms are used: privacy, anonymity and deniability (which focus on people more than on assets), but also untraceability and fungibility (which instead focus on the indistinguishability of asset units, but is, in turn, strictly connected with deniability, since a common way Bitcoin users could be spied upon is by leveraging a lack of fungibility of units, as we will see in detail in Part 6).



So far, we've learned:

- how to exchange your wealth, giving up your solitary lifestyle for a cooperative one;
- how to specialize in the production of something specific, advising your trade partners to do the same; and
- how to focus on goods that show good "hardness" and "scaleness," but also good "darkness."

But how can you exchange with a growing number of people if the complexity of all the different combinations of goods, from the demand and the supply points of view, grows even faster? This is something you will discover in "Discovering Bitcoin Part 3: Introducing Money."

Discovering Bitcoin Part 3: Introducing Money

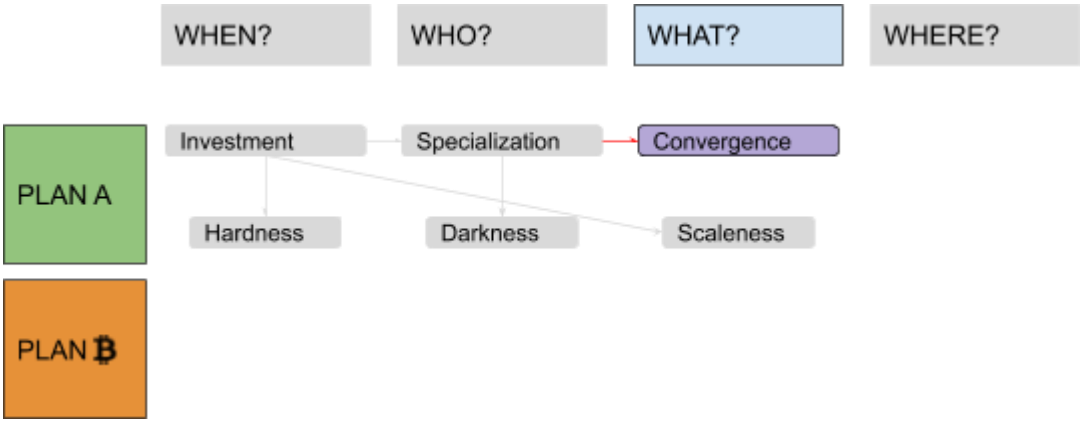
This is the third installment of bitcoiner Giacomo Zucco's series "Discovering Bitcoin: A Brief Overview From Cavemen to the Lightning Network." Read the Introduction to his series, Discovering Bitcoin Part 1: About Time and Discovering Bitcoin Part 2: About People. In this installment of the "Discovering Bitcoin" series, we will build on the previously acquired strategies of exchanging wealth, specializing production and focusing on goods with good physical "hardness," "scaleness" and "darkness" to explore concepts of scarcity, liquidity and social "hardness."

From Barter … to Liquidity Maximization …

This third step along our "Plan A" for money will focus on the topic of scarcity and on the question "What?" In Part 2, you invented and popularized practices such exchange and specialization, enabling an unprecedented level of wealth and cooperation. Good job! There is still a problem, though. In the context of barter, which is what you and your fellow cavepeople are practicing now, utility grows with the number of people exchanging, but the friction to match demand and supply for every good versus any other grows as well, since the number of all the possible combinations increases quickly! This problem has two sides: one concerns how to calculate, communicate and keep track of all of the combinations of trading couples (each caveman must declare how much of everything he would accept in exchange for everything else). The other concerns liquidity within different pairs (in many scenarios the exchange simply cannot happen, because of what economists call "non-coincidence of wants": Alice has something Bob wants, but not the other way around, or at least not in that moment). The former side can be mitigated with advancements in information technologies (such as the invention of writing, to keep track of different combinations), while the latter can be mitigated by delaying the actual delivery of one of the two exchanged goods (basically the invention of credit, which is very useful where the wants do not coincide if considered in real time, but would instead coincide in different time-frames). But the problem still exists, slowing down the specialization process.

… to Convergence!

In order for commerce to keep growing, your little cave-economy must converge toward some specific kind of good, namely the one with the best combination of monetary attributes, which will always represent one side of every trade, in order to simplify calculation and bridge liquidity with respect to every other good. This practice is known as indirect exchange: Alice trades what she offers for this "bridge-good," which she will later trade again for something she wants. The great news is that you don't have to try to convince your cave-friends one by one. This switch naturally happens due to so-called "network effects": The value of a network increases more than linearly with the number of participants, creating a kind of gravitational black-hole effect. The goods that fare better in hardness, scaleness and darkness will compete, and the first one to reach a critical mass will start swallowing the others, as far as monetary uses are concerned.



Cave-ladies and cave-gentlemen … introducing Money! It serves three functions. The first is "store of value," which was actually already served by our stored goods within the context of pre-convergence barter economies. The others are "unit of account" and "medium of exchange," which are the answers to the problems of pricing and liquidity, respectively. This is an important step in human evolution, so much so that from now on I will stop addressing you and all of your friends, as "cave-somethings." With the level of prosperity that money-based economies give you over barter-based ones, you can all get out of those smelly caves and enjoy stone houses and castles!

How to Get Good Money

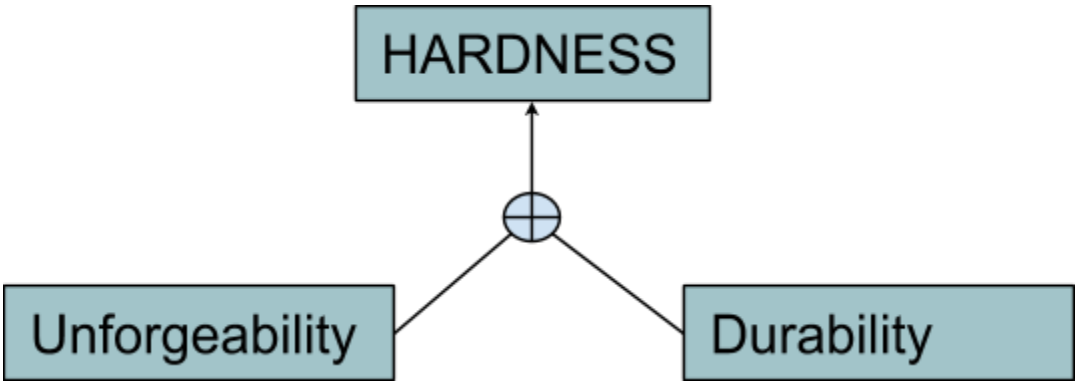
So, you just entered the magical world of so-called "commodity money"! Historical examples are seashells, beads, spices, squirrel pelts, dolphin teeth, tea bricks, salt (the word "salary" comes from that) and sheep (the word "pecuniary" from that). But now you have to face another challenge, once again related to the problem of salability across time (thus back to the "When?" question)! Imagine you've convinced your tribe to use smoked fish as money. This created more demand than the one granted by food consumption alone: Not only do people want to eat it, but they now also want to use it as money. Its price shows what is called a "monetary premium." This incentivizes you to restructure your enterprise in order to produce more of it — but then you increase the global smoked-fish supply. And the price is a result of demand and supply: If the latter keeps increasing, while the former doesn't, the price will start falling. So, even if smoked fish remains as durable as before in a physical sense, it will perform poorly as a way to store value across time. Price dynamics affect hardness in a "social" way: In the context of solitary consumption, the good would still maintain its ability to provide utility over time, but in the more advanced context of a monetary economy, that ability actually drops. And a lousy store of value cannot be a good medium of exchange, since nobody wants to lose value storing it for indirect exchange! This is not just a smoked-fish thing. It's very general: The more any good gets used as money, the more interesting it becomes for its typical producers to increase the supply in order to profit. The more the supply increases, the less that good can be used as money. This cycle isn't a smooth and gradual negative-feedback loop that tends toward equilibrium over time — the changes to the production structure in order to increase the supply take some time to be done and aren't easily undone after the value decreases! The typical outcome is more of a "boom and bust" kind. There are many historical examples of this "money trap," usually involving disastrous outcomes. This is typical of goods with a low "stock to flow" ratio, where even small percentages of change in the flow (amount of good produced or extracted in a unit of time) are comparatively huge, and thus particularly disruptive, with respect to the stock (amount already circulating in the economy).

Social "Hardness"

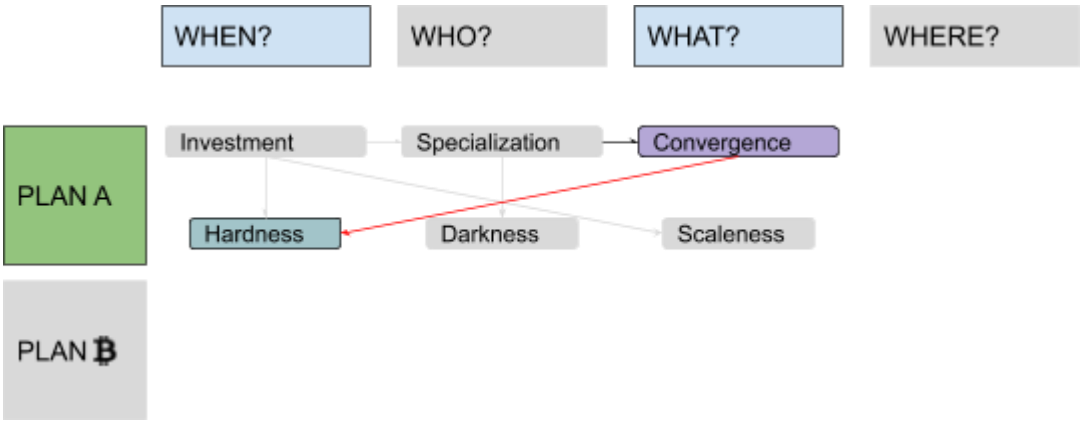
You soon realize that seashells trapped on your fishing nets, which you used to collect, provide a better money than your deliciously useful smoked fish, in this regard. And that those relatively "useless" gold nuggets you used to collect on the shelf next to seashells are even better!

Image courtesy of CryptoScamHub

Actually, you probably want to use both gold and silver. The reason is that they perform better on different sides of the scaleness spectrum: While gold is more portable, silver is more divisible. Indeed, commodities that possess a consumption value higher than their monetary premium are not very good candidates for monetary use: Since they get consumed, their stock tends to diminish, lowering their stock-to-flow ratio. In this sense, "commodity money" is more an evolution of collectibles than of actual industrial commodities. Different terms are used to address the attribute of having a supply that tends to remain inelastic with respect to increases in the demand, keeping its value over time. Various sources call it "soundess," "unforgeable costliness" or "unforgeability." I will extend the word "hardness," which we already used for the physical side of the durability problem, equating it with the more general concept of salability across time, in a physical and social sense as well.



This is a jump back to the "When?" column, to complete our analysis of the relation between time and value: The higher the degree of hardness of some monetary good, the more resistant it is to having its value compromised, either by physical decay or by supply inflation.



The question of hardness influences the process of monetary convergence: Any monetary good that can have its supply cheaply and easily increased will rapidly destroy the wealth of those using it as a store of value. For a good to assume a dominant monetary role within an economy, it must exhibit superior hardness to competing monetary goods. When discussing hardness, purely economic considerations overlap with ideological, political and ethical ones, just like with darkness. As noted in Part 1, they mostly have to do with the notion of time preference, a topic with deep ramifications in sociology, but they also relate to the problem of inflation as a way to transfer wealth, and the problem of interest-rate manipulation as a cause of financial crises. So far, you've learned:

- to advise your trade partners to converge over a single good to maximize liquidity;
- to choose that good among the ones with a better mix of physical "hardness," "scaleness" and "darkness"; and
- to consider the social, supply-related aspect of "hardness," along with the physical one.

In a word, you've basically discovered money. But can you make it better? This is something you will discover in "Discovering Bitcoin Part 4: A Wrong Turn (New Plan Needed)!"

Discovering Bitcoin Part 4: A Wrong Turn (New Plan Needed)!

This is the fourth installment of bitcoiner Giacomo Zucco's series "Discovering Bitcoin: A Brief Overview From Cavemen to the Lightning Network." Read the Introduction to his series, Discovering Bitcoin Part 1: About Time, Discovering Bitcoin Part 2: About People and Discovering Bitcoin Part 3: Introducing Money. In this next installment of the "Discovering Bitcoin" series, we will build on the previously acquired strategies of optimizing "hardness," "scaleness" and "darkness" to explore concepts of virtualization and decentralization.

The Path Toward Virtualization

The question "Where?" will bring us to the (quite unhappy) end of Plan A and the beginning of Plan ₿! Thanks to your noble efforts, everybody is now using gold and silver as money. (With such a track record, you decide monetary innovation is your actual vocation: You sell your fishing fleet to focus on that exclusively.) The next innovation you introduce is "coinage." While people used to sustain important verification costs when receiving metal money, now you can pre-sign standard measures (obviously you ask for a fee for such a service, called "seigniorage"), and everybody can just cheaply verify your signature.

Image courtesy of CryptoScamHub

Coinage (which is particularly interesting for Bitcoin, since it's similar to the dangerous practice known as "SPV," which we will discuss later in Part 7) increases hardness locally, since lower verification costs

mean higher forgery costs for occasional counterfeiters. But while it may increase locally, hardness may also decrease globally: Now you have the ability to inflate the money supply with a trick called “debasement” (just put less gold in your coins than you originally promised, secretly increasing your seigniorage fee). Next, you invent “custody”: Instead of securing their coins directly, people can entrust them to you, in exchange for convertible certificates. Since you leverage economies of scale and specialization, you’ve become quite efficient at securing other people’s money (for a fee, of course).

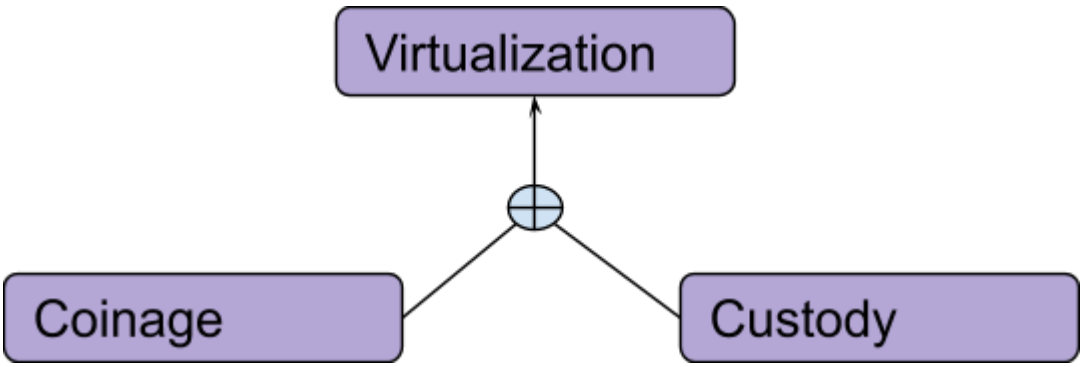
Image courtesy of CryptoScamHub

Custody increases scaleness dramatically! So much so that it helps the convergence process to reach its ultimate completion: Having to store just paper instead of physical gold (not very divisible) and physical silver (not very portable), people converge over the former (harder money), demonetizing the latter (the monetary premium of which will eventually collapse). But global darkness and hardness may instead decrease: In the redeeming phase, you could easily track and censor transactions, or you may practice what is called “fractional reserve” (keeping less collateral than issued certificates, basically inflating the “virtual” supply).

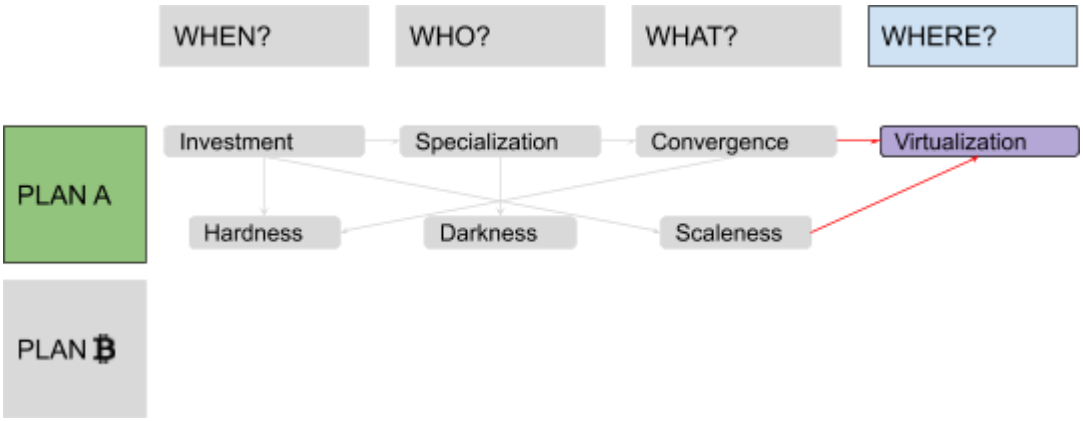
Complete Virtualization

Your next proposal is complete virtualization. (Funny note: Bitcoin is often called “virtual money,” but money has already been “virtual” for centuries!) It’s the merging of custody and coinage: Instead of just entrusting you with

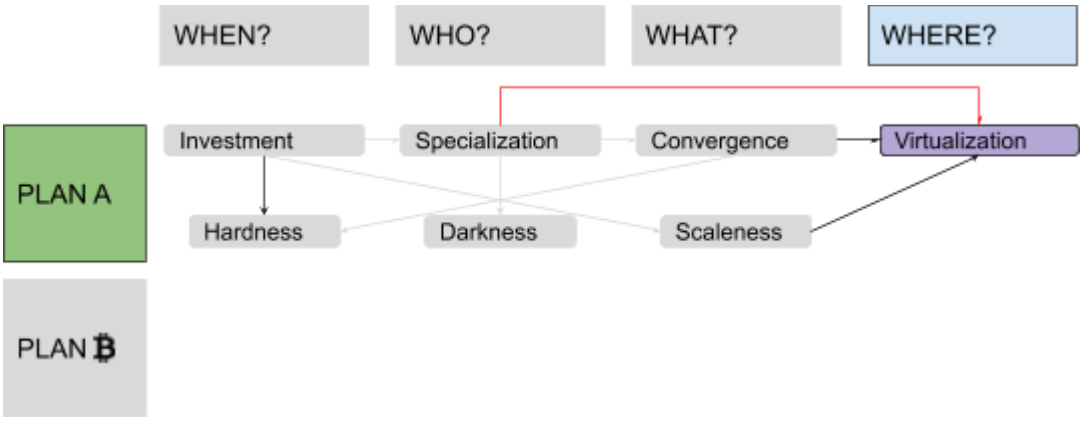
some signed coins in order to redeem them later themselves, people can start trading your signed paper certificates directly, using them as a medium of exchange. You finally invented “banknotes”!



It’s not commodity money anymore; it’s some kind of “information money” (not yet what we call “fiat money,” though — it’s still a form of free-market innovation, emerged from society without any kind of legal imposition, provided by different competing actors and collateralized with physical gold in custody). Sure, you could abuse censorship, debasement and fractional reserve, if you wanted, but you aren’t Mallory (our bully from Part 3); you’re a reputable professional, and these bad incentives are mitigated by the competitive pressure of several other providers.



We could consider the process of virtualization as an extreme case of specialization (after money enabled division of labor, money management itself become a specialized job itself). It’s a centralizing process: Collateral physically moves from many users to the few service providers.



Ultimately, the "Where?" question isn't really geographical in nature: It's more about control. The provider may have vaults, or mints, distributed across the world, but their control is centralized.

A Wrong Turn: Monopoly

You haven't forgotten about Mallory the bully, right? Good, because he is the main character in the transformation from free-market virtual money to fiat money! For a while he posed as a mere competitor to your services of custody and coinage, but now he is revealing his true colors. While it was pretty difficult for him to take over the very decentralized process of people exchanging gold nuggets, there are now a few big, public, trusted, vulnerable entities he can easily seize control of. First, he uses threats of physical violence to establish a compulsory monopoly on virtual money (or even on money tout court, regardless of whether or not the physical variant is out of fashion anyway by now), ruling all the alternative money services, including yours, "illegal." Then he forces everyone to always accept his particular brand of virtual money as payment at face value. (He likes to call this obligation "legal-tender laws.") Finally, he abolishes any kind of redeemability of his certificates in actual gold collateral. Now the supply of money is politically defined (by Mallory-appointed central bankers, who can finally implement "monetary policies" to shape the economy based on his political goals), while the demand for money is politically driven (since people are forced to own the legal tender to pay taxes to Mallory, and are forced to accept it at nominal value when they trade).

Image courtesy of CryptoScamHub

Until now, in the context of free-market virtual money, competition and market forces could have somehow still incentivized banknote issuers to "behave." With fiat money, thanks to legal monopoly and legal-tender laws, there's no competition anymore, at least not within the context of Mallory's "jurisdiction." (There are other, smaller Mallories around the world, but they all joined the Big Mallory in a huge cartel).

The Internet and Digitalization

Enter the digital era! With e-commerce, people need to transact over the internet, but they can't exchange paper there. Mallory's fiat money (which is already virtual) migrates to digital versions that are orders of magnitude more efficient: Scaleness increases again! Somebody could argue that in leveraging digital technologies, scaleness would have gone up even more in the competitive context of digital free-market money (since a monopoly keeps costs high while keeping efficiency, transparency and innovation rates low). But since things are improving anyway, nobody complains too much. But hardness and darkness decrease dramatically: The money supply can be manipulated to degrees never seen before, and Mallory can track and censor transactions to Orwellian extents.

Image courtesy of CryptoScamHub

As a money entrepreneur, you try to leverage the same innovations that made Mallory's money so powerful in order to bring back free-market representative money, only this time "on digital steroids." Your hope is that the very same internet that Mallory leveraged to increase his power could also be leveraged by you to bypass, ignore and circumvent Mallory's impositions. You launch a startup called "e-gold" (this is all completely fictional, of course). Your

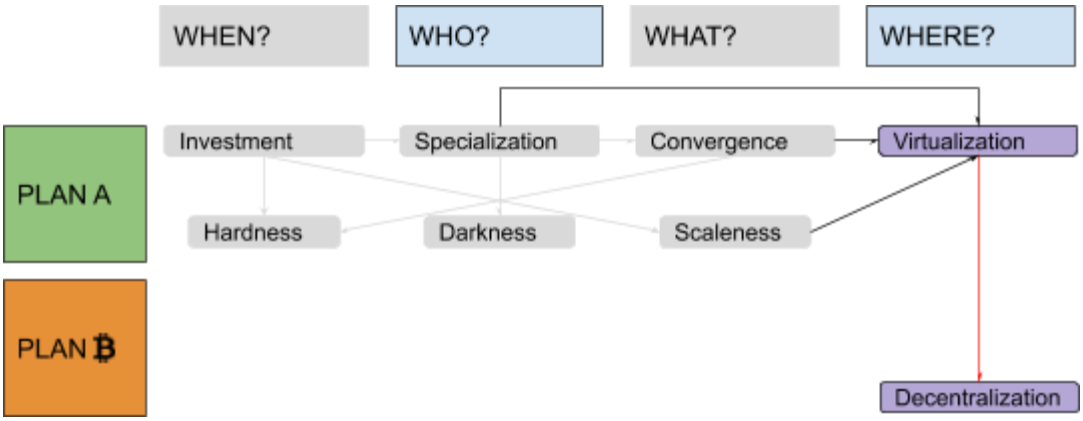
service allows pseudonymous users to open accounts denominated in grams of physical gold, freely transacting among them. You set it up using technological best practices and you devise innovative governance structures. After some time, your system has grown to 5 million accounts, processing the equivalent of 2 billion Mallory-dollars per year! But despite your great execution and the positive market reception, all of your technical and legal skills cannot protect you from Mallory's violence forever. Eventually, he manages to shut your business down and send you to jail, discouraging other entrepreneurs from following your example. (They pivot to some traditional, Mallory-approved, digital fiat services instead.)

Image courtesy of CryptoScamHub

Decentralization: A New Hope?

During the time you "serve" in jail as a retribution for daring to try to provide better money than Mallory's, you realize something: It was very easy for Mallory to send you to jail, close your company and shut down its servers, because the personal, legal and technical structures were all easy targets. What if, this time, you replace your official identity with some internet pseudonym (the Japanese-sounding "Satoshi" may be just as good a choice as any), your for-profit company with an open FLOSS project, and your server with a peer-to-peer protocol? Then Mallory would have no CEO to incarcerate, no legal entity to seize, no server to shut down! The idea is to reverse the centralization trend that has prevailed until now, while retaining

most of the advantages of technological progress that enabled e-commerce and e-finance.



So far, you've learned:

- that the process of money virtualization greatly increases its "scaleness";
- that the same process enables violent monopolies, which in turn greatly decrease "hardness" and "darkness," especially in the digital era; and
- that you cannot effectively fight monopolization using centralized entities. You have to aim for *decentralized* solutions.

But how can you actually decentralize asset issuance and ownership? We will answer the first of these two questions in "Discovering Bitcoin Part 5: Digital Scarcity."

Discovering Bitcoin Part 5: Digital Scarcity

This is the fifth installment of bitcoiner Giacomo Zucco's series "Discovering Bitcoin: A Brief Overview From Cavemen to the Lightning Network." Read the Introduction to his series, Discovering Bitcoin Part 1: About Time, Discovering Bitcoin Part 2: About People, Discovering Bitcoin Part 3: Introducing Money and Discovering Bitcoin Part 4: A Wrong Turn (New Plan Needed)! Next in the "Discovering Bitcoin" series, we will build on the previous events of money virtualization, establishment of dangerous monopolies and emergent needs for decentralization, to explore concepts of scarcity in the "virtual" world, energy consumption and digital hardness.

Proving Work: Digital Puzzles

Welcome back to this journey through our Plan ₿ for money, which brings us, for the second time, to focus on the topic of scarcity and the question "What?" Value needs scarcity, but in the digital world that's really difficult to get: Information tends to always be infinitely reproducible. In your previous e-gold experiment, digital units represented actual physical gold stored by your centralized company. But how can you create a protocol in which everybody can independently agree on what is being transmitted, without any central authority? If such a method required a centralized third party, you would be back where you started, with a central point of failure vulnerable to Mallory. If such a method was "everybody can issue however many units they want," the system couldn't work: Incentives would push the supply of units toward infinity, and their price toward zero. The answer you finally come up with is *puzzles*! You write an open procedure that everybody can run on their computers in order to try to solve some puzzles with the characteristics of being "ad hoc" (specifically built around every issuance attempt, otherwise solutions could be reused many times), asymmetric (difficult to solve but easy to verify, otherwise the system would be vulnerable to denial-of-service attacks) and "useless" (otherwise external use cases for the same solution effort could distort incentives within the system). Every solution will grant the "right" to issue a certain number of units.

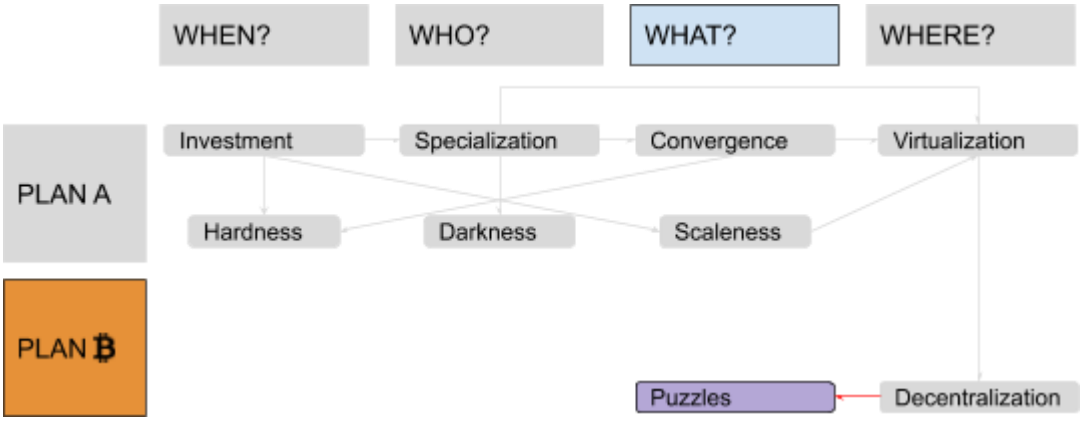
Image courtesy of CryptoScamHub

Non-digital examples of similar puzzles are sudokus or crosswords: "useless" games in which finding the solution (which depends on some specific parameters that are different every time) requires a lot of trial and error, while verifying that solution, once it has been found, is trivial and quick. More technically, what you need is called "proof of work" (PoW). It's somewhat similar to a CAPTCHA, but intended for computers and not humans to solve.

Hashcash

Your choice falls on a specific kind of PoW called "Hashcash" (created by your friend Adam and originally intended for spam prevention in the context of anonymous email exchanges). The way it works is through "hash collision": a kind of "brute force attack" where a machine automatically tries out several slightly altered versions of the original message, over and over, with little changes every time, until one of the versions, passed through a one-way function called a "hash" (the mathematical equivalent of fingerprints or footprints), results in a string that respects some kind of constraint. Hash functions, while deterministic (starting from the same message, they give the same result every time), are also unpredictable (slightly different messages will result in completely different hashes, in a way impossible to guess or predict before actually calculating them) and irreversible (it's easy for everybody to verify the hash of a known message, but it is not possible to go back to a single message from just a hash). If your users want to "deposit" digital assets, they have to create a "deposit" transaction, add some random

number and apply a hash function, repeating the process over and over again until the result, for some number, is verifiably smaller than a certain threshold, called "difficulty."



Energy Consumption

Your users will have to "waste" some energy to find solutions, but this is a requirement, not a bug: The only way to make something scarce is to make it costly to produce — there's no other way around it. This "waste" argument is often used by critics of your system (especially Mallory and his friends) to accuse your pseudonymous alter ego of being "environmentally unfriendly." This is not really the case, for several reasons. First, energy spent in PoW is no more "wasted" than in any other production process for any other (physical or intellectual) good. Second, the consumption of energy in your system is likely going to remain lower than historical alternatives (we are talking orders of magnitude less than the energy consumption for gold extraction, for example). Third, entrepreneurs generating PoW to get some "digital gold" aren't incentivized to consume more energy — if anything, they are incentivized to consume *less* of it (to them it's a cost, not a revenue). This drive toward using less energy increases optimization and efficiency with new technological breakthroughs or with smart generation choices, which in turn can have a waterfall effect on other energy-consuming industries. There would be no advantage to complicated kinds of PoW that make optimizations difficult. Indeed, the opposite is true: The most efficient PoW is one that is friendly to optimizations (the ideal being a process close to the thermodynamic limit).

Hardness Problems

Now, anyone in the network can verify that a certain amount of computational work has been uniquely "committed" to a certain asset deposit, but no one can reproduce that same proof for other types of statements. But this proof of work by itself is not enough to give your "digital gold" any hardness. It doesn't guarantee that the supply will remain inelastic

with respect to the demand. The hashcash model would actually be, in and of itself, very inflationary: The more the demand for your "digital gold" increases, driving the price up, the more machine power will be deployed to perform PoW, and the more resources will be invested to increase energetic efficiency, thus increasing the supply, if the latter is not additionally restricted.

The next innovation you need to include in your system is called "controlled supply."

A New Paradigm: "Controlled Supply"

Basically, whenever the issuance rate is above (or below) a certain target, the puzzle difficulty increases (or decreases), balancing the rate. You set a target of one "issuance," on average, every 10 minutes, as measured every 2,016 "issuances" (which means about every two weeks). This makes for an almost perfectly constant issuance rate. Actually, you just launched the very first asset in history with an almost totally inelastic supply compared to the demand. Whenever the monetary demand for your "digital gold" increases, the price increases, incentives to perform PoW increases and the issuance rate starts increasing as well, but then the difficulty increases and the supply goes back to being stable again — and the other way around, of course, in case the demand goes down. But you decide to go even further. Instead of having just a fixed schedule, you aim for a *fixed total supply* and introduce the "halving" mechanism: At the end of every "era" of about four years, the issuance rate is cut in half, eventually approaching a fixed stock with zero flow! The first era starts with a maximum issuance of 5 billion virtual "units," which the users call "satoshis" or "sats," as a tribute to the pseudonymous alias you came up with in Part 4. In the second era, only 2.5 billion sats will be deposited every 10 minutes, on average. In the third era, that number will go down to 1.25 billion, and so on. You chose this model to approximate the way a physical gold mine would become exhausted over time, and you call it "mining" to emphasize the analogy.

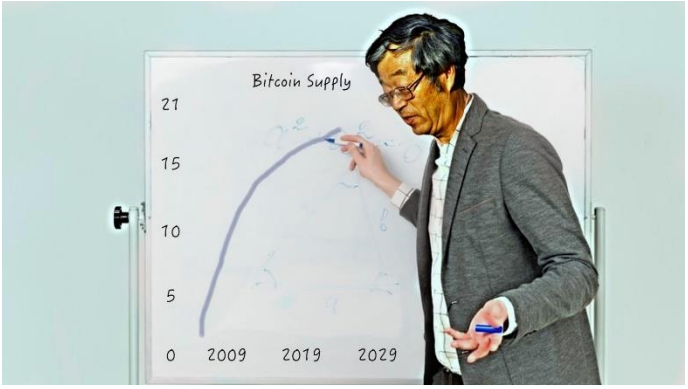
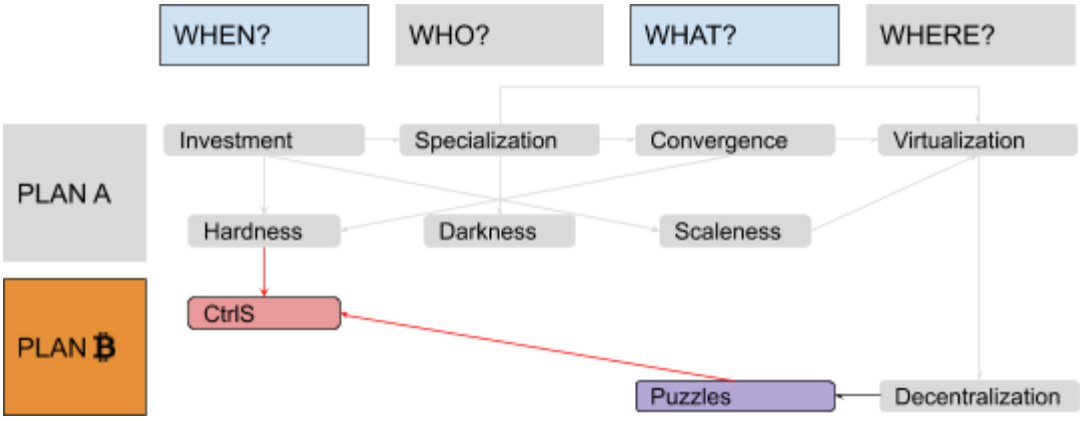


Image courtesy of CryptoScamHub

When you were using a centralized approach, you could simply piggyback the (relatively) stable price of physical gold. This new "digital gold" will require, instead, a long, difficult and volatile process of price discovery. The disinflationary nature of the issuance schedule could make some phases of this process even more "violent."



So far, you've learned:

- that in order to launch a completely decentralized system, you cannot leverage physical scarcity;
- that you can reproduce scarcity digitally and decentralize issuance, using special digital puzzles; and
- that in order to grant some hardness to your digital money, you need a strict supply control.

But now that you have effectively decentralized issuance, how can you do the same for ownership? We will answer that in "Discovering Bitcoin Part 6: Digital Contracts."

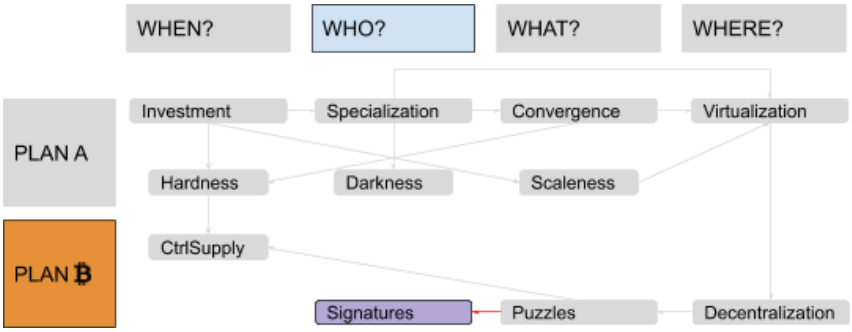
Discovering Bitcoin Part 6: Digital Contracts

This is the sixth installment of bitcoiner Giacomo Zucco's series "Discovering Bitcoin: A Brief Overview From Cavemen to the Lightning Network." Read the Introduction to his series, Discovering Bitcoin Part 1: About Time, Discovering Bitcoin Part 2: About People, Discovering Bitcoin Part 3: Introducing Money, Discovering Bitcoin Part 4: A Wrong Turn (New Plan Needed)! and Discovering Bitcoin Part 5: Digital Scarcity. In Part 6 of this "Discovering Bitcoin" series, we will build on the idea of using digital puzzles as a way to reproduce scarcity, and on the importance of a supply-control mechanism to grant some hardness to digital money, to explore concepts of proving ownership through signatures and scripts, and the technique known as CoinJoin.

Proving Ownership: Signatures

Our Plan ₿ for money brings us, for the second time, to focus on the topic of people and the question "Who?" You established the conditions for the issuance of new sats, but what about their transfer? Who is authorized to change the data in the shared balance sheet, transferring ownership? If there was a central authority in charge of reassigning sats, following instructions by current owners (maybe logged in to the system with the classical username-and-password approach, like in your previous e-gold experiment), there would be a Mallory-vulnerable single point of failure again: Why then even bother moving from physical gold to PoW-based "digital scarcity"? If, on the other hand, each user had an equal right to reassign ownership, then your system could not work at all: Everybody would be encouraged to continuously assign other people's sats to themselves. You need some kind of consistent authority-defining protocol, which everybody could independently check. The solution is a cryptographic technique called a "digital signature." It works like this: First, Alice chooses a random number called a "private key," which she will keep absolutely secret. Then, she passes this number through a special mathematical function, easy to apply in one direction but practically impossible to reverse. The result is another number called a "public key," which Alice doesn't keep secret at all: Instead, she makes sure that Bob gets to know it. Finally, she passes the private key and the message through a

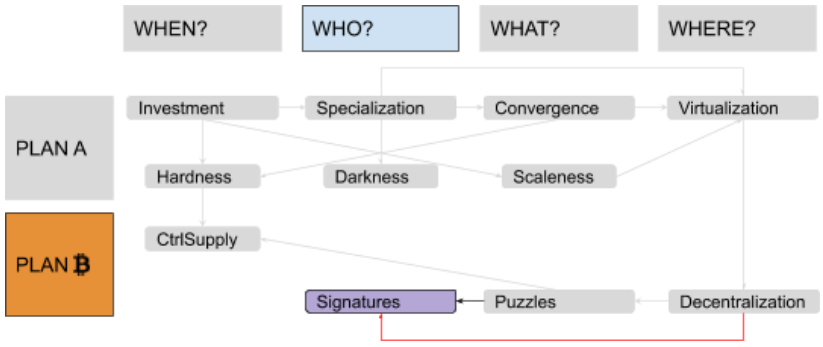
second function, again difficult to reverse, which results in a very big number called a "signature." A third and last mathematical function can be applied by Bob to the message, the signature and Alice's public key, resulting in a positive or negative verification. If the result is positive, he can be sure that Alice authorized that message ("authentication"), that she will not be able to later deny that authorization ("non-repudiation") and that the message was not altered in transit ("integrity").



In a way, it's similar to handwritten signatures (thus the name), which are easy for everybody to check against some public sample, but difficult to reproduce without being the owner of the "correct hand." Or to wax seals: easy for everybody to check against a public seal registry, but difficult to reproduce without the correct wax stencil. So, you change your protocol in order to make fractions of proofs of work independently reusable via digital signatures. The first model you implement is trivial: Each user independently generates a private key and creates a public "account," labeled with the corresponding public key. When users want to transfer ownership, they create a message including their account, the receiving account and the amount of sats they want to transfer. Then, they digitally sign and broadcast the message, which everybody can verify. Interestingly enough, a similar scheme can be used by many renowned (yet possibly pseudonymous) developers to sign different versions of your software so that they can freely change, improve, fix, update, audit and review it, and any final user of your system can independently verify said signatures before running their preferred version, leveraging a network of minimized and fragmented trust, without a need for a single authority to centrally distribute the software. This process enables a true decentralization of code.

Script and "Smart Contracts"

You don't want to limit the conditions that every peer has to check, before accepting any change in the shared balance sheet, to mere digital-signature validity, though. You decide that each message can also include a "script":



a list of instructions describing additional conditions that the receiving account (or accounts) will have to satisfy in order to spend again. For example, the sender could require a combination of several secret keys (in conjunction or disjunction) or a specific waiting time before spending. Starting from these very simple (and easy to audit) primitives, complex "smart contracts" can be built, making money effectively "programmable," even in the absence of central parties.

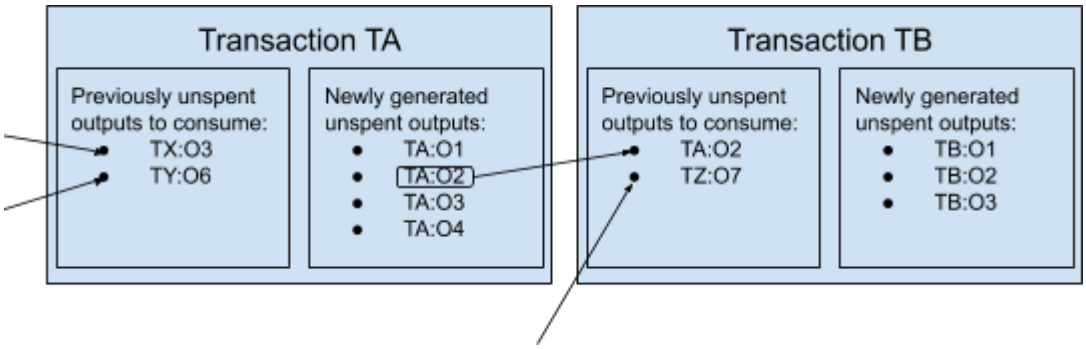
Darkness (and Scaleness) Problems

Unlike an encrypted messaging system (where if Alice sends Bob some messages, only Bob can read them), your scheme isn't really optimized for darkness (if Alice sends Bob sats, her message will have to be revealed beyond Bob — at the very least to those who will receive those same sats later on). Money circulates. Payees cannot trust any money transfer, even if properly signed, if they cannot verify that the transferred sats have actually been transferred themselves to that specific payer, and so on, upstream, back to the very first PoW-based issuance. With enough circulation of sats, active peers would get to know a huge number of past transactions, and forensic analysis techniques could be employed to statistically correlate amounts, timings, metadata and accounts, thereby deanonymizing many users and stripping them of their deniability. This is problematic: As discussed in Part 2, darkness is a fundamental quality for money, both for economical and sociological reasons. Smart contracts make this problem even worse, since particular spending conditions may be used to identify particular software implementations or specific organization policies. This lack of darkness is more serious than the one that affected your previous e-gold experiment: It's true that, back then, you stored most transaction metadata on your central servers, but at least it was only you, as opposed to quite literally anybody (including many of Mallory's agents), who had access! Furthermore, you could implement some particularly advanced cryptographic strategy to make yourself at least partially "blind" to what was actually going on between your users. There's also a minor scaleness problem connected with this design: Digital signatures are quite big, and the chain of transfers that a payee needs to receive in order to validate everything would include many signatures, making validation potentially more expensive. Furthermore, account changes are quite difficult to validate in parallel.

A New Paradigm: "CoinJoin"

To mitigate such problems, you decide to change the fundamental entities of your model from bank-like "accounts" to "Unspent Transaction Outputs" (UTXOs). Instead of instructions to move sats from one account to another, each message now includes a list of old UTXOs, coming from past transactions and "consumed" as ingredients, and a list of new UTXOs,

"generated" as products and ready for future transactions. Instead of publishing a single, static public key to be used as general account reference (like a bank IBAN or an email address), Bob must provide new, single-use public keys for each payment he wants to receive. When Alice pays him, she signs a message that "unlocks" some sats from some previously created UTXO, and "locks" them again into some new UTXO.



Just like with physical cash, spendable bills don't always match payment requests — change is often required. If, for example, Alice wants to pay 1,000 sats to Bob, but she only controls several UTXOs locking 700 sats each, she will sign a transaction consuming two of those 700-sats UTXOs (unlocking a total amount of 1,400 sats) and generating two new UTXOs: one associated with Bob's keys, locking the payment (1,000 sats), and the other associated with Alice's keys, locking the change (400 sats). Provided that people don't reuse keys for different payments, this design increases darkness in and of itself. But even more so when your users start to realize that UTXOs consumed and generated by a single transaction don't have to come from just two entities! Alice can create a message spending old UTXOs she controls and generating new UTXOs (associated with Bob), then she can pass said message to Carol, who can simply add her old UTXOs she wants to consume and the new UTXOs (associated with Daniel) she wants to create. Finally, Alice and Carol both sign and broadcast the composite message (paying both Bob and Daniel). This special use of the UTXO model is called "CoinJoin." (Trigger warning: Within the actual Bitcoin history, this use wasn't Satoshi's design rationale for the UTXO model itself, but was discovered as a potential twist on said design by other developers, many years after the launch.) It breaks the statistical linkability between outputs, while preserving what is called "atomicity": Transactions are either entirely valid or invalid, thus Alice and Carol don't have to trust each other. (If one of them tries to alter a partially signed message before adding their own signature, the existent signature becomes invalid.)

There is a possible change to your system that may actually improve the situation even more: a different digital-signature scheme, alternative to the one you're using now, which is "linear in the signatures." That means: In taking two private keys (which are nothing but two numbers), signing the same message with each and adding together the resulting signatures (which also are nothing but two very big numbers), the result happens to be the correct signature corresponding to the sum of the two public keys associated with the two initial private keys! This sounds convoluted, but the implication is simple: Alice and Carol, when CoinJoining, could add up their individual signatures and broadcast just the sum, which everybody could verify against the sum of their public keys! Since, as we said, signatures are the "heaviest" part of transactions, the possibility of broadcasting just one instead of many would save up a lot of resources. External observers would end up suspecting every transaction of being a CoinJoin, since many users could be after efficiency gains. This assumption would break most of the forensic heuristics.

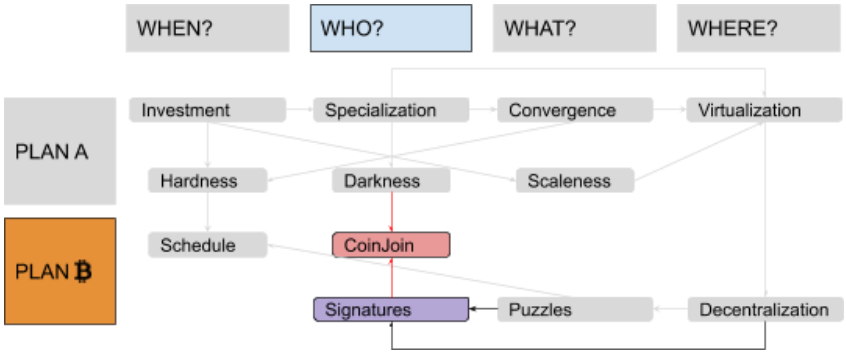
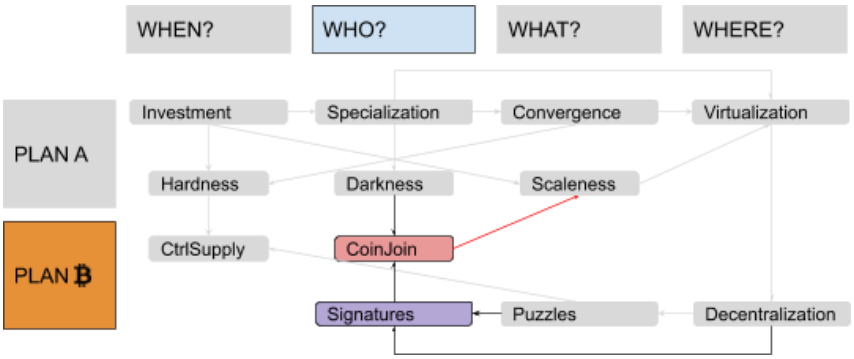


Image courtesy of CryptoScamHub

Even without this further improvement, the UTXO model already somehow increases scaleness: Unlike state changes in the account model, it allows validation to be efficiently batched and parallelized.

So far, you've learned:

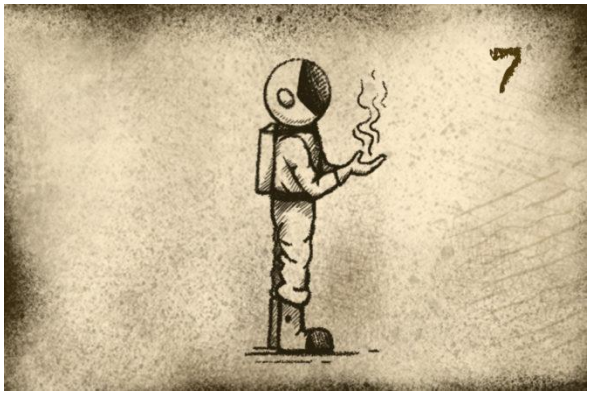
- that you can decentralize ownership using digital signatures for transfer;
- that you can turn transactions into programmable "contracts" with a script system; and



- that a more complex paradigm called CoinJoin can further increase darkness and scaleness.

But now that your users can issue sats and transfer them in a completely decentralized way, how can they all be sure that a single chronology is followed, preventing double-spending attacks or attempts to tinker with the inflation schedule? We will answer that in our final installment, "Discovering Bitcoin Part 7: The Missing Pieces."

Discovering Bitcoin Part 7: The Missing Pieces



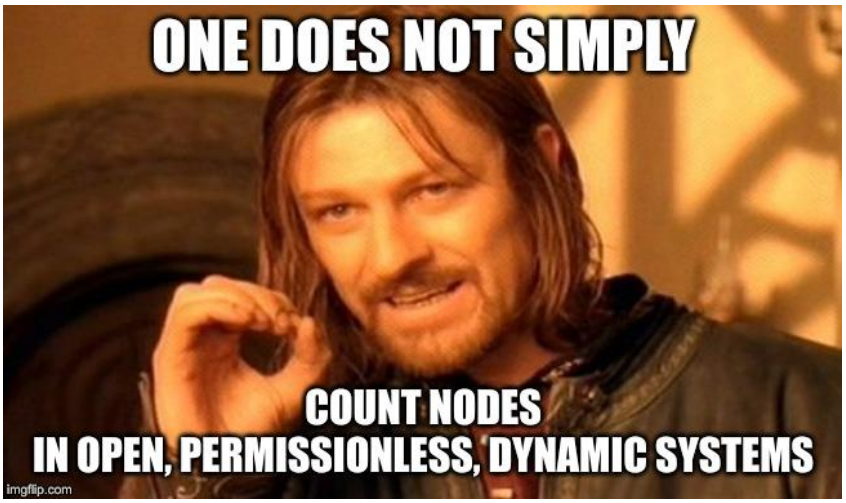
This is the seventh and final installment of bitcoiner Giacomo Zucco's series "Discovering Bitcoin: A Brief Overview From Cavemen to the Lightning Network." Read the Introduction to his series, Discovering Bitcoin Part 1: About Time, Discovering Bitcoin Part 2: About People, Discovering Bitcoin Part 3: Introducing Money, Discovering Bitcoin Part 4: A Wrong Turn (New Plan Needed)!, Discovering Bitcoin Part 5: Digital Scarcity and Discovering Bitcoin Part 6: Digital Contracts. As we conclude our "Discovering Bitcoin" series, we will build on the use of digital signatures and of the CoinJoin paradigm to explore concepts of unique chronology, mining fees and off-chain transactions.

Proving Unicity: Timechain

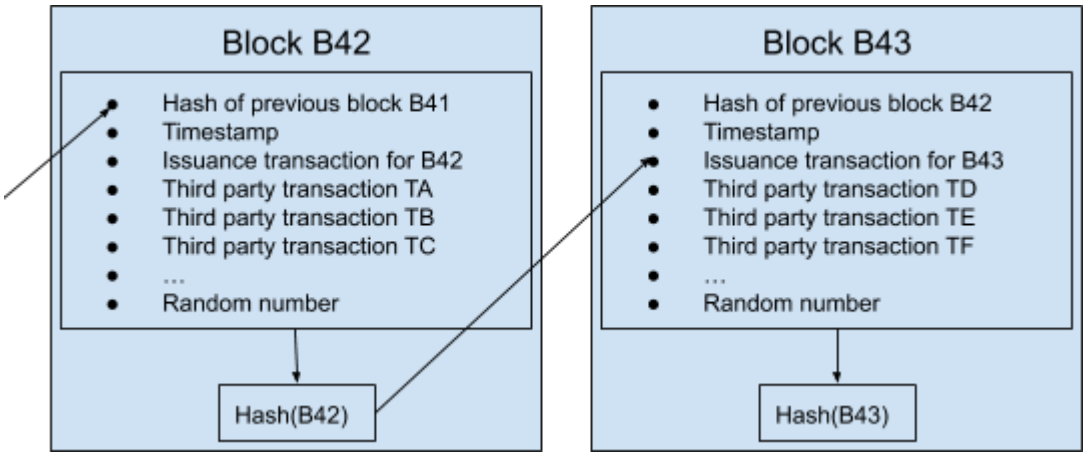
We are finally at the end of our exploration of Plan ₿, back again to the question "When?" from whence we started. It's an important question, as it justifies the introduction of the so-called "blockchain technology," a decidedly abused expression that, in its original meaning, just labeled the answer to a problem of unique chronology. (It's interesting, in this regard, that Satoshi himself called this structure "timechain," which is also the term we are going to use here … sorry, Peter!).

Let's try to understand what problem it solves, by getting back to our little story. You designed a digital cash system in which issuance and ownership are both decentralized, leveraging puzzles and signatures in a clever combination. But how do you prevent users from double-spending the same UTXO? If Carol, a dishonest user, transfers sats to an address controlled by

Daniel, and then signs another transaction that retransmits those very same sats to an address controlled by herself, which transaction will the network enforce? They would both be "valid" from the point of view of the chain of signatures and scripts, and both would point to a valid initial issuance, with a correct PoW difficulty. And how do you prevent "miners" from lying about the correct timestamp, tricking the difficulty adjustment algorithm to increase the issuance rate? If the miner Minnie manages to solve hundreds of PoW puzzles at low difficulty, but she includes forged timestamps that depict the solutions as only 10 minutes apart from each other, how can a generic user, maybe just recently connected to the system, discover and prove such dishonest behavior? Within your previous e-gold experiment, your trusted timestamp server trivially solved both issues. But now there is no central server, so who defines the unique chronology of events? If the network could somehow "vote," it could reach a "democratic" consensus about it. But voting processes, while feasible in systems with a fixed number of known actors (often called "federations"), can't work within dynamic sets of unknown, anonymous actors. You can't simply use "node count" as a proxy for voting rights, since every user could pretend to "be" millions of different nodes in what is known as a "Sybil attack." You need another, "Sybil-resistant" way to push all the nodes to find (and keep) consensus over one single, consistent, immutable history.

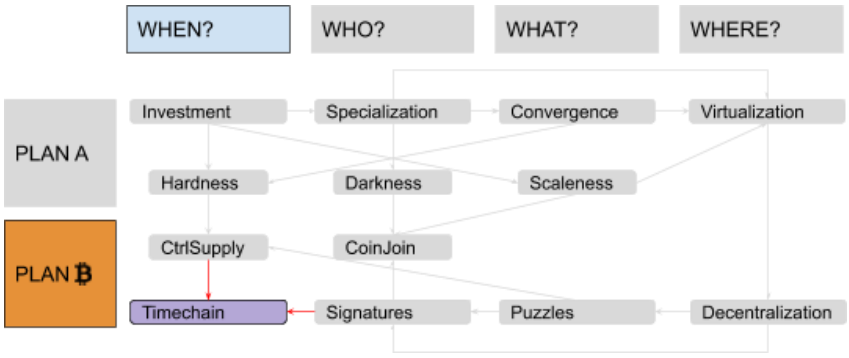


Unfortunately, a deterministic and final solution based on mathematics is theoretically impossible. But a statistical and asymptotic solution based on economics is practically possible, and you are smart enough to find it. This is the idea: Every time miners try to solve PoW puzzles, they should include in their messages compact snapshots of the current transactional timeline! Instead of just their issuance messages, they should pass through the hash function more complex "blocks" of information, each containing (along with said issuance message, a timestamp and a random number needed to solve the puzzle at the correct difficulty) the solution of the previous block (which had been found by other miners about 10 minutes before) and a list of transactions recently made by other users.



A block that contains transactions already included in previous blocks is considered invalid. A block carrying a timestamp that is significantly incompatible with the previous ones is also discharged. Using this trick, all actors are incentivized to converge on a consistent version of the same chronology. Minnie *could* include a valid transaction contradicting (double-spending) a previously confirmed one, or alter the timestamp to trick the difficulty adjustment, but then other nodes would reject such a block, and she would lose the value of the new issuance, having wasted time and energy for nothing. Miners spend money to solve puzzles, and thus it's quite safe to assume they want to enjoy the associated rewards, creating blocks that aren't rejected, at least in scenarios where they only follow financial incentives endogenous to the system.

Mining Fees

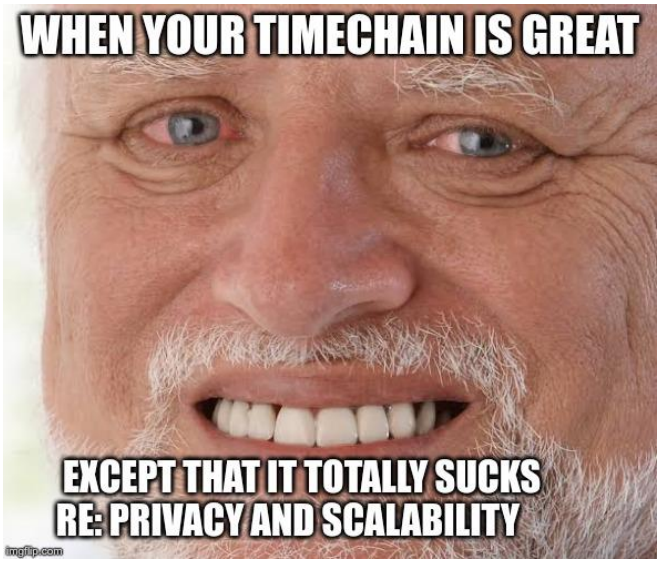


This solution, while brilliant, still lacks incentives for miners to include other people's transactions. They could just opt to save the computing power needed to verify scripts and signatures (which, while not being as much as the one needed for hash collision, is still relevant) and to include only their own valid issuances in otherwise empty blocks. Also, the diminishing amount of sats allowed in such issuances, due to the controlled-supply paradigm, would reduce (even discounting for an increase in sats' purchasing power) the incentive to solve blocks at all, eventually canceling it completely at the end of the last era, when there will be no inflation. You solve this problem by introducing "mining fees": a small "extra" that users can attach to their transactions to incentivize miners to include them. It works like this: The system allows

miners to include in their reward transactions, along with the issuance of newly "minted" sats (compatible with the current era), also the difference in sats between created and consumed UTXOs of all the valid transactions included in the block. Fees never depend on the amount transacted, but only on the transaction size (script complexity, number of signatures, etc.) and the desired priority within blocks.

Scaleness (and Darkness) Problems

The minimum mining fee necessary for a transaction to be included in a block fluctuates depending on supply and demand of "block space." On the supply side, the number of transactions that can be added to the timechain are limited by a maximum block size (less than 4 megabytes for each block) and a maximum block rate (about one every 10 minutes). On the demand side, each user has different constraints and preferences (some can wait more to pay less, some can pay more to wait less, some use wallets with excellent dynamic fee estimation, some don't). In general, a rising demand for block space would imply a rise in mining fees. This clearly limits the scaleness of the system (in particular, since miner fees are independent from the amount of value transferred, we could say that it actually reduces divisibility). More, in general, using a timechain implies that every node in the network must forever keep track of everything: Every single on-chain transaction must be downloaded and verified by every actor who will use the system for its entire history, even far into the future. Such a system is clearly not scalable. It also lacks darkness, since everyone has to keep a copy of every transaction forever, enabling any kind of forensic analysis and deanonymization attempt.

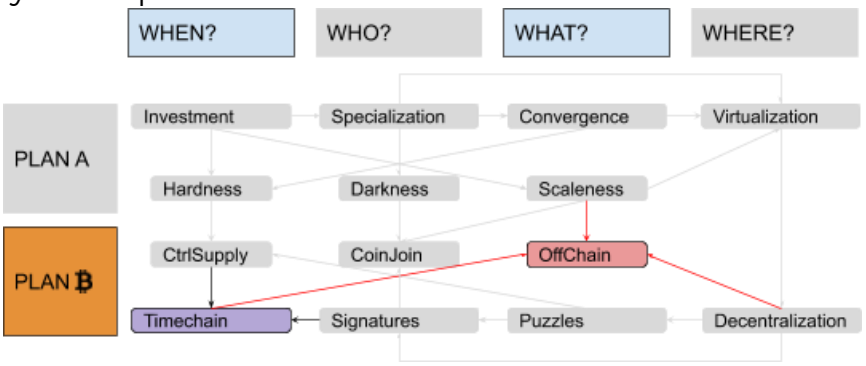


It would be possible to make the situation look better for some users, at the cost of creating another more "privileged" class of users. For example, if you increase the size and frequency of blocks, then the block-space supply increases, and its price decreases. But the cost of running nodes, with the ability to independently verify the validity of transactions and blocks, increases way faster than said supply, centralizing the topology of the entire system. Sure, a new class of specialized nodes could serve as some kind of "signed message" to inferior, non-validating users, giving them some guarantee that a transaction is valid. After

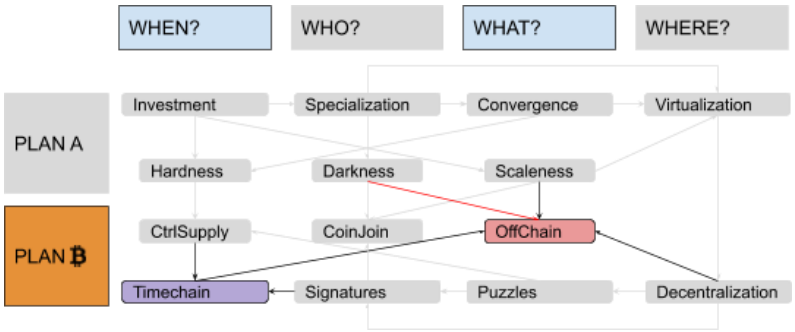
all, coinage was introduced in order to delegate to a few specialized trusted entities the expensive task of verifying precious metal coins. But, just like coinage, this strategy (knowns as "SPV") implies a strong centralization, with all the attached risks of political interference or censorship by the likes of Mallory.

A New Paradigm: "Off-Chain"

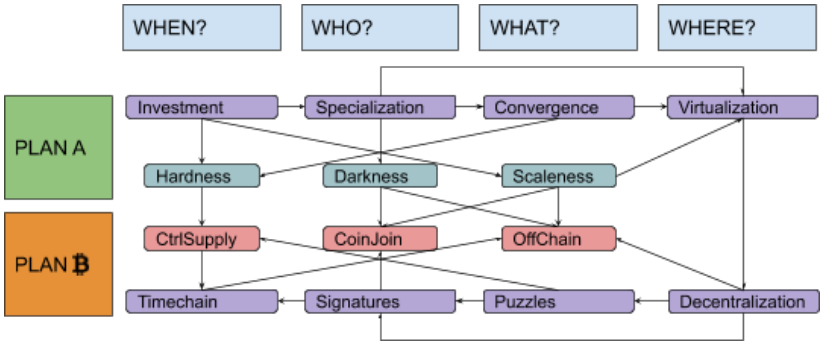
There's a smart way to mitigate the fundamental scaleness limits of global consensus systems without sacrificing its decentralization. We will call it the "off-chain paradigm." The idea is simple: Just refrain from committing every transaction to a block until it's strictly necessary, keeping most of the traffic off the public timechain (with its expensive global consensus) and only using it for conflict resolution and periodic settlement. This evolution is similar to the way people use courts and contracts in common-law systems: Courts can create publicly binding precedents, reaching some sort of "legal global consensus," but they are comparatively slow and expensive, so most trading parties usually only sign private bidirectional contracts, asking courts to verify and enforce them only when conflicts arise or when some periodic settlement is due. Advanced smart contracts could be used to make this kind of "recourse" trust-minimized: Unlike an actual legal system, the decentralized timechain could avoid human bias and corruption, relying mostly on cryptography and code. Unlike the credit certificates discussed in the context of virtualization, off-chain transactions are not "virtual"; they are actual valid transactions, with high probability of being enforced by the system regardless of the honesty of the parties involved.



You soon realize that this kind of paradigm could highly improve the darkness of your system as well. Instead of having all the nodes registering all transactions forever, most of those transactions would be exchanged privately between the interested parties alone, making forensic analysis by malicious eavesdroppers harder, costlier, less complete and less reliable.



The main implementation of such a strategy is a secondary network of pre-funded, bilateral "payment channels" that can route transactions across many hops in a trust-minimized, atomic way. Users call it by a very poetic name: "the Lightning Network" (the acronym for which is often included in the label of the whole protocol suite of your system, named "LNP/BP" as analogous to the historical "TCP/IP"). But there are other minor instances of the same paradigm; for example, several techniques to keep the actual script off the timechain until needed, saving block space and privacy as well. (People call these techniques many strange names, like "Taproot," "Graftroot," "g*root," "Scriptless Script" and so on.)



With the introduction of these final pieces of technology, your users finally have everything they need to use the system in real life, in order to take back some of the most important features of money. Thank you, "Satoshi"!

Image courtesy of CryptoScamHub

You have come a long way since your early caveman innovations, far in the past. Now, only the future can tell us if this Plan ₿ of yours will work out. To the moon. *A final thank you to Nicki DiCicco for her cover art and to CryptoScamHub for his meme art contributions to this series!*

Tweetstorm: How to Outperform Bitcoin

By Michiel Lescrauwaet

Posted September 19, 2019

1/ "How to outperform Bitcoin" - a thread based on my recent presentation at #bh2019

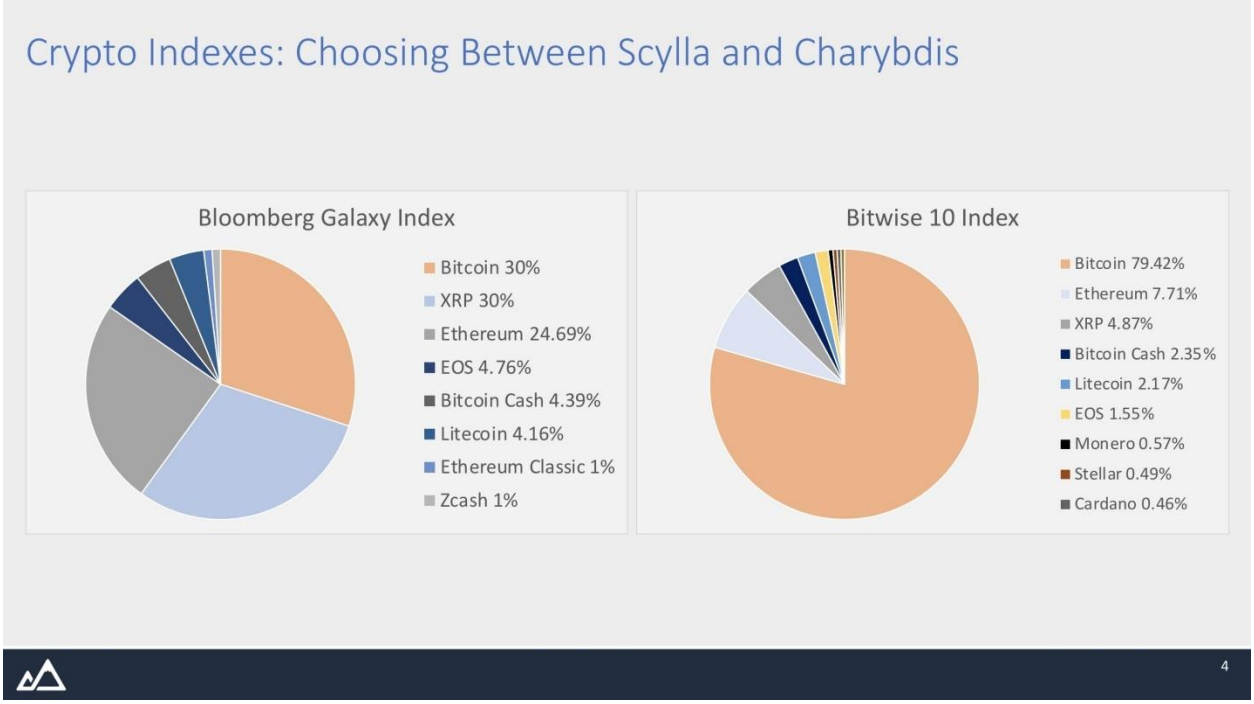
2/ We see 3 reasons why BTC should be the benchmark in crypto:

- a) Current portfolio indices are flawed and won't stand the test of time
- b) BTC is way ahead of its competition to become a monetary standard
- c) It helps investors think in the right direction

3/ Imo crypto indices are DOA:

The Bloomberg Galaxy Index is a subjective mix of heterogeneous assets: no rational justification for the weightings.

For Bitwise 10 the question becomes: why include Bitcoin at all? Analogous to adding 80% AMZN to a junior index.



4/ We think Bitcoin stands on its own as digital gold and should not be mixed with experimental altcoins:

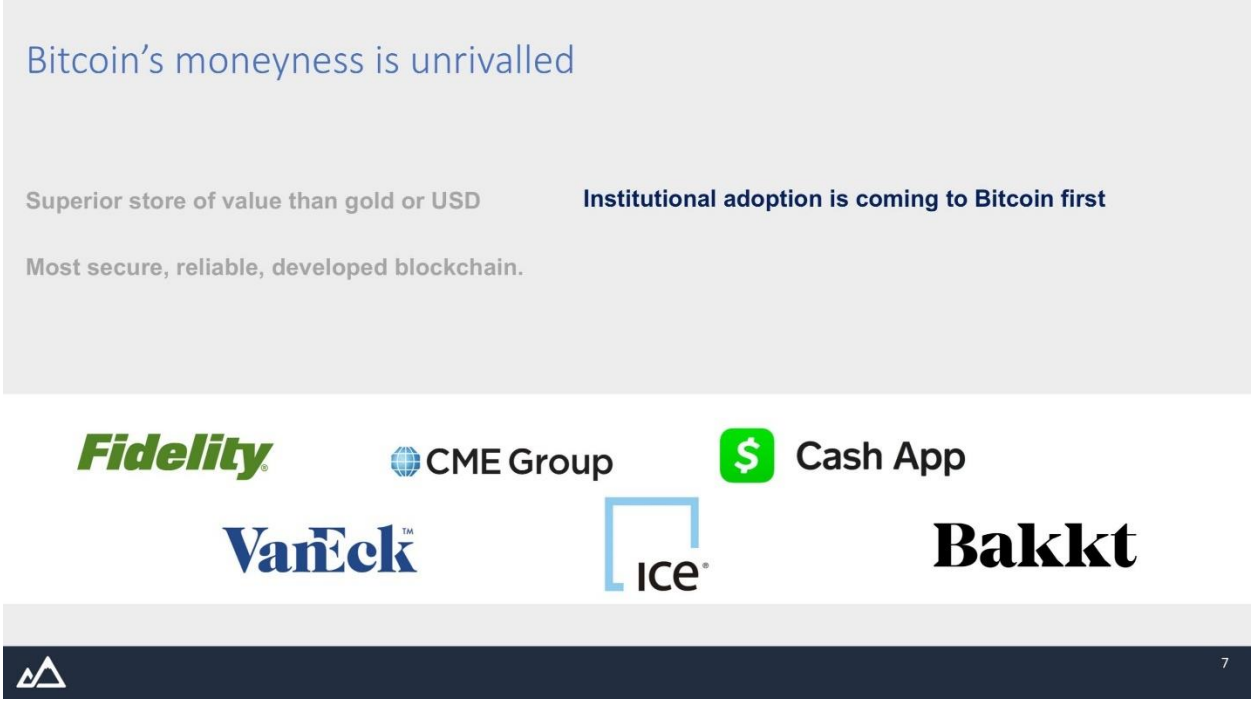
"Diversification is a security against ignorance. It makes little sense if you know what you're doing" - Warren Buffett

5/ When we look at proxies for moneyness, Bitcoin performs at least 10X better than the next 4 projects.

State of the networks (200 day average)	BTC	ETH	XRP	LTC	BCH	Average BTC multiple
Transaction fees	$626,000	$99,437	$560	$1590	$219	25X
51% attack cost/day	$ 24 million	$ 2.9 million	NaN	$ 0.58 million	$ 0.66 million	17.4X
Current market cap	$181 billion	$29 billion	$11 billion	$ 4billion	$5 billion	15.4X
Realized value	$85 billion	NaN	NaN	$ 4 billion	$ 5 billion	NaN
On-chain tx value	$6.25 billion	$541 million	$175 million	$ 262 million	$ 1.17 billion	11.6X

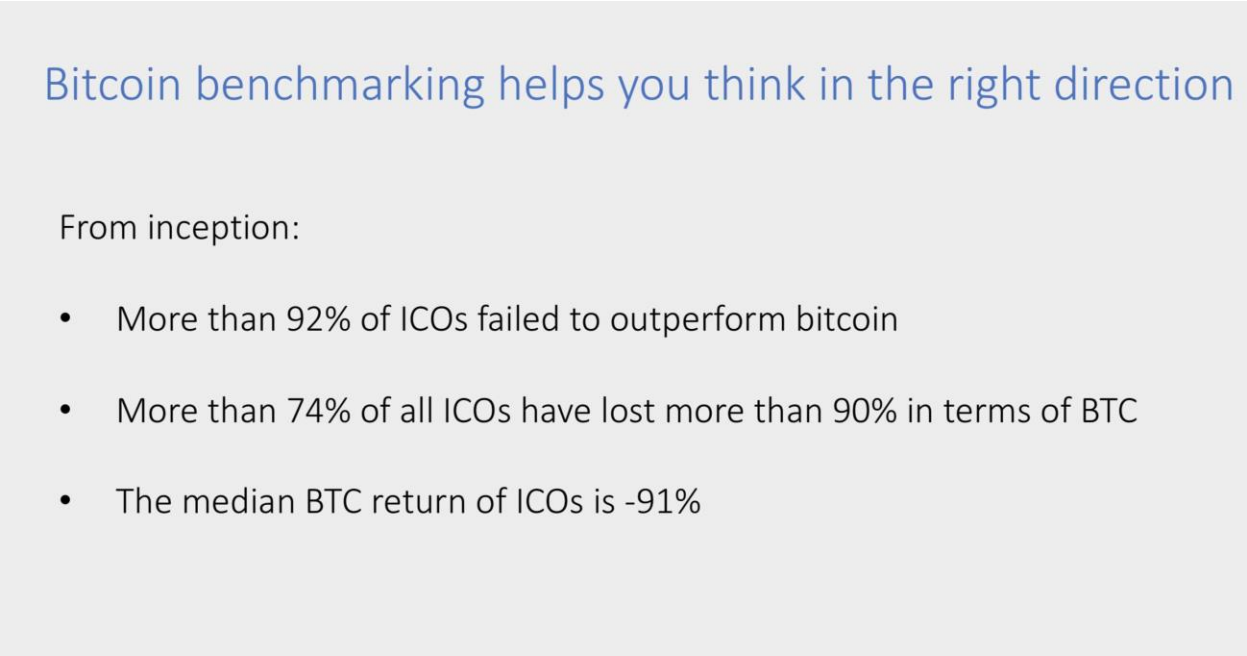
6/ Institutions are coming - and they're coming to Bitcoin first.

This shouldn't be a surprise: they have a long-term mindset and a reputation to uphold.



7/ The opportunity cost of selling BTC is huge & long-term it's hard for an asset to outperform BTC.

Not thinking in terms of Bitcoin can cost you a lot of bitcoins.



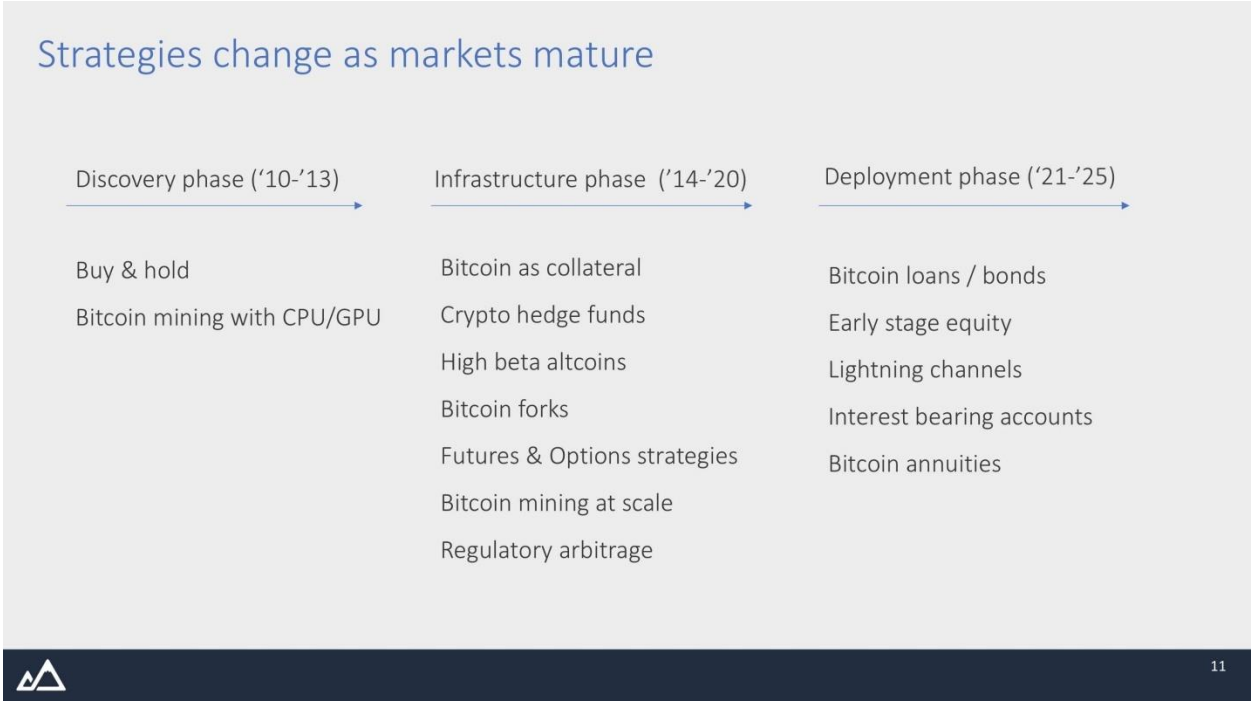
8/ If we accept that Bitcoin is the benchmark, the question that follows is: How to outperform Bitcoin?

Here are a few frameworks that helped us think about Bitcoin alpha.

9/ The risk/reward of each strategy depends on the maturity of the BTC ecosystem.

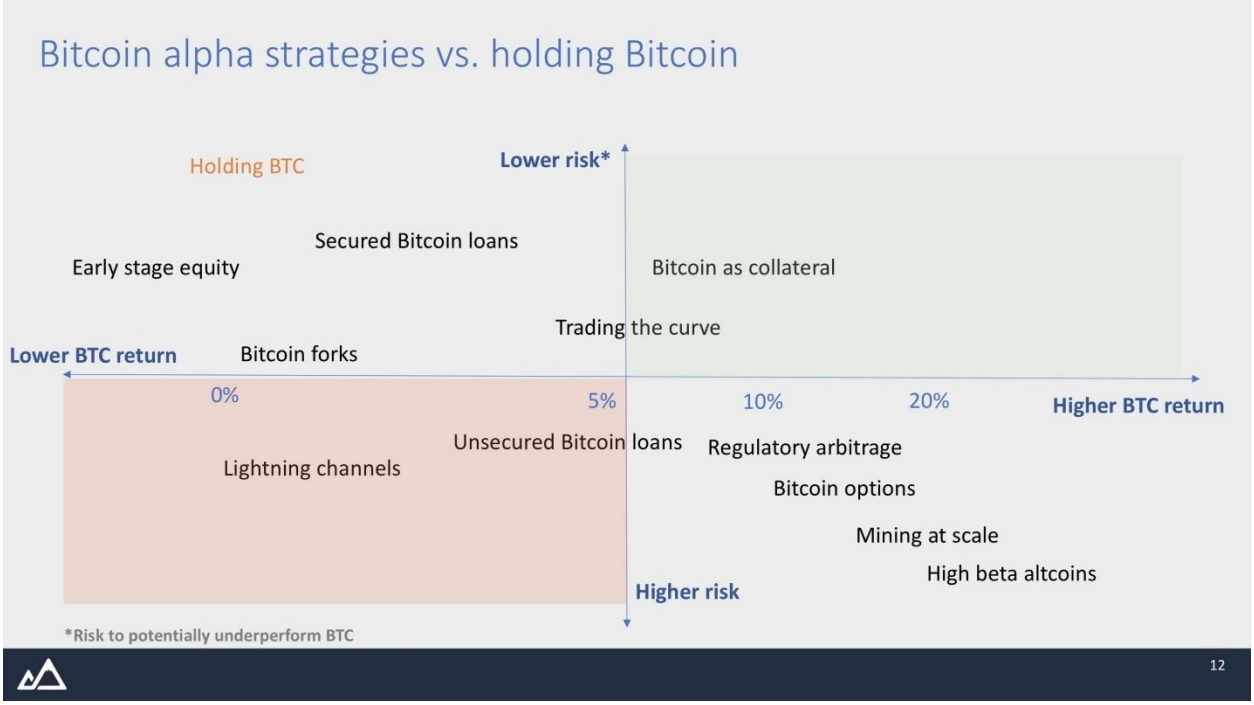
You could've gone levered long BTC on Bitcoinica in '11, but then lost everything in the bankruptcy.

At the same time, today it's too early to lock up you BTC in Lightning channels.

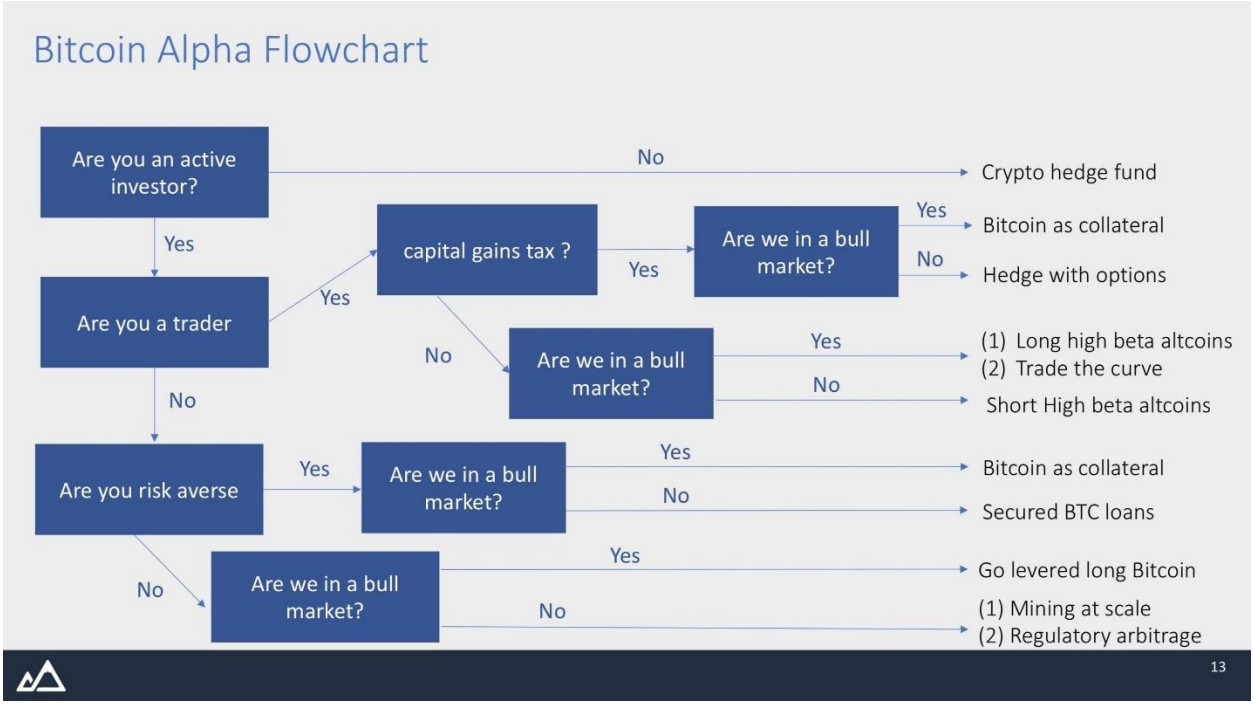


10/ Here is a suggested look at the risk/reward profile for every strategy (note that the positions depend to some extent on the skillset).

The take-away is that you want to identify a strategy that offers a relatively high return for a relatively low risk.



11/ Finally, context matters. It's important to ask the right questions, in the right order.



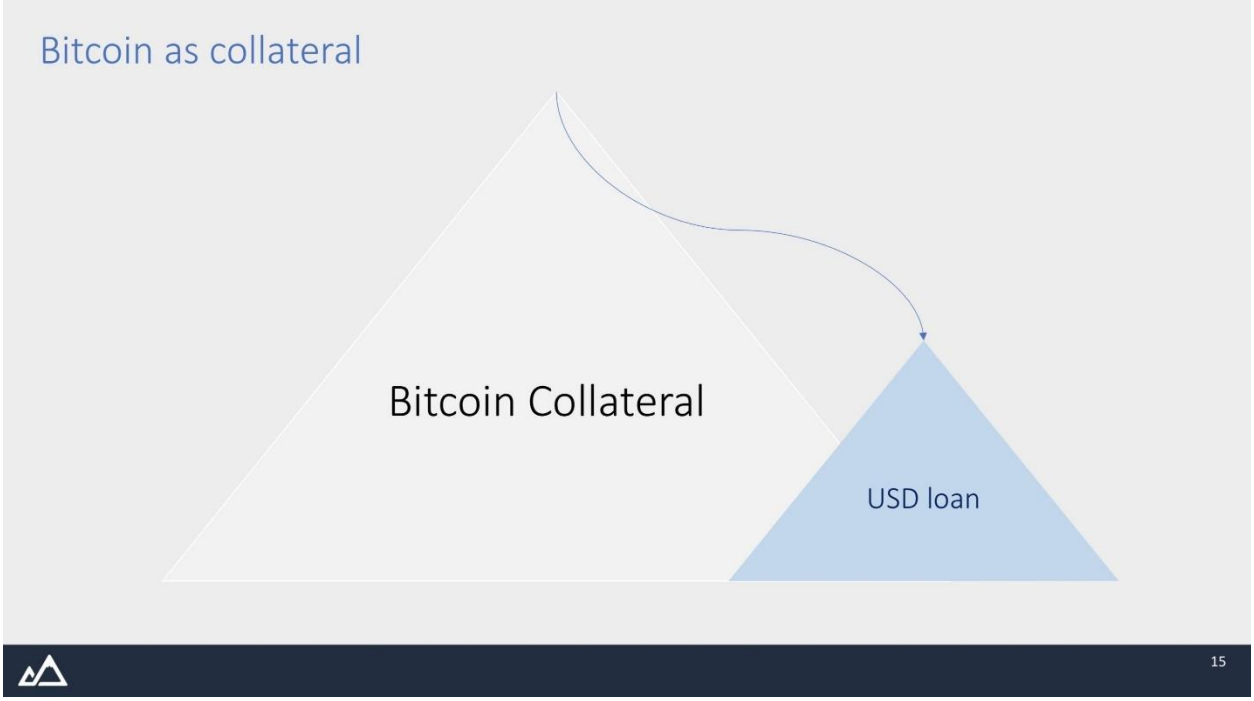
12/ Let's now look at a few strategies in more detail.

13/ If you're lending out your bitcoins, you will earn around 2.5% APR - the reason is that there's less demand for BTC borrowing in a bull market as shorting / hedging is less of a concern.

Keep in mind that counterparty risk is still material, esp. in a bull market.

14/ An alternative strategy is using Bitcoin as collateral to borrow extra USD, which is reinvested (leverage):

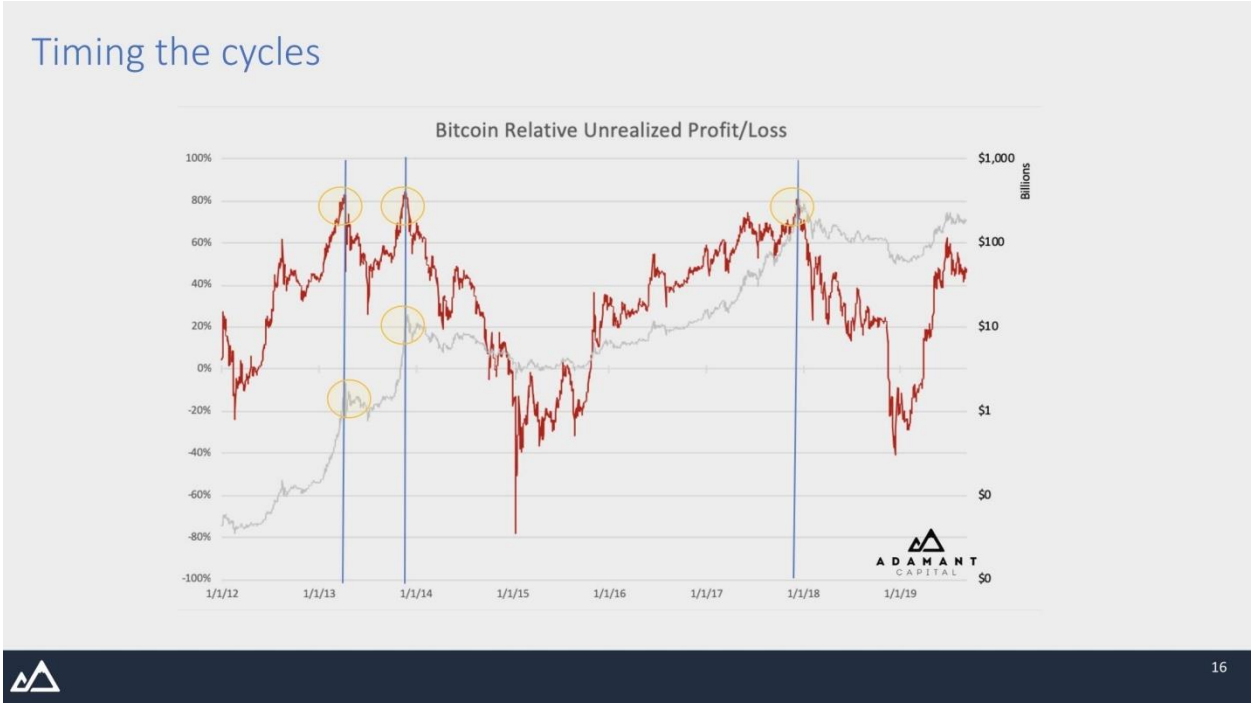
1. Flexibility to manage risk
2. Bitcoin is excellent collateral
3. Possibility for tax-efficiency.



15/ When levering up/down it's important to be able to time the cycles.

An indicator that we like is the Relative Unrealized P&L. It's a proxy for paper profits/losses.

We're at 40% now. Historically, 80% was an important level for a reversal in trend.



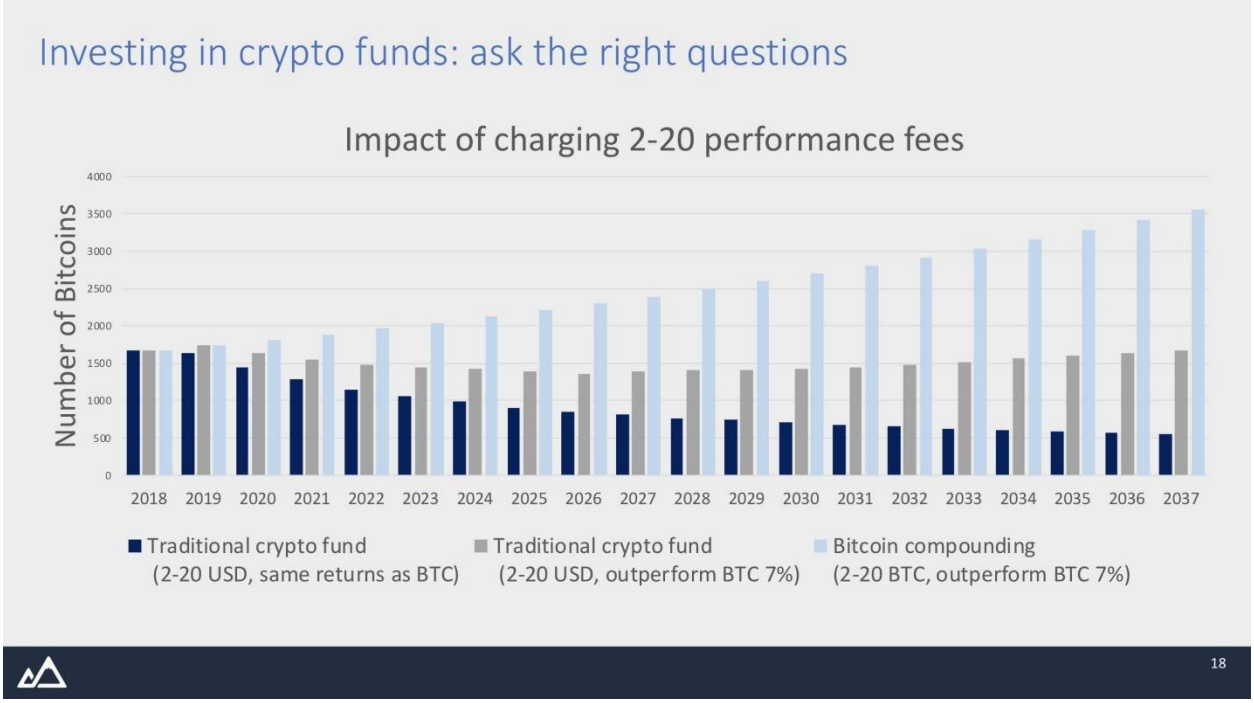
16/ When investing in crypto (hedge) funds, it's critical to ask the right questions:

1. What is the performance benchmark?
2. How much is committed by the GP?
3. Does the strategy align with my outlook?
4. What was the performance?
5. How are the fees structured?

17/ The fee structure is important because BTC tends to move up violently

Let's say you invest 100k (or 10 BTC), BTC does a 5x and the fund's return = BTC return. The fund charges 80k (20%), and you now have 420k instead of 500k when holding BTC.

Charging fees in BTC fixes this



/18 In conclusion, we believe that:

1. BTC as a benchmark is the future of crypto asset mgmt and those who adopt it early will benefit.
2. When pursuing BTC alpha, it's crucial to know how mature the market is, to know your skillset & ask the right questions.

Bitcoin's power oscillator

By Harold Christopher Burger

Posted September 20, 2019

Disclaimer: This article is not financial advice.

In the article "Bitcoin's natural long-term power-law corridor of growth", we looked at bitcoin's long-term price history and created a simple power-law based model to make predictions regarding bitcoin's future price developments. This article is based on the previous article, but attempts to answer a different question: Is bitcoin currently over- or under-priced?

Answering this question perfectly is impossible, as this would require perfect knowledge of future prices. Instead, we attempt to build a model that is intentionally as simple as possible, and requires no manually chosen parameters. Yet, it is able to indicate when bubbles burst with remarkable precision. It is also able to identify moments when bitcoin is unlikely to depreciate further and hence are good times to buy bitcoin.

We show with a simple financial simulation that the oscillator built in this article is indeed useful. However, this article should not be taken as financial advice. In fact, no single indicator should be used to inform a buy or sell decision, and the oscillator described in this article is no exception. The oscillator is certainly not perfect, but it is simple.

Simplicity is an achievement in itself. Having fewer parameters to play with makes it more difficult to "cheat" or to let the data tell the message one desires. Indeed, a model with more parameters is more prone to overfitting [1].

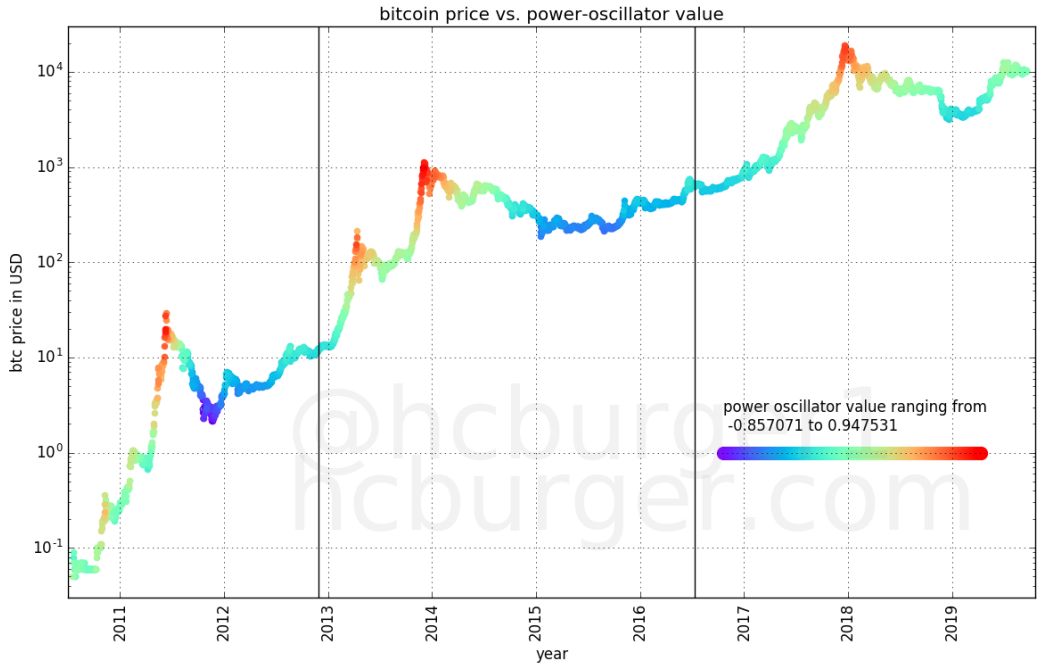
"With four parameters I can fit an elephant, and with five I can make him wiggle his trunk." — John von Neuman

Introduction

An oscillator is a tool for technical analysis which varies over time within a certain band [2]. The oscillator built in this article is built primarily for bitcoin and takes as input bitcoin's price history.

More precisely, the oscillator describes the log-price deviation between the current market price and the power-law fit from the beginning of bitcoin's history to the current point in time (we'll get into this later). The resulting oscillator looks like this:

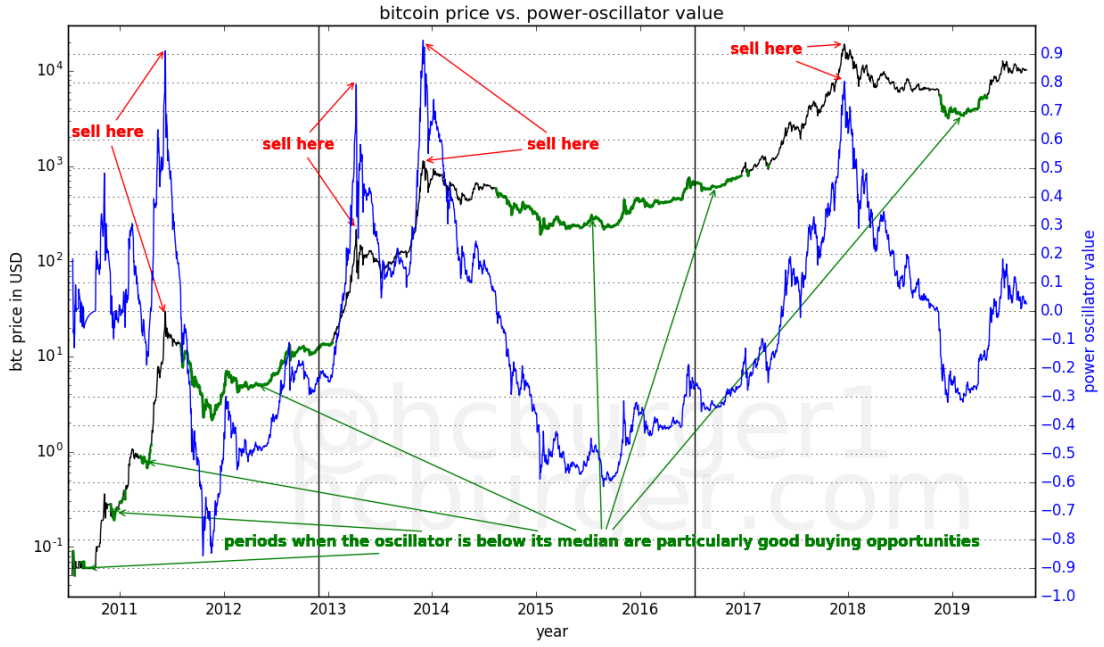
It moves approximately between -1 and 1 over time. If we color-code bitcoin's price history with the oscillator value at the same time, we get the following chart:



Market tops or all-time-highs coincide with high oscillator values perfectly. And market lulls coincide with lower oscillator values. Indeed, all four all-time-

highs were achieved in a narrow oscillator band. These bubbles popped shortly after reaching that band.

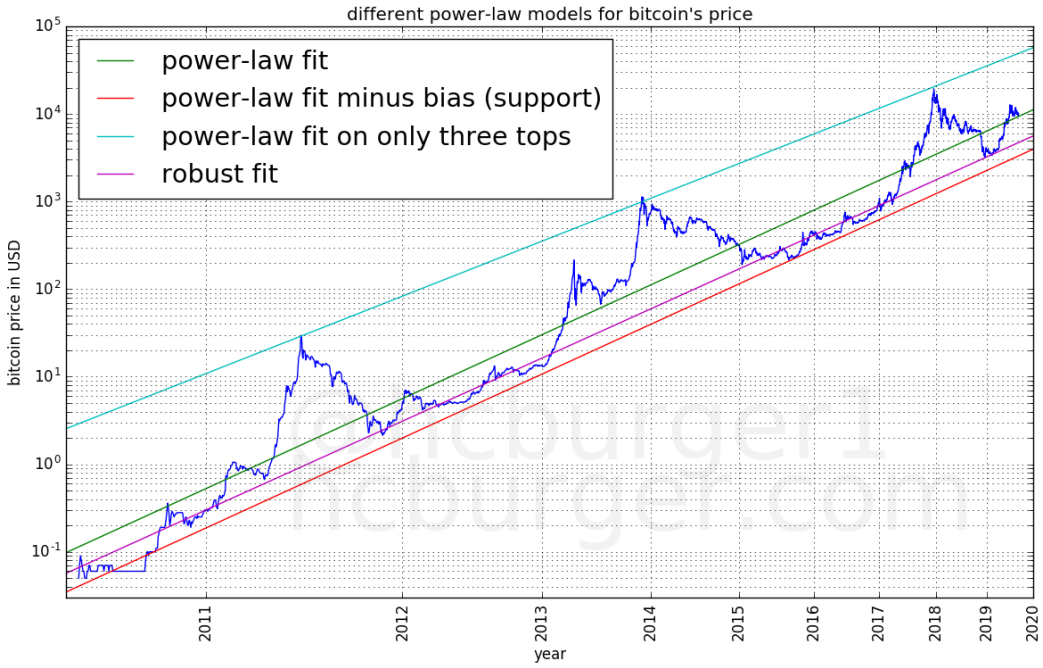
The green region describes the lower region in which the oscillator spends half its time. These moments can be considered to be particularly good times to buy bitcoin. The oscillator therefore recommends the following buying and selling strategy:



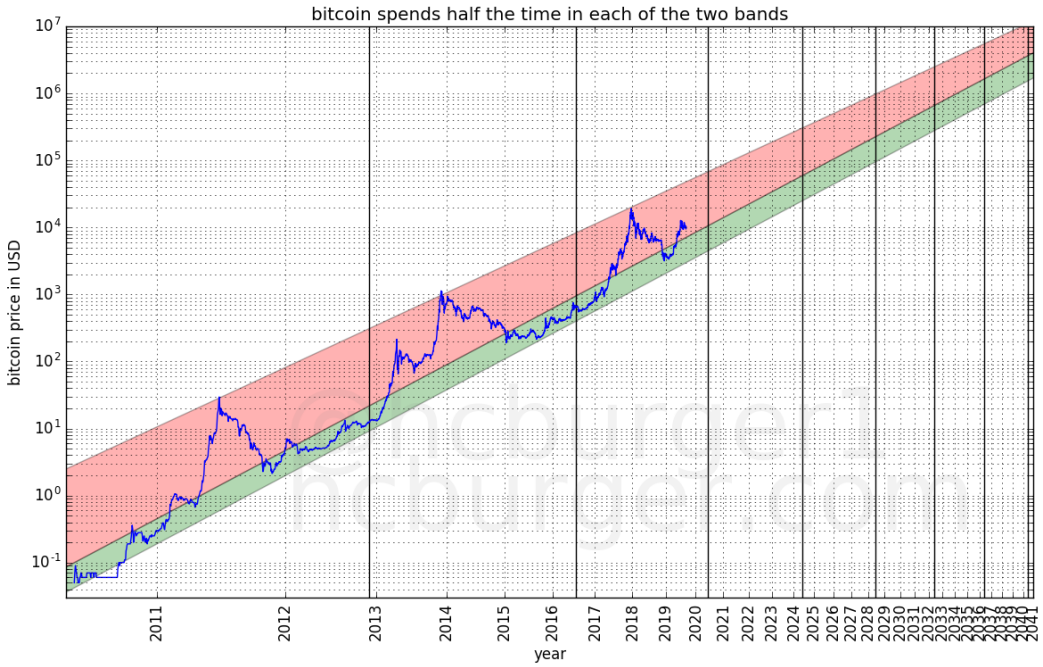
Even though these recommendations are not a perfect trading strategy, it is remarkable that the oscillator catches the market tops so well: All four all-time-highs are caught. The market lows are also caught quite well.

The power-law model

In the article "Bitcoin's natural long-term power-law corridor of growth", we have seen that bitcoin's price history looks very linear in a log-log plot [3]. The support line looks very linear, and three market tops also seem to lie a on a straight line. The overall price evolution also looks linear even though there is some volatility, and a robust fit yields similar results.



Straight lines in a log-log plot are in fact power-laws. Since the x-axis represents time, the power-laws are based on time. These lines can be projected into the future, leading to price predictions, which was the subject of the previous article:



What is interesting for this article is that the price moves within a corridor described by two power-laws. The intuition behind the oscillator described here is to look at where in the corridor the price is currently located.

The oscillator does not "cheat" because it only looks at the price information given at the time: it does not look into the future. This means that the oscillator value for the year 2014 does not assume knowledge of the bitcoin prices of 2015 for example.

Also, new market data does not change previously computed oscillator values. So no matter what the bitcoin prices will be in 2020 or beyond, the oscillator values that have already been computed will not change.

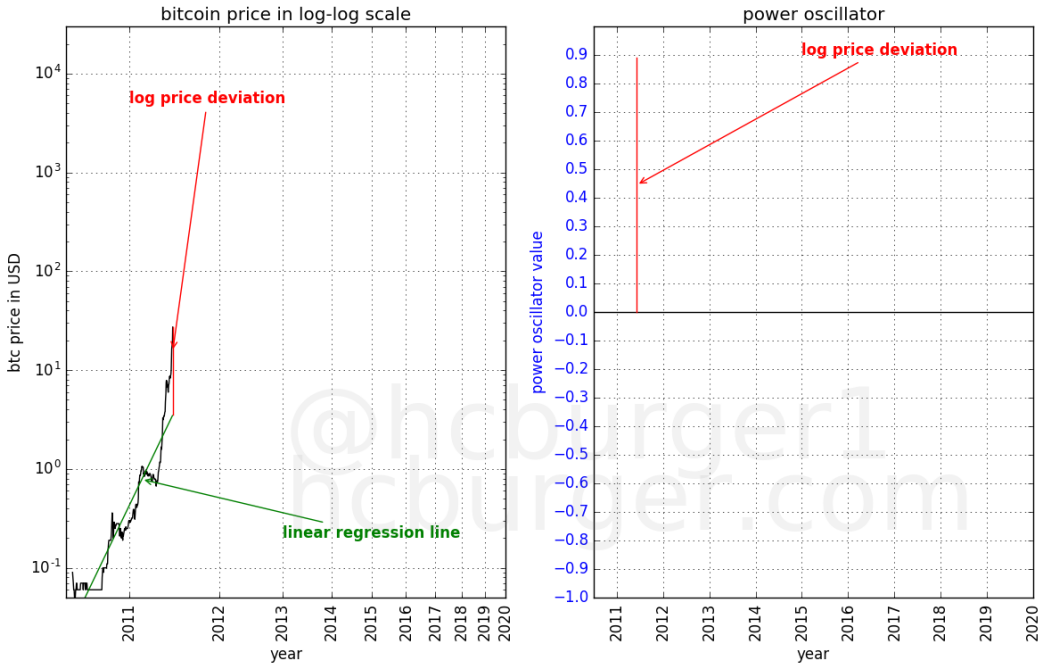
Since the oscillator is based on power-laws, we're going to call it the *power oscillator*.

How to compute the power oscillator

The power-oscillator is based on a linear regression of the price information in a log-log plot [4]. This is the same principle as was used in the previous article. The below plot on the left shows bitcoin's price history (in black) until the bubble of 2011, when it reached a price of approximately $30.

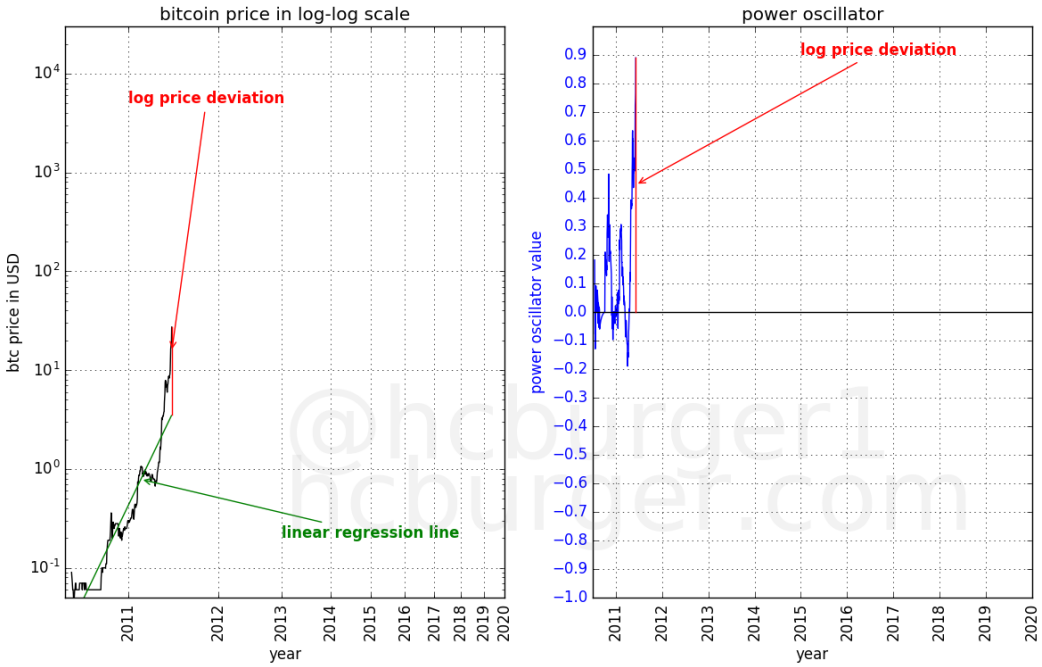
Linear regression is performed on this data, yielding the linear regression fit displayed in green. The deviation between the end of the price history and the end of the price fit is displayed in red: this is the log price deviation.

We take the length of this deviation and insert it into the plot on the right, for the same date. Since the actual price is above the price predicted by the linear regression fit, the deviation is positive:

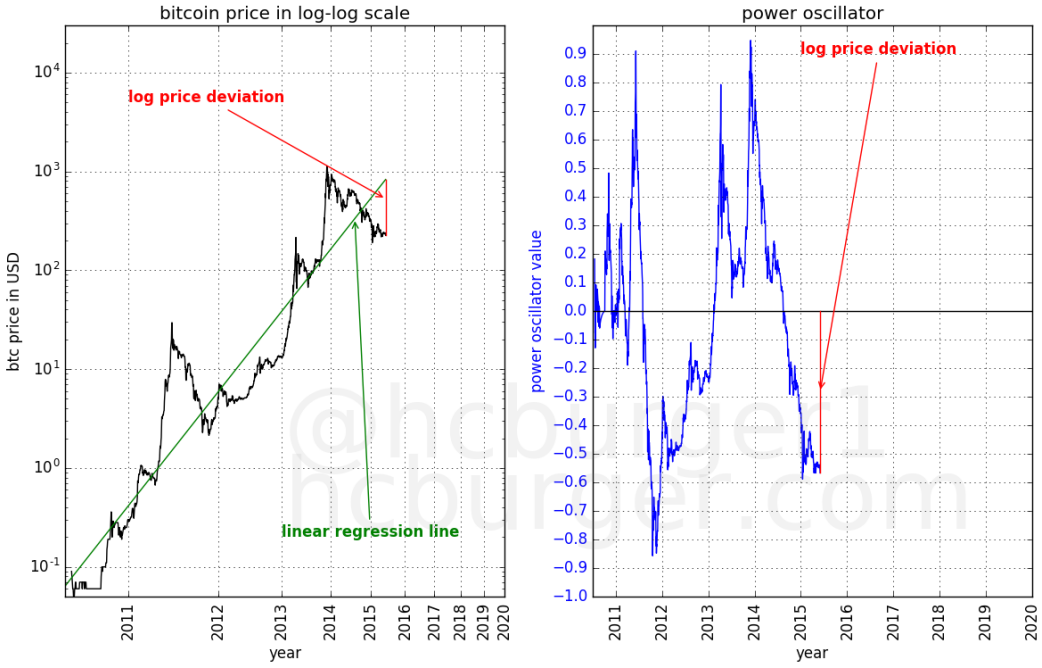


Note that only the price data available until 2011 is used. The regression is performed only on that data. Future prices are ignored because they are unknown.

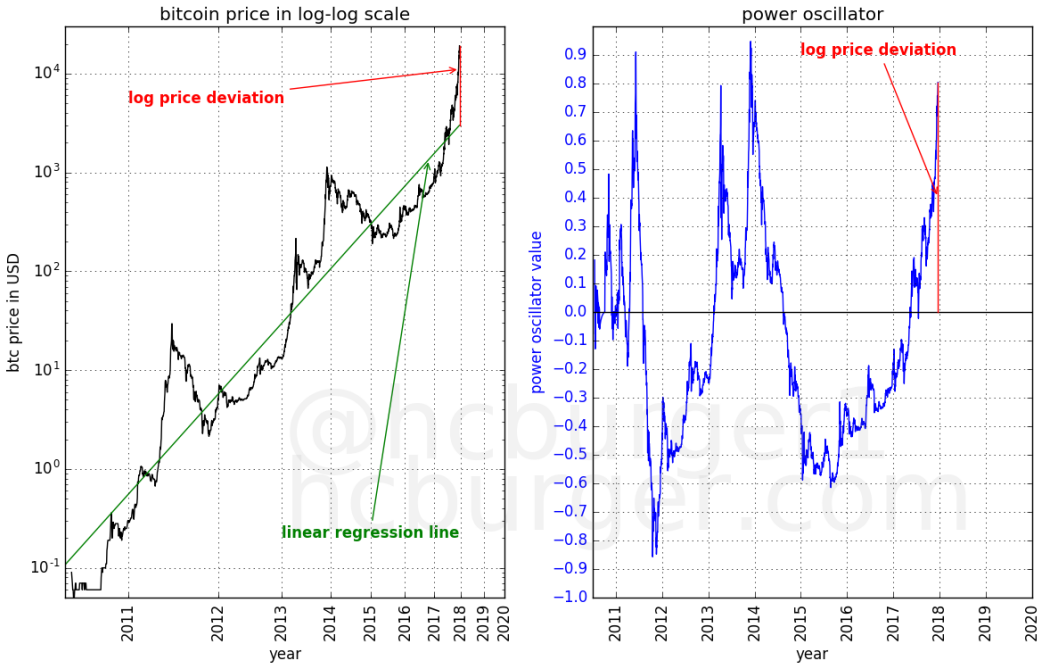
Had we performed the same procedure as above for each point in time until that date in 2011, and inserted a blue point in the graph for each log deviation, we would obtain the following figure:



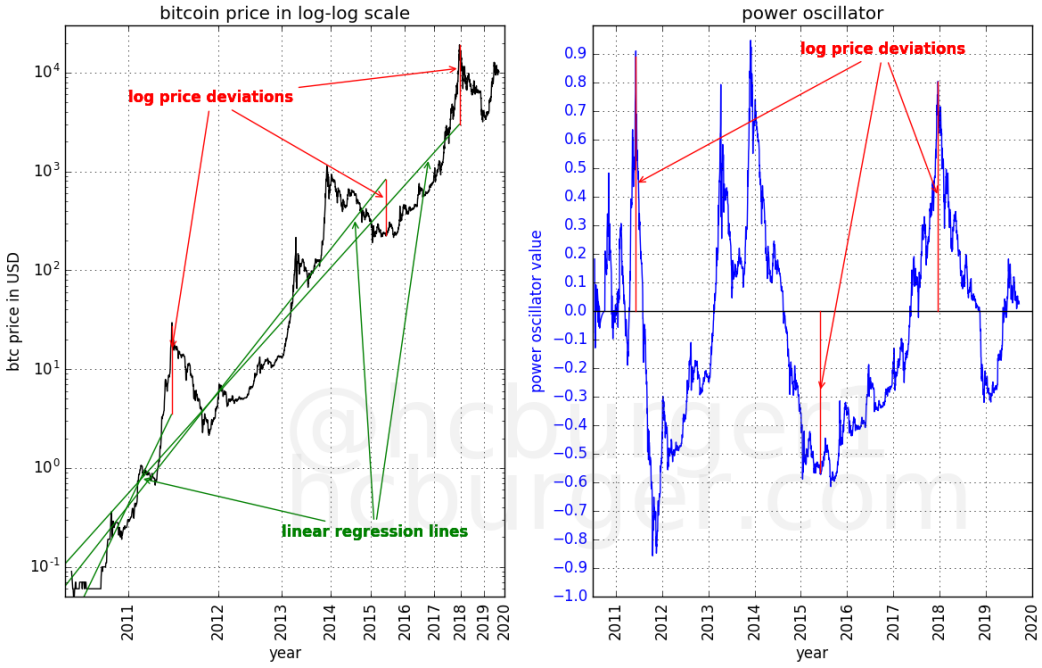
Let's continue in the same fashion until mid-2015. Here the log-price deviation is negative because the actual price is lower than the price predicted by the linear regression model. Hence the oscillator has a negative value on that date:



Let's keep going until the price peak achieved at the end of 2017:



And finally, let's use all price data available to date. During this process of moving forwards in time, the oscillator values that have previously been computed have not changed. Current prices affect only the present oscillator value — past values are not changed.



Super-imposed on the price data on the left graph we have the three different linear regression fits we obtained at the three time points we had

chosen above. The linear regression models change over time: the slope can become larger or smaller. But only the log price deviations are used in the power oscillator.

The power oscillator up to the date of writing looks like this:

Interpretations

good moments to buy bitcoin

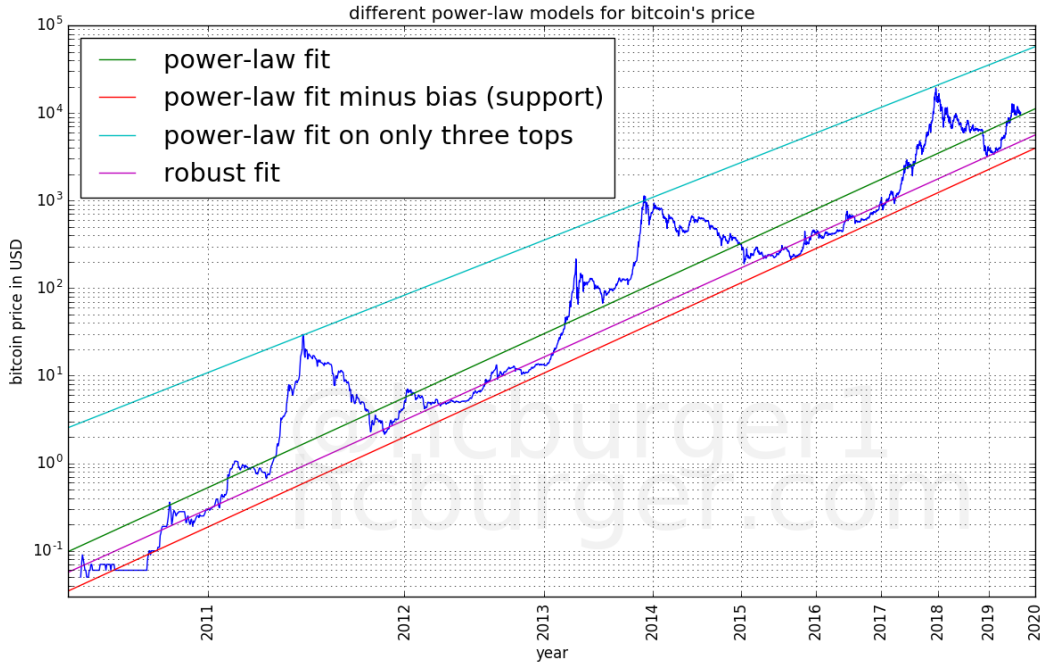
Low oscillator values indicate moments in time when the price of bitcoin is low compared to its long-term growth (power-law) trend. These moments should therefore present good opportunities to buy bitcoin. We will pick the moments were the oscillator is lower than the median oscillator as "good moments to buy". We choose the median because it means that the oscillator spends half its time above this value, and half its time below this value. The median also has to be updated with time, since new data will influence its value. The green line in the plot below shows the median of the oscillator. Moments when the oscillator is below this curve can be considered particularly good times to buy:

Using the median is also convenient because there is no need to hand-pick a certain threshold value, e.g. -0.1.

when to sell bitcoin

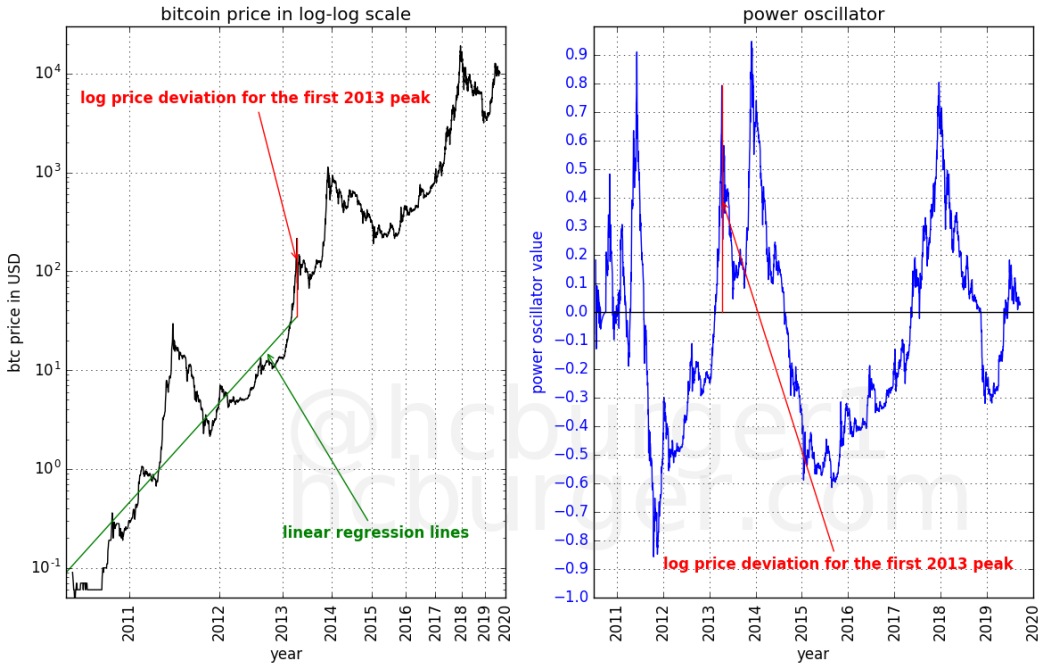
The reverse question is when to sell bitcoin. We notice that all four all-time-highs coincide with oscillator values that lie within a narrow band between about 0.8 and 0.9:

This is surprising. We have previously seen that **three** (not four) all-time-highs lie on a straight line in a log-log plot:



Two all-time-highs occurred in 2013, and only one of those lies on the top of the long-term price corridor. Yet, the power-oscillator catches this first bubble of 2013 as a market top.

How come? If we do a power-law fit to the bitcoin price data available up to the first 2013 bubble, we see that the price of the bubble indeed deviates significantly from the long-term fit of the time:



the magic threshold

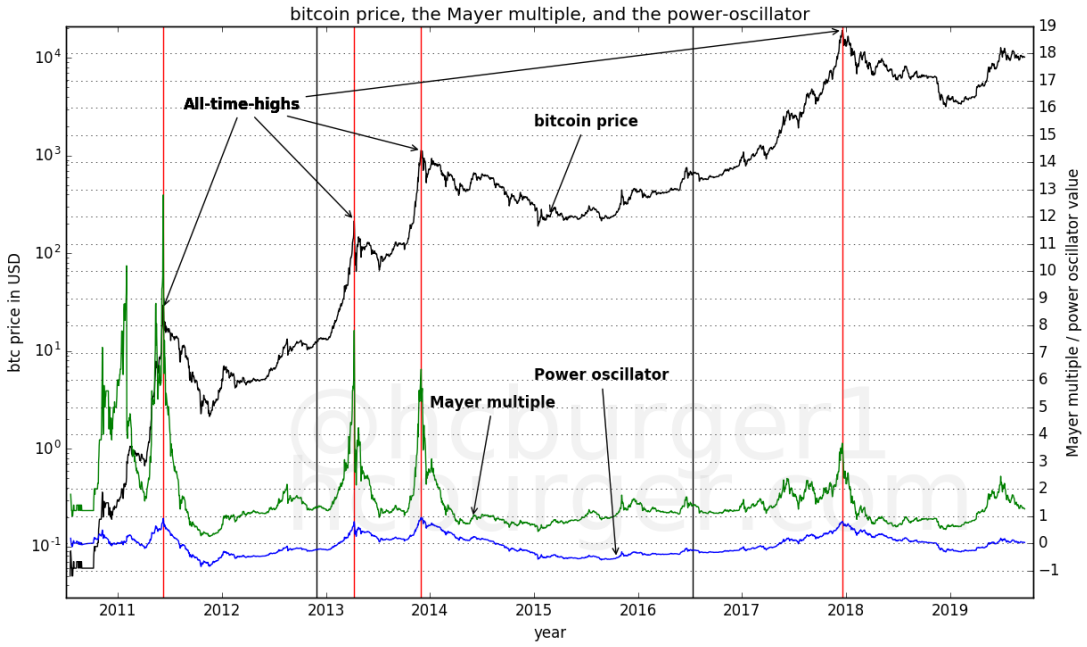
The fact that bubbles burst in the 0.8 to 0.9 oscillator band means that the market cannot support prices that are above a certain level above the long-term trend. If this threshold is breached, an abrupt downward correction occurs. Oscillator values of 0.8 to 0.9 correspond to a price that is about 6.3 to 8 times higher than the long-term power-law regression fit.

more lines — percentiles

For the more technically inclined reader, in the below graph I have not only inserted the median, but also all other percentiles from 10 to 90 in steps of 10 [5]:

Relation to the Mayer multiple

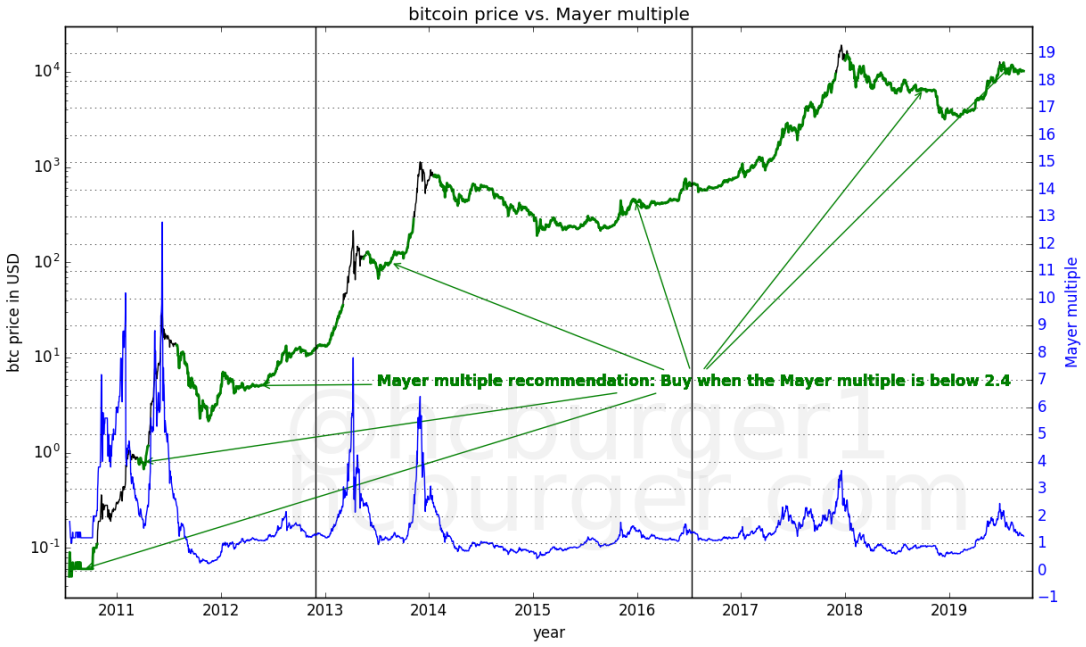
The power oscillator superficially resembles the Mayer multiple [6]. The Mayer multiple was proposed by Trace Mayer and compares the price of bitcoin to the 200-day moving average of the price. The Mayer multiple is the ratio between these two values: A Mayer multiple of 5 on day x means that the bitcoin price is 5 times higher than the 200-day moving average.



We immediately notice that the Mayer multiple and the power oscillator look superficially similar: they both achieve high values during market peaks, and lower values during market lulls.

However, an important difference is that the power oscillator has virtually the *same* value (0.8) at each all-time-high, whereas the Mayer multiple does not: It ranges between approximately 3.5 and 12 for the four different all-time-highs. The Mayer multiple is therefore not as useful as the power-oscillator at timing all-time-highs.

It is claimed that it has been found that it is best to accumulate bitcoin when the Mayer multiple is below 2.4. Following this recommendation implies accumulating bitcoin during the green periods below:



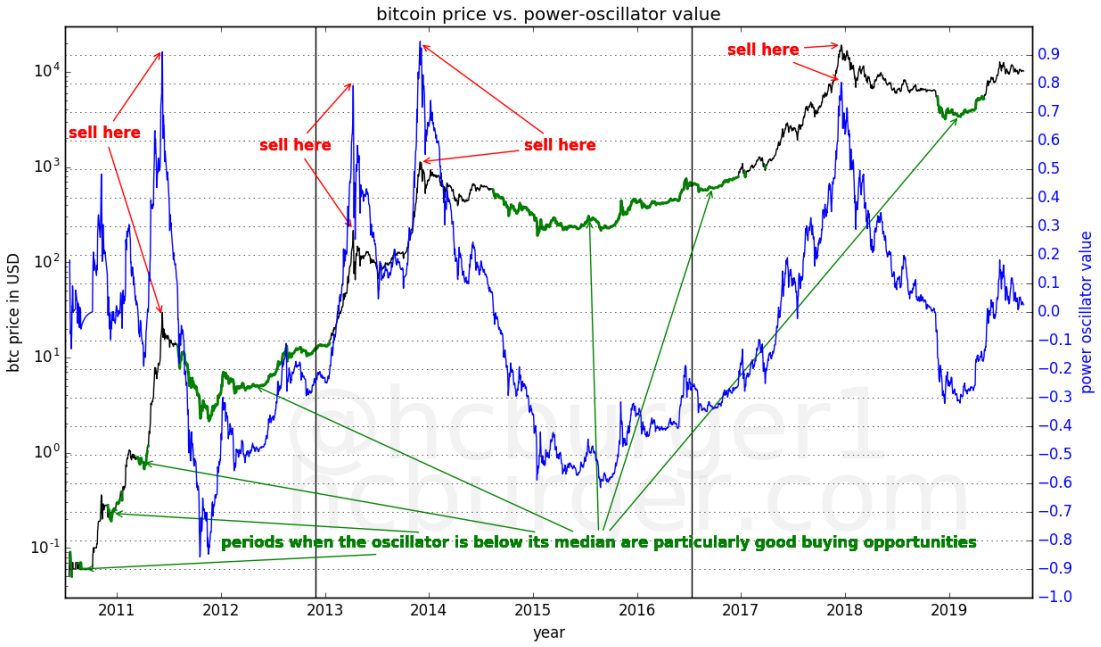
The results are not very convincing: the recommendation is to accumulate bitcoin at virtually all times. Such a strategy is unlikely to be the best performing we can come up with.

An important difference between the Mayer multiple and the power oscillator is that the Mayer multiple depends on a manually chosen parameter: the 200-day moving average. It is not a priori clear why the choice of 200 should be the correct one. In fact, it is not clear that this parameter should not change over time, given that bitcoin's price grows slower and slower over time.

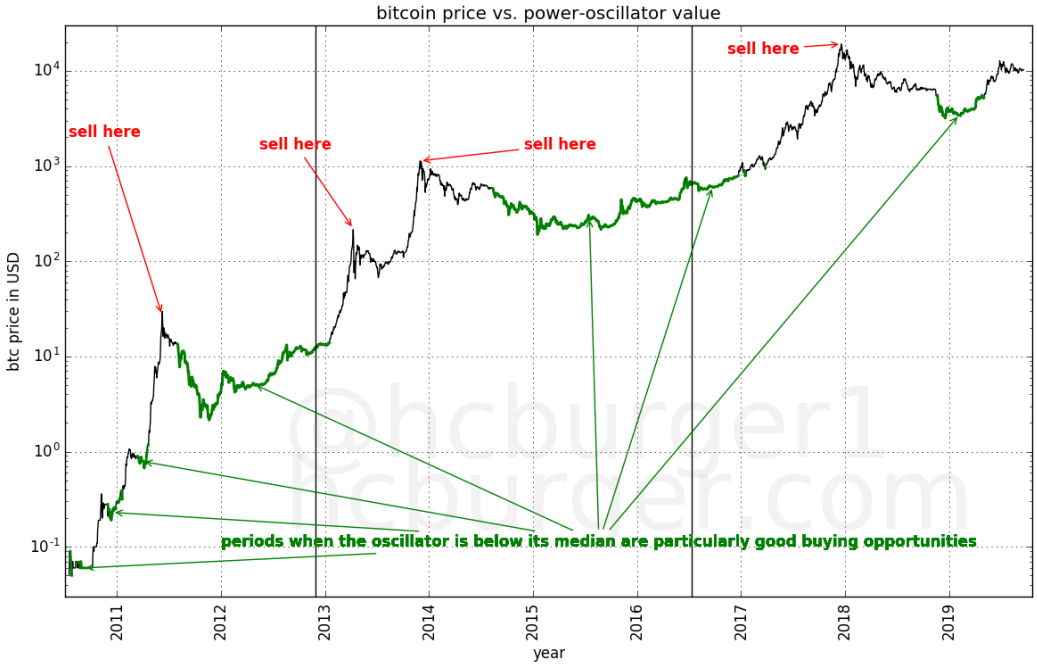
The power oscillator has no parameter that needs to be manually chosen. It relies solely on the principle that bitcoin is likely to follow a power-law growth.

Overall strategy and simulation

The above recommendations that flow naturally from the power-oscillator are summarized in the figure below:



To make the plot less crowded, let's look at just the price data:

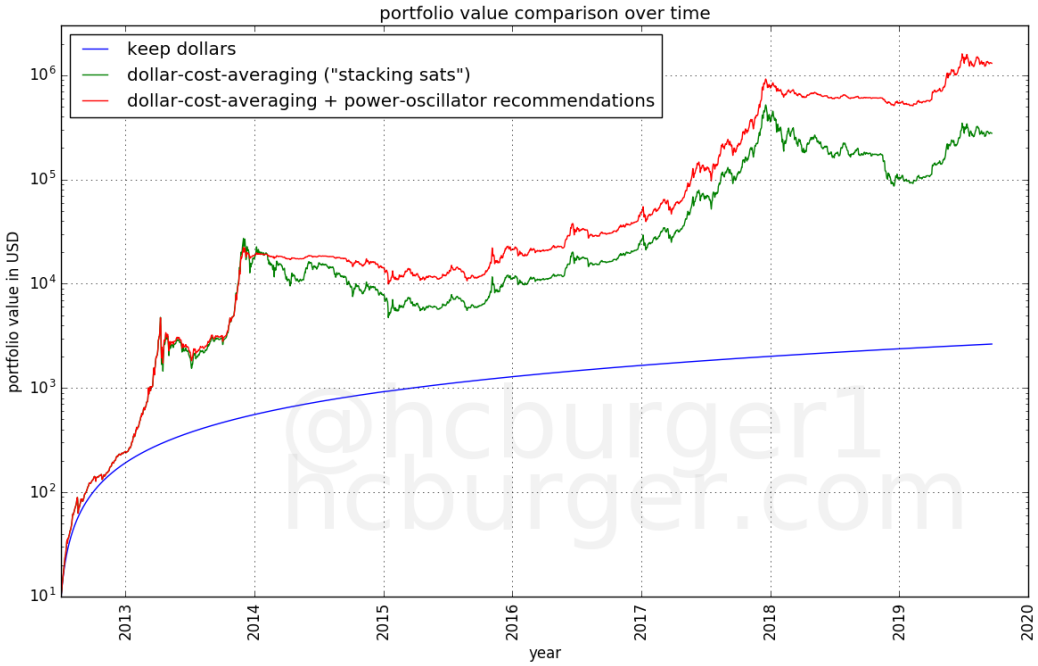


Let's use these recommendations to devise a simple trading strategy where the investor:

- uses dollar-cost-averaging (or "stacking sats") as a base investment strategy

- starts selling his saved bitcoin when the oscillator is above a given threshold (e.g. 0.7) and uses this money to buy more bitcoin when the oscillator is below its median value.

Let's compare this strategy to dollar-cost averaging, and let's assume that the lucky investor does not have to pay taxes. Let's let the simulation begin in mid-2012:



We see that the strategy guided by the power oscillator:

- achieves returns that outperform dollar-cost-averaging significantly. An investor who started investing in mid-2012 and followed this strategy with a budget of one dollar a day would now have a portfolio that is worth $1285938. Whereas an investor who started at the same time but stuck to dollar-cost-averaging would have a portfolio worth $273848 (approximately 4.7 times lower).
- achieves smaller fluctuations than dollar-cost averaging.

At first glance, it would therefore appear that the power-oscillator can be a useful tool in guiding a trading strategy. The threshold of 0.7 in this scenario was admittedly manually chosen, but it was also chosen to lie well below the usual value at which bubbles burst, so as to make the strategy more robust.

The above strategy is certainly not perfect. For example, there is no buy recommendation after the first sell recommendation during the first bubble

of 2013. The next buy recommendation came at a much higher price than the peak of the first 2013 bubble.

Another imperfection is that the model seems to recommend to buy somewhat too early after a bubble.

Other trading strategies can certainly be devised using the power-oscillator (e.g. based on other thresholds or percentiles), but the goal of this article is not to find a perfect trading strategy but to present a simple indicator.

Conclusion

We have introduced the power oscillator, an oscillator which:

- is based on bitcoin's natural power-law based growth model.
- does not depend on hand-chosen hyper-parameters such as the 200-day moving average in the Mayer multiple [7].
- detects good moments to buy bitcoin without the introduction of a hand-chosen parameter.
- reliably detected all four bitcoin all-time-highs.
- is more useful than the Mayer multiple.

Another way of saying that bubbles pop at a power oscillator value above 0.7 is to say that the market cannot sustain prices that are more than about 5 times higher than what the power-law based trend-line would indicate. This is another indicator that power-law models are natural to bitcoin's price history.

The same reasoning holds for prices that are too low compared to the long-term power-law trend, except that corrections occur more slowly.

High values of the power oscillator are only possible if the price of bitcoin rises quickly. If the price rises more slowly, the power-law estimate of the price has time to adapt, leading to smaller power oscillator values.

oscillator must oscillate

It is worth noting that the power-law oscillator is indeed expected to keep oscillating, as long as bitcoin's price growth continues to follow a kind of power-law. Should bitcoin's price growth accelerate instead of decelerate (as is the case with power-laws), the power-oscillator would keep growing.

The fact that the power oscillator indeed oscillates around 0 (instead of e.g. growing perpetually), shows that bitcoin's price history continues to follow a power-law, instead of e.g. exponential growth.

the power oscillator is but one more tool

No tool is likely to be the perfect tool for timing the market. The power oscillator is no exception. I remind the reader that this article is not financial advice. I am not recommending any position in this article.

Acknowledgements

I would like to sincerely thank BitcoinEcon for the numerous interesting exchanges we had, and the early feed-back he gave me when reading drafts of this article. Thank you very much!

References

1. https://en.wikipedia.org/wiki/Overfitting
2. https://www.investopedia.com/terms/o/oscillator.asp
3. https://en.wikipedia.org/wiki/Log%E2%80%93log_plot
4. https://en.wikipedia.org/wiki/Linear_regression
5. https://en.wikipedia.org/wiki/Percentile
6. https://mayermultiple.info/
7. https://en.wikipedia.org/wiki/Hyperparameter

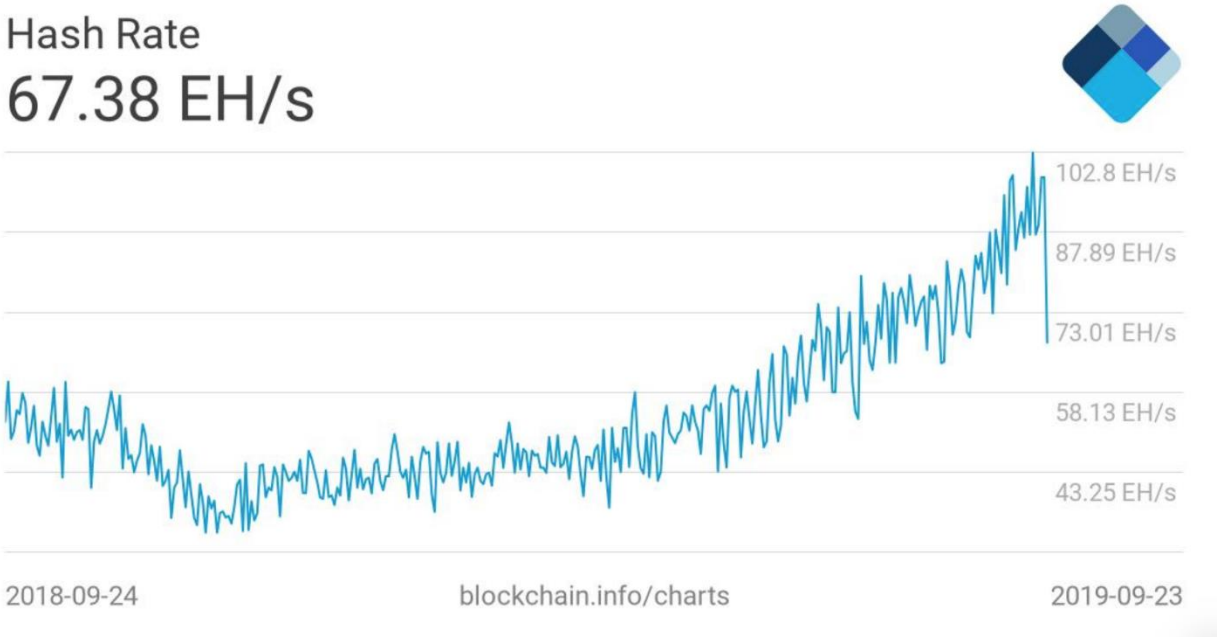
A Note On Variance in Bitcoin Mining

By Christopher Bendiksen

Posted September 25, 2019

It doesn't take much to create FUD in the Bitcoin space, intentional or not. But before we get all worked up over scary graphs, let's all sit down for a second and look at how things actually work.

Yesterday (and it seems to be continuing today even though the graphs have reverted to the mean), one after another, Twitter pundits and news outlets started posting worried remarks about the Bitcoin hashrate accompanied by some pretty stark-looking charts of the hashrate dropping hard, in some estimates by more than 50% in less than one week.



(and this wasn't even the worst estimate)

On the surface, one can understand the concern. Looking at the charts the numbers appear clear. One day the hashrate tops out at more than 120 EH/s and less than 10 days later it has dropped to 58 EH/s. Seems catastrophic.

It's not.

But to understand why, we need to look a little deeper into how these graphs are calculated.

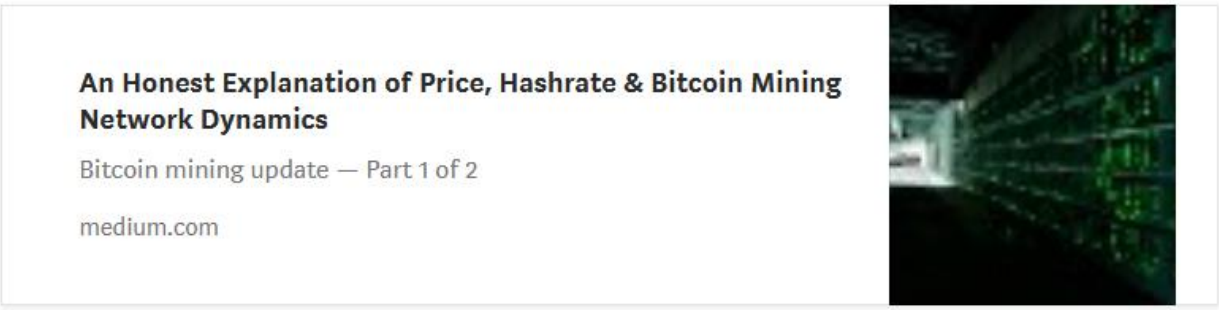
So let's start with something you might not know: the Bitcoin hashrate is actually not a known measure. It is *technically* not even knowable (kinda like

the number of air atoms in a balloon isn't knowable). All one can do is estimate the hashrate based on the frequency of past blocks and the mining difficulty. And while those estimates can be *really good* they have to be done right.

As an example of an estimate done properly we can actually look at how the Bitcoin protocol itself deals with this issue in difficulty adjustments.

It works (kinda) like this: Every 2016 blocks, the protocol calculates the average block time over that interval. It then compares the result against its benchmark of 10 minute blocks. If the blocks came 8% faster than 10 minutes, it increases the mining difficulty by 8%. If they came 15% slower than 10 minutes, it decreases the difficulty by 15%. This ensures that the mining difficulty is set such that blocks arrive every 10 minutes on average.

This also has a host of other consequences which we discuss in some more detail here:



Estimating the hashrate is done in a very similar fashion. While the protocol doesn't bother itself with the actual nominal hash power measure, we can use the same information plus the difficulty to arrive at an estimate of the hashrate. Knowing the difficulty, one can know what time it should take a certain amount of hash power, on average, to find a certain amount of blocks. This estimate gets more accurate the longer the interval one measures it over.

And herein lies the essence of the problem. If the measurement interval is too short, the estimate becomes vulnerable to the inherent variance in block times.

Block times are Poisson distributed

That sounds fancy but somewhat simplified, all it means is that the probability of finding a new block *remains the same, no matter how many hashes you have already tried.*

Which has some pretty counterintuitive effects such as the following statement:

“No matter how long the network’s been hashing since the last block, on average, the next block is always 10 minutes away.”

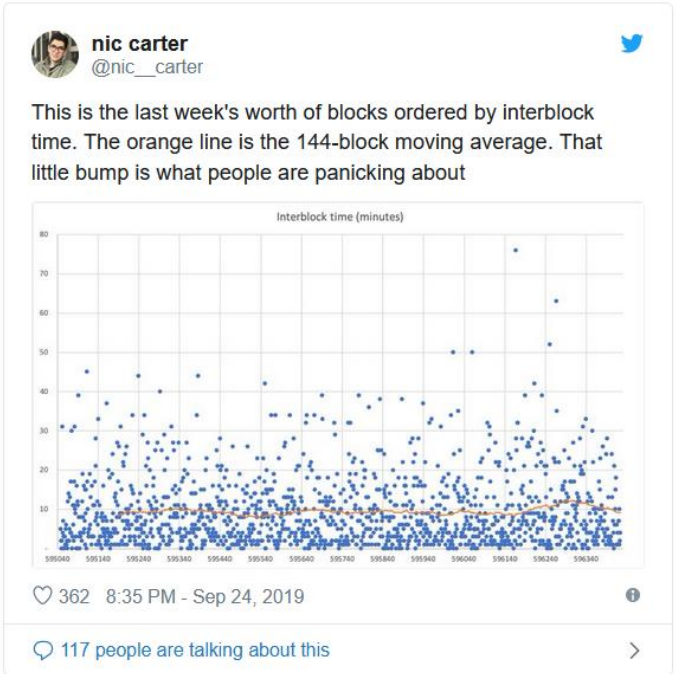
Weird, I know.

But the most important effect in terms of our discussion here is that it leads to *probabilistic variance in the block times*. In other words, while blocks come out at 10 minutes *on average,* sometimes they take 14 minutes, sometimes 58 minutes, sometimes 33 seconds. You get the gist.

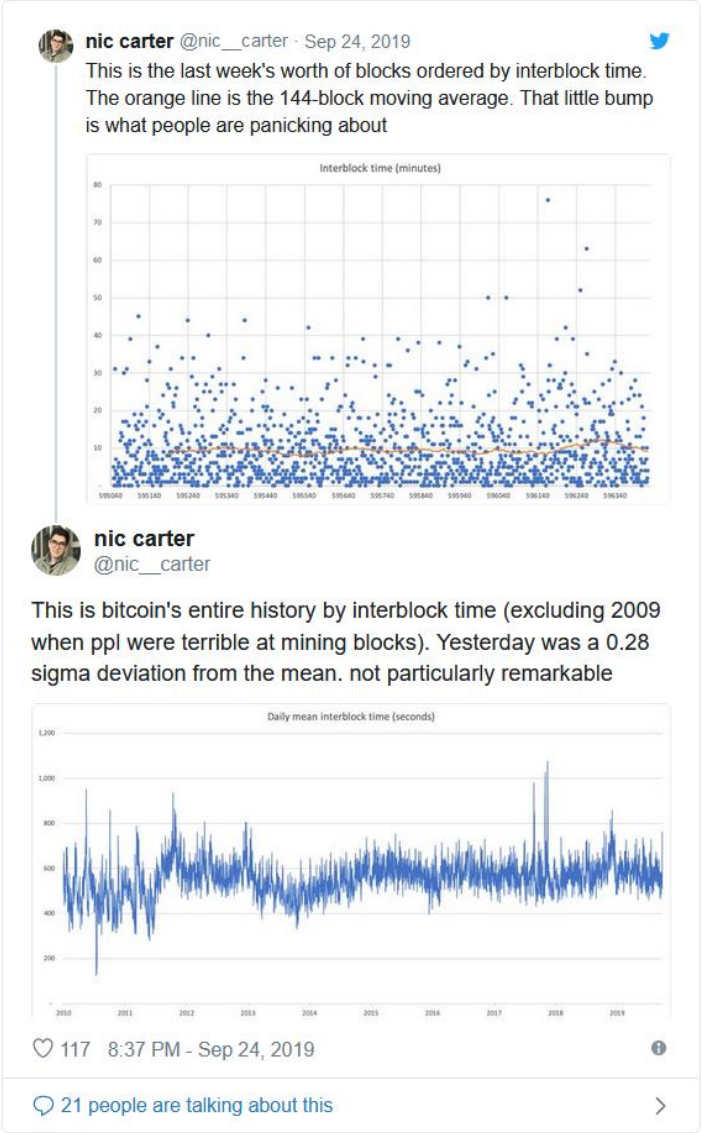
This impacts these hashrate estimates, and the impact is greater the shorter their measurement interval. When you look at the daily hashrate estimates, the curves are super spiky in both directions. This is not because the hashrate fluctuates wildly on a daily basis (but you’d be surprised how many people, even some within the mining industry, actually believe this).

The reason is that probabilistically distributed variance does funny things sometimes. Sometimes a bunch of fast blocks happen in relatively rapid succession. Sometimes the opposite. This is what causes those spikes. A series of randomly slow or quick blocks happen within the measurement interval of the hashrate estimation algorithms, which is then extrapolated to make it seem like the hashrate either cratered or exploded.

As per usual, Nic Carter does everyone the favour of actually running the numbers and showing *exactly* what happened these last few days. Have a look:



See those five blocks above 50 minutes in the upper right corner? That's pretty much what this was all about. His next tweet shows the event in context of (almost) the entire block history:



As you can see, this latest event (the right-most upward spike) was indeed spikier than "normal", but only marginally spikier.

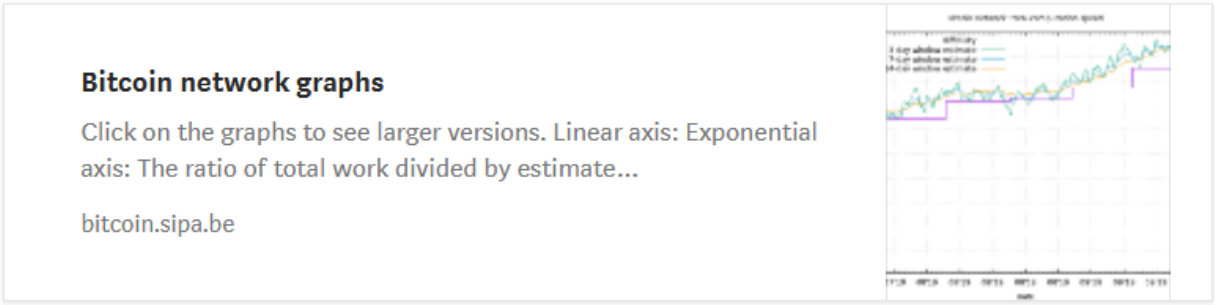
So what's the real hashrate then?

Like I said: no one knows — at least not precisely.

But let's revisit the figures from the beginning of this post. The hashrate never actually reached 120 EH/s. Nor did it drop to 58 EH/s. When reading these graphs the best way to do it is to look at the 7 or 14 day averages. You'll

remember from above that the Bitcoin protocol itself uses the 14 day average for its Difficulty Adjustment Algorithm — for this exact reason.

When looking at the 7 or 14 day estimates for example here (btw Sipa, the creator of that website, is Bitcoin developer Peter Wuille):



You'll see that the curve is, unsurprisingly, much smoother and easier to read. The spikes are dampened and large tops and bottoms are much more rare — the noise is filtered out. In addition, you'll see that the hashrate probably hasn't even reached 100 EH/s yet, let alone 120 EH/s. And if there is indeed a large drop-out of mining power happening somewhere (doesn't appear to be the case), it will materialise soon enough on the 14 day average curve.

And until it does, my plea is one that I feel like I've repeated many times over:

Resist the urge to cry wolf. At the very least look into how measurements work before sounding the alarm at readings you find weird.

FUD isn't always intentionally generated, but it is FUD nonetheless.

Disclaimer

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

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

Digital assets and related technologies can be extremely complicated. The digital sector has spawned concepts and nomenclature much of which is novel and can be difficult for even technically savvy individuals to thoroughly comprehend. The sector also evolves rapidly. With increasing media attention on digital assets and related technologies, many of the concepts associated therewith (and the terms used to encapsulate them) are more likely to be encountered outside of the digital space. Although a term may become relatively well-known and in a relatively short timeframe, there is a

danger that misunderstandings and misconceptions can take root relating to precisely what the concept behind the given term is.

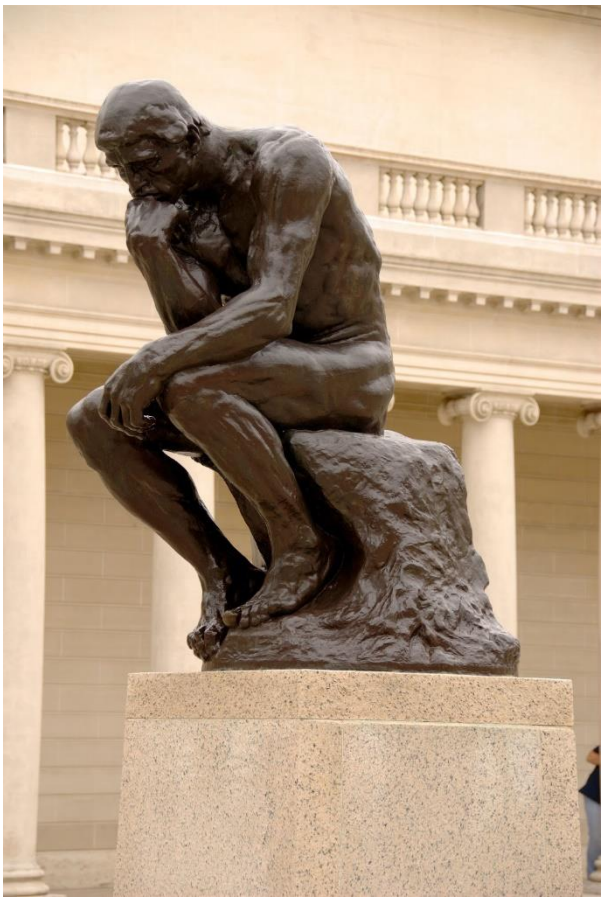
The purpose of this Blog Post is to provide objective, educational and interesting commentary. This Blog Post is not directed at any particular person or group of persons. Although produced with reasonable care and skill, no representation should be taken as having been given that this Blog Post is an exhaustive analysis of all of the considerations which its subject matter may give rise to. This Blog Post fairly represents the opinions and sentiments of its author at the date of publishing but it should be noted that such opinions and sentiments may be revised from time to time, for example in light of experience and further developments, and the blog post may not necessarily be updated to reflect the same. The opinions expressed in this blog post are the opinions of CoinShares (UK) Limited and do not represent the opinions of Sapia Partners LLP. The blog post content is for general informational purposes only and is not intended to provide specific advice or recommendations for any individual or on any specific security or investment product. It is only intended to provide education about the financial industry.

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

Envisioning LSPs in the Lightning Economy

By Roy Sheinfeld

Posted September 25, 2019



Our recent post about Lightning Service Providers has generated plenty of feedback. (Your attention is flattering.) Many people in the Lightning community have responded with something along the lines of:

"Sure, we get the structural necessity of LSPs in the network, and it's nice to have a catchy term for these entities, but we don't understand how LSPs are actually going to work *in practice*. Who are they? What's their incentive structure? How do they work as businesses?"

Glad you asked. We've been thinking about these questions a lot lately, and I'd be happy to share our ideas to help concretize LSPs and the Lightning economy more generally.

Some startups have hammocks and ping-pong tables. We think the old fashioned way. On our chins. (Source: Wikimedia)

Quick recap: what's an LSP again?

LSPs provide Lightning users with network services. These services include things like routing, guaranteeing uptime, SLAs, rebalancing channels *with other LSPs* to keep the network fluid, and — perhaps most importantly — opening funded channels.

To understand why these functions are so vital, let's think backward from the endpoint of a functioning Lightning economy. Yes, Lightning already works very well for a nascent technology. But to expand from thousands of users to billions, we need to simplify and streamline the onboarding process. It's not enough to be more convenient and attractive than bitcoin; we have to make Lightning more convenient and attractive than fiat.

For example, fiat users are accustomed to having access to their funds and being able to receive payments immediately. Waiting ten seconds at a card reader when making a purchase on a busy shopping day is considered an inconvenience. Fiat banks have buried routing deep in their backend via SWIFT, leaving users in blissful ignorance of its complexity. Fiat and banks have had years, decades, centuries to streamline their UX and move the complexity of the system into the backend.

Lightning has to do the same, and LSPs are the way to do so at scale. Functions like rebalancing, opening funded channels, and guaranteeing uptime are services LSPs have to provide to let users just be users, not network admins.

A few months ago, I quoted Alfred North Whitehead, who said that "Civilization advances by extending the number of important operations which we can perform without thinking about them." The Lightning Network advances by extending the number of important operations users can perform without thinking about them. LSPs multiply users' capabilities while reducing demands on their time and expertise.

If you want a Lightning economy, you need onboarding, and LSPs are how to make it happen.

Do any LSPs exist yet, and if so, who are they?

Yes, LSPs exist. They're here. They're among us. One of them is sharing his ideas with you right now.

Remember: anybody could be an LSP. Are you listening, or were you paying attention to the LSP in the red dress? (Source: Warner Bros. Studios)

At the moment, LSPs are those few firms developing Lightning clients, providing services, and running nodes. They just offer different selections of user services.

For example, Eclair runs a node, opens channels under certain conditions, and provides a wallet app. Bitrefill's Thor opens channels with inbound liquidity for users, which they can access by a third-party wallet app. Their up-market Thor Turbo service also provides users with some outbound BTC

liquidity … for a price. LNBIG and LightningTo.me open channels with users' existing wallets, giving them varying amounts of inbound capacity. Olympus and Sparkswap open channels for users and let them buy bitcoin with fiat, depositing the satoshis directly into the users' payment channels. (More on these last two below.)

Breez opens pre-configured, non-custodial channels, provides a full-service wallet app, gives users incoming liquidity at no extra charge, lets users manage all their bitcoin from a single balance, publishes a highly informative and entertaining blog, and is kind to small children and puppies.

This list is illustrative, not exclusive. There are more, and we're not trying to make a point by leaving anybody out.

Incentives for first-generation LSPs

Innovation takes a certain kind of attitude. I mean, we're all doing okay, so the conventional wisdom would be not to change a running system, right? Innovators need the audacity to look at a running system and to say to themselves, "Nope, this could be better."

Different people investing their time and energy into starting an LSP might have any number of different motives. Some might see a chance to get rich by riding the growth of the Lightning economy, and others might believe in bitcoin and its potential to change the world for the better, sensing a duty and an opportunity to realize that better world. (Where do we stand? Here's a hint.)

Tradition is the beauty of the green grass beneath our feet. Progress is the result of trying to reach the greener grass on the other side. (Source: Su — May)

Because Lightning is still so new and it's still changing so fast, nobody has really cracked the formula yet. Nobody knows the best business model for LSPs. Indeed, there might be several viable, scalable business models for different kinds of LSPs servicing different niche markets. We're just surveying what's currently possible, concretizing our vision of the coming Lightning economy, and interpolating between the two.

Today's LSPs are on the cutting edge. We're the early adopters, the first movers, the cool kids on the Lightning network. Since we're committed to — and certain of — the coming Lightning economy, the time, effort, and coin we're spending on building the network and our user base now is an investment in our future. The future is our incentive, and progress is our reward.

Speaking of the future...

The second wave of LSPs

As the Lightning network and the Lightning economy grow, the LSP model will become more attractive. Indeed, for some current market actors, expanding their businesses into Lightning services will be a requirement for survival. A couple of existing business models will feel pressure to become LSPs in the next, say, one to three years. First are the exchanges. Second are existing payment apps, like Square's Cash App and Venmo.

Think about it: as the Lightning economy grows, bitcoin will gradually suck fiat out of the economy, and exchanging currencies is what exchanges do. Ergo "exchanges." Existing bitcoin users are already familiar with exchanges, and many incoming fiat users will have to pass through an exchange before joining the Lightning economy. (Unless, of course, their LSP offers a handy, in-app means to top-up their balances.)

Occupying the conduit between crypto and fiat, the exchanges won't be able to miss the flow towards Lightning. And not expanding their services to take advantage of that position would be ludicrous.

In fact, as bitcoin expands to become the default medium of exchange with Lightning as its medium, exchanges are going to face a very busy transition period, after which, however, they're going to need a new business model. In the absence of fiat, there won't be as much left to exchange. Expanding their offerings to include LSP services would be a natural, rational way to master the transition.

Further, running an exchange is also a capital-intensive undertaking. They need to have bitcoin on hand anyway, but bitcoin doesn't accrue interest. Now, if the exchanges could put some of that bitcoin into funding users' channels, they could even make some money on the bitcoin that would otherwise just be sitting around collecting digital dust.

The proof of exchanges' interest in the LSP model is in the fact that a couple of them *are already doing it*. Sparkswap and Olympus let users purchase bitcoin with USD, so they're exchanges. But they also open channels for users, like LSPs. Sparkswap opens users' channels immediately (just like Breez), and

Olympus opens the channel when the user buys bitcoin through a Turbo channel. They're effectively exchanges that offer Lightning services as well.

As for the payment apps, integrating Lightning as the preferred means of transferring everyday quantities of bitcoin is a natural progression from their existing businesses. Cash App *already* facilitates bitcoin transfers (well, sort of, because it's custodial, so it's not really bitcoin, is it?). Lightning is simply a better way to do what they're already doing.

The evolving LSP business model

When the exchanges enter the LSP space, we can expect more attention and more entrants to join the party. We're all used to bandwagons by now, right? But that's a good thing because it means that more people will start experimenting with more different kinds of LSP models. Some might be very large and serve hundreds of thousands of users; others might be very small and might only service a few dozen friends. The LSP model scales in both directions, up and down, which is great for decentralization.

The Lightning economy needs many people to help cultivate it, and decentralization has always been in bitcoin's DNA, so this trend is good for all of us and good for bitcoin.

At this stage, growth (read: onboarding) is the name of the game. A number of business models are thinkable for LSPs with sufficient capital. Each has to balance cost with scalability, onboarding with revenue.

If everyone jumps on the same bandwagon, it's a revolution. (Costumes optional) (Source: Wikimedia)

Freemium models

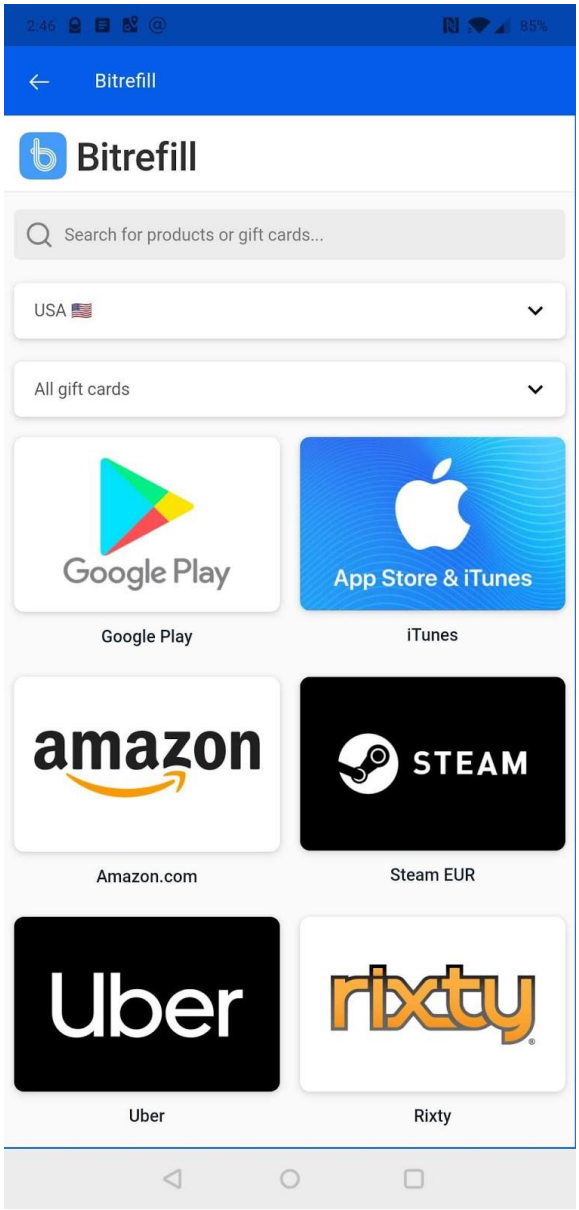
Now, if a firm is entering an existing but very promising space with incumbent, pioneering competitors, it'll need to catch up with and then surpass that competition. It has to grow faster than the existing providers, just like Spotify, Medium, Dropbox, and Skype have done in their respective markets. They started with good, competitive products, and *gave them away* — at least their basic functions or in some limited quantity.

The LSP business also lends itself to such freemium models. Since Lightning allows for transaction fees, a “free” service would effectively run on a pay-as-you-go basis, charging users transaction fees that are high enough to cover their costs. Limits on, say, channel capacities would also help contain the LSPs’ costs and provide users with an incentive to upgrade.

Such free user plans would be great for private users who want to experiment with Lightning before committing to a paid plan or for users who require limited capacity and a low-cost service (e.g. students). However, other classes of users, like businesses, will need better service, optimal reliability, more flexible capacity, and they’ll also be willing to pay for it.

In order to serve clients who need enterprise-grade performance, there will also be a market for paid, premium LSPs. Premium services could include higher channel capacities, higher transaction volumes, lower fees, SLA-guaranteed provision quality, and so on in exchange for a flat monthly fee.

Upselling



We've all seen those ads for phones that only cost $1. It's also the case that you can usually buy bananas in grocery stores in the northern hemisphere for less than the cost of shipping them thousands of kilometers. These providers can lose money on phones and bananas because they make far more on the mobile contracts and laundry detergent they sell to those same customers.

Perhaps counterintuitively, such loss leaders can be rational and profitable because they attract customers to associated products or services with higher margins.

An in-app marketplace in practice. More revenue streams = faster growth = accelerating progress.

LSPs could pursue a similar strategy by offering some services for free, like opening and funding channels, as long as users commit to using other services, like exchanging, for a price. If the margin on the profitable services and the user volume are sufficiently large, the LSPs can afford to offer some services for free. Indeed, they might even have an incentive to do so at scale.

Having users' attention when they're paying and making transactions is also a valuable commodity in itself. There is no reason why LSPs have to restrict their business models to their own services. They can also sell *products* and third-party services. More specifically, why not let users purchase directly from an in-app marketplace? Doing so requires another button in the app and perhaps a few B2B partnerships, but LSPs are working on that kind of thing anyway.

Additional revenue streams, like in-app marketplaces, also help to increase customer lifetime value (CLV). That's an important consideration, since services like opening funded channels increase the customer acquisition cost (CAC) — at least in the very short term. What matters, though, is the overall CAC:CLV ratio, so raising the CAC is not a bad thing if doing so raises the CLV even higher.

LSPs in a maturing Lightning economy

Once the second wave has hit, we can expect "LSP" and "the Lightning economy" to be household terms, even if many people aren't entirely sure how they work — much like bitcoin now. At that point, the banks will be sweating because the entire economy will be excising the middlemen. So who would be the next entrants into the LSP market? Who would stand to gain from widespread disintermediation?

In a word: everyone. It's hard to estimate what the banking system costs the world, but a decent first estimate is to add up the value of all the world's banks. They've been able to amass around $124 trillion in assets, a number that grows somewhere around 10% per year. That's the size of the pie that stands to be recut. And LSPs are the knives.

Mmmm. Slicing the pie. Is this the first pastry analogy we've used? No. Is it possible that I have a thing for sweet, delicious pastries? Maybe. (Source: skeez)

That pie is big enough for everyone to have a slice, so the LSP market is sure to flourish. The range of small-scale LSPs is likely to expand rapidly, but they won't be the only ones.

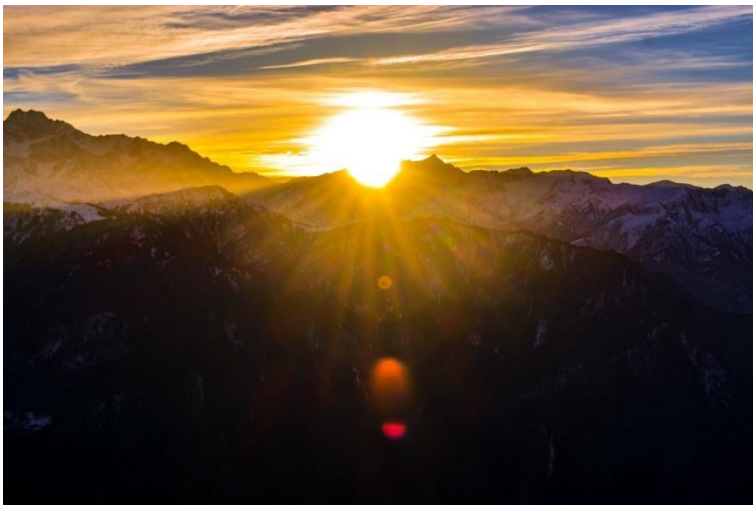
Other things being equal, those companies with the greatest transaction volumes — excluding banks — will be the ones with the greatest incentive to foster the Lightning economy. Those with vast user bases will also have an advantage in entering the LSP market. So which businesses have vast user bases and process vast quantities of transactions? The FAANG crew (possibly without Facebook, pending the fate of Libra) come to mind, and they are likely to join the third wave of LSPs.

Third-wave business models

The image in the crystal ball gets fuzzier the farther forward we look. Business models might be as diverse as the scales of the actors providing LSP services. Small LSPs might rely on personal contacts and low overheads, like a corner barber shop. Medium-sized ones might rely on custom localizations and brand tie-ins, like many current franchise operations. The largest have vast opportunities to onboard their current users while cutting costs and expanding their revenue streams.

To imagine a big tech player entering the LSP business, consider a company like Netflix. In 2018, Netflix had around 140 million subscribers, and their gross sales were around $18 billion. Imagine the number of transactions involved and the magnitude of transaction fees they had to remit to banks. If Netflix wanted to set up an LSP, they could pay for the R&D out of petty cash, and they could maybe save a few hundred million per year by disintermediating all those payments. Considering what banks currently make, a company like Netflix could soon be generating more revenue from a growing FinTech arm than they do from their traditional video-on-demand business.

In the third wave, scale will remain important, as always. But the key is always to find the right solution for the niche. Some people prefer processed cheese from a factory; others prefer artisanal Chesires ripened strictly in the cold months. We're eager to see where the Lightning economy goes, and we're excited to be growing along with it.



Like the sunrise, the fact that the Lightning economy is coming is more important than the exact timing. And they're both beautiful to watch. (Source: Rohit Gangwar)

Bitcoin is Not Backed by Nothing

By Parker Lewis

Posted September 27, 2019

Contrary to popular belief, bitcoin is in fact backed by something. It is backed by the only thing that backs any form of money: the credibility of its monetary properties. Money is not a collective hallucination nor merely a belief system. Over the course of history, various mediums have emerged as money, and each time, it has not just been by coincidence. Goods that emerge as money possess unique properties that differentiate them from other market goods. While The Bitcoin Standard provides a more full discussion, monetary goods possess unique properties that make them particularly useful as a means of exchange; these properties include scarcity, durability, divisibility, fungibility and portability, among others. With each emergent money, inherent properties of one medium improve upon and obsolete the monetary properties inherent in a pre-existing form of money, and every time a good has monetized, another has demonetized. Essentially, the relative strengths of one monetary medium out-compete that of another, and bitcoin is no different. It represents a technological advancement in the global competition for money; it is the superior successor to gold and the fiat money systems that leveraged gold's monetary properties.

Bitcoin is out-competing its analog predecessors on the basis of its monetary properties. Bitcoin is finitely scarce, and it is more easily divisible and more easily transferable than its incumbent competitors. It is also more decentralized, and as a derivative, more resistant to censorship or corruption. There will only ever be 21 million bitcoin, and each bitcoin is divisible to eight decimal points (1 one-hundred millionth). Value can be transferred to anyone and anywhere in the world on a permissionless basis, and final settlement does not rely on any third-party. In aggregate, its monetary properties are vastly superior to any other form of money used today. And, these properties do not exist by chance, nor do they exist in a vacuum. The emergent monetary properties in bitcoin are secured and reinforced through a combination of cryptography, a network of decentralized nodes enforcing a common set of consensus rules, and a robust mining network ensuring the integrity and immutability of bitcoin's transaction ledger. The currency itself is the keystone which binds the system together, creating economic incentives that allow the security columns to function as a whole. But even still, bitcoin's monetary properties are not absolute; instead, these properties are evaluated by the market relative to the properties inherent in other monetary systems.

Coinbase Pro: bitcoin exchange rate for dollars over the last six months (as of September 27, 2019).

Recognize that every time a dollar is sold for bitcoin, the exact same number of dollars and bitcoin exist in the world. All that changes is the relative preference of holding one currency versus another. As the value of bitcoin rises, it is an indication that market participants increasingly prefer holding bitcoin over dollars. A higher price of bitcoin (in dollar terms) means more dollars must be sold to acquire an equivalent amount of bitcoin. In aggregate, it is an evaluation by the market of the relative strength of monetary properties. Price is the output. Monetary properties are the input. As individuals evaluate the monetary properties of bitcoin, the natural question becomes: which possesses more credible monetary properties? Bitcoin or the dollar? Well, what backs the dollar (or euro or yen, etc.) in the first place? When attempting to answer this question, the retort is most often that the dollar is backed by the government, the military (guys with guns), or taxes. However, the dollar is backed by none of these. Not the government, not the military and not taxes. Governments tax what is valuable; a good is not valuable because it is taxed. Similarly, militaries secure what is valuable, not the other way around. And a government cannot dictate the value of its currency; it can only dictate the supply of its currency.

Venezuela, Argentina, and Turkey all have governments, militaries and the authority to tax, yet the currencies of each have deteriorated significantly over the past five years. While it's not sufficient to prove the counterfactual, each is an example that contradicts the idea that a currency derives its value as a function of government. Each and every episode of hyperinflation should be evidence enough of the inherent flaws in fiat monetary systems, but unfortunately it is not. Rather than understanding hyperinflation as the logical end game of all fiat systems, most simply believe hyperinflation to be evidence of monetary mismanagement. This simplistic view ignores first principles, as well as the dynamics which ensure monetary debasement in fiat systems. While the dollar is structurally more resilient as the global reserve currency, the underpinning of all fiat money is functionally the same, and the dollar is merely the strongest of a weak lot. Once the mechanism(s)

that back the dollar (and all fiat systems) is better understood, it provides a baseline to then evaluate the mechanisms that back bitcoin.

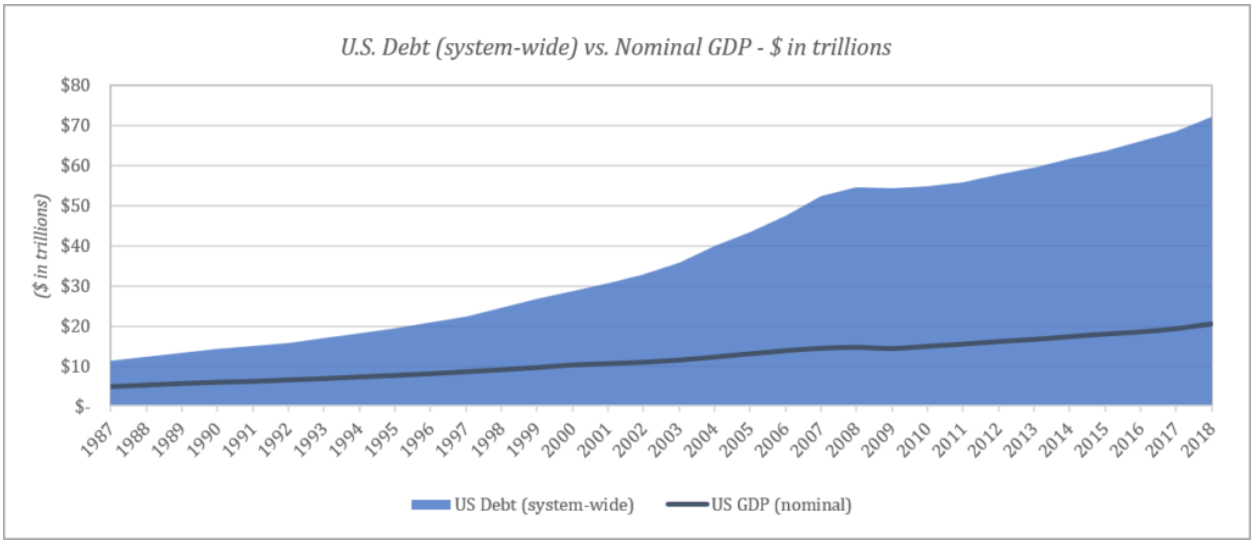
Why does the dollar have value?

The value of the dollar did not emerge on the free market. Instead, it emerged as a fractional representation of gold (and silver initially). Essentially, the dollar was a solution to the inherent limitations in the convertibility and transferability of gold; its inception was dependent on the monetary properties of base metals, rather than properties inherent in the dollar itself. It was also initially a system based on trust: accept dollars and trust that it could be converted back to gold at a fixed amount in the future. Gold's limitation and ultimate failure as money is the dollar system, and without gold, the dollar would have never existed in its current construct. For a quick review of the dollar's history with gold:

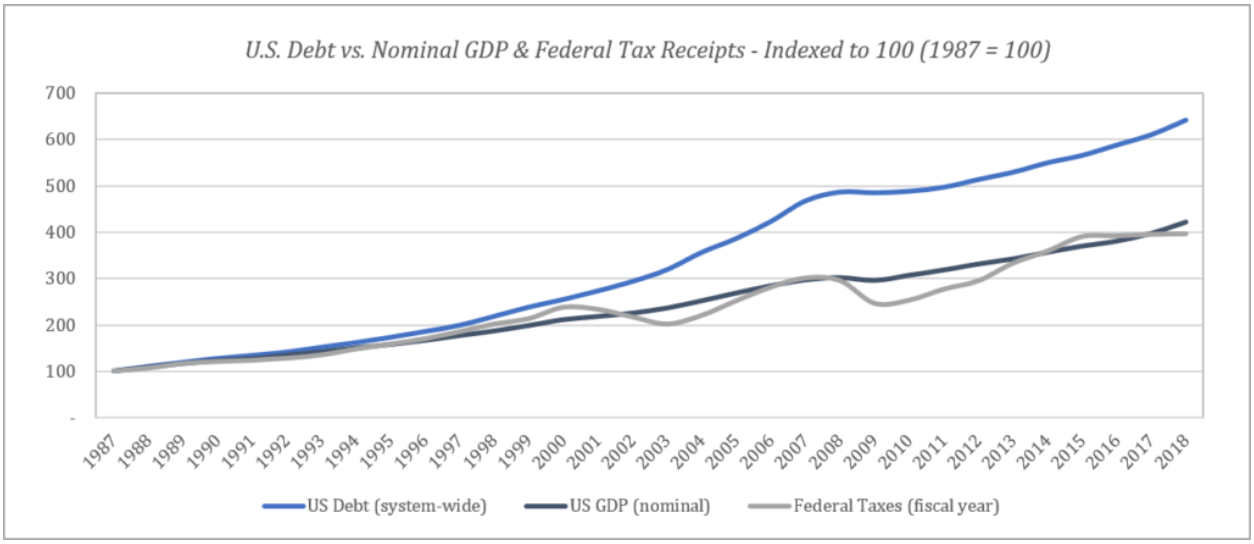
1900	Gold Standard Act of 1900 established that gold was the only metal convertible to the dollar; gold convertible to dollars at $20.67/oz.
1913	The Federal Reserve was created as part of the Federal Reserve Act of 1913.
1933	President Roosevelt banned the hoarding (saving) of gold via Executive Order 6102, requiring citizens to convert gold to dollars at $20.67 per ounce or face a penalty in the form of a fine up to $10,000 and/or up to 5 to 10 years imprisonment.
1934	President Roosevelt signed the Gold Reserve Act, devaluing the dollar by approximately 40% to $35 per ounce of gold.
1944	Bretton Woods agreement formalized ability of foreign governments and central banks to convert gold to dollars (and vice versa) at $35/oz and established fixed exchange ratios between dollars and other foreign currencies.
1971	President Nixon officially ended all convertibility of dollars to gold, effectively ending the Bretton Woods system. The value of dollar was changed to $38/oz of gold.
1973	The U.S. government repriced gold to $42 per ounce.
1976	The U.S. government then decoupled the value of the dollar from gold altogether in 1976.

Over the course of the twentieth century, the dollar transitioned from a reserve-backed currency to a debt-backed currency. While most people never stop to consider why the dollar has value in the post gold era, the most

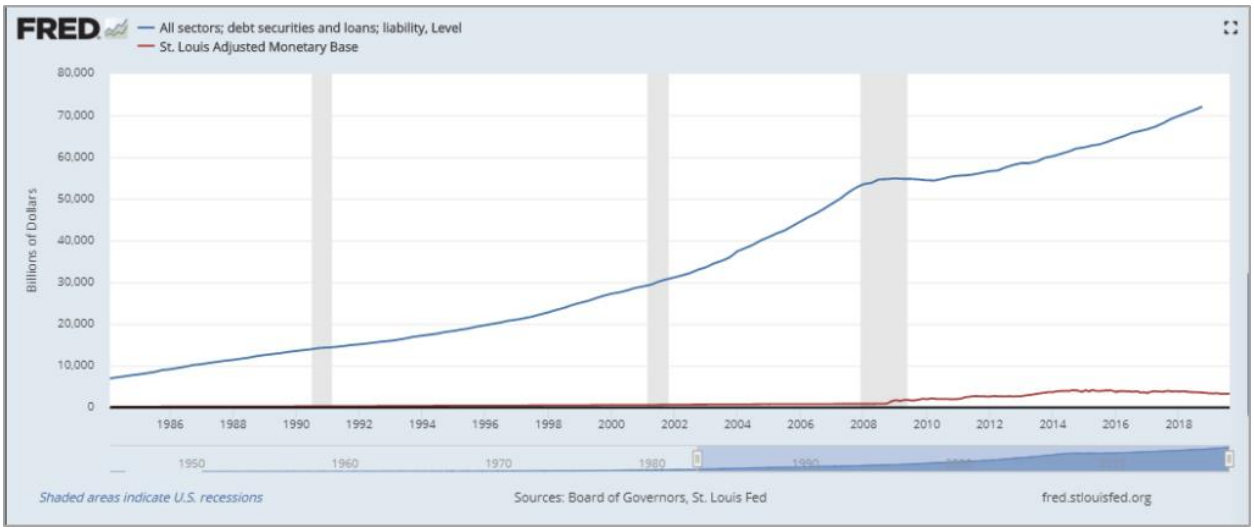
common explanation remains that it is either a collective hallucination (i.e. the dollar has value simply because we all believe it does), or that it is a function of the government, the military, and taxes. Neither explanation has any basis in first principles, nor is it the fundamental reason why the dollar retains value. Instead, today, the dollar maintains its value as a function of debt and the relative scarcity of dollars to dollar-denominated debt. In the dollar world, everything is a function of the credit system. Nominal GDP is functionally dependent on the size, and growth of the credit system, and taxes are a derivative of nominal GDP. The mechanisms that fund the government (taxes and deficit spending) are both dependent on the credit system, and it is the credit system that allows the dollar to function in its current construct.



The size of the credit system is several times larger than nominal GDP. Because the credit system is also orders of magnitude larger than the base money supply, economic activity is largely coordinated by the allocation and expansion of credit. However, the growth of the credit system has far outpaced the growth of GDP over the course of the last three decades. The chart below indexes the rate of change of the credit system compared to the rate of change of both nominal GDP and federal tax receipts (from 1987 to today). In the Fed's system, credit expansion drives nominal GDP which ultimately dictates the nominal level of federal tax receipts.



Today, there is $73 trillion of debt (fixed maturity / fixed liability) in the U.S. credit system according to the Federal Reserve (z.1 report), but there are only $1.6 trillion actual dollars in the banking system. This is how the Fed manages the relative stability of the dollar. Debt creates future demand for dollars. In the Fed's system, each dollar is leveraged approximately 40:1. If you borrow dollars today, you need to acquire dollars in the future to repay that debt, and currently, each dollar in the banking system is owed 40 times over. The relationship between the size of the credit system relative to the amount of dollars gives the dollar relative scarcity and stability. In aggregate, everyone needs dollars to repay dollar denominated credit.



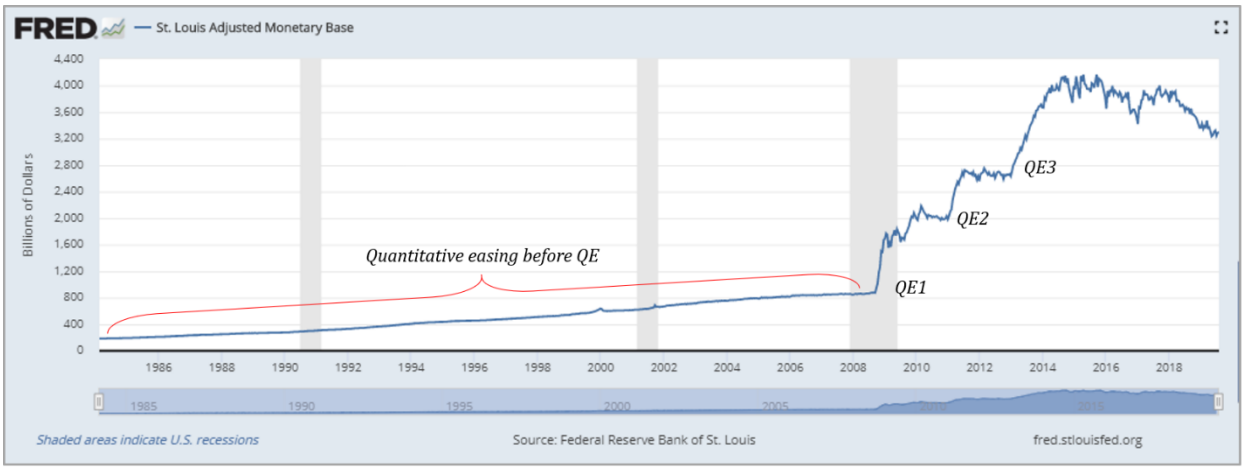
The system as a whole owes far more dollars than exist, creating an environment where on net there is a very high present demand for dollars. If consumers did not pay debt, their homes would be foreclosed upon, or their cars would be repossessed. If a corporation did not pay debt, company assets would be forfeited to creditors via a bankruptcy process, and equity could be

entirely wiped out. If a government did not pay debt, basic government functions would be shut down due to lack of funding. In most cases, the consequence of not securing the future dollars necessary to repay debt means losing the shirt on your back. Debt creates the ultimate incentive to demand dollars. So long as dollars are scarce relative to the amount of outstanding debt, the dollar remains relatively stable. This is how the Fed's economy works, incentivize credit creation and you create the source of future demand for the underlying currency. In a sense, it's kind of like a drug dealer. Get an addict hooked on your drug and he will keep coming back for more. In this case, the drug is debt, and it forces everyone, on net, to stay on the dollar hamster wheel.

The problem for the Fed's economy (and the dollar) is that it depends on the functioning of a highly leveraged credit system. And in order to sustain it, the Fed must increase the amount of base dollars. This is what quantitative easing is and why it exists. In order to sustain the amount of debt in the system, the Fed has to systematically increase the supply of actual dollars, otherwise the credit system would collapse. Increasing the amount of base dollars has the immediate effect of deleveraging the credit system, but it has the longer-term effect of inducing more credit. It also has the effect of devaluing the dollar gradually over time. This is all by design. Credit is ultimately what backs the dollar because what the credit actually represents is claims on real assets, and consequently, people's livelihoods. Come with dollars in the future or risk losing your house is an incredible incentive to work for dollars.

The relationship between dollars and dollar credit keeps the Fed's game in play, and central bankers believe this can go on forever. Create more dollars; create more debt. Too much debt? Create more dollars, and so on. Ultimately, in the Fed's (or any central bank's) system, the currency is the release valve. Because there is $73 trillion of debt and only $1.6 trillion dollars in the U.S. banking system, more dollars will have to be added to the system to support the debt. The scarcity of dollars relative to the demand for dollars is what gives the dollar its value. Nothing more, nothing less. Nothing else backs the dollar. And while the dynamics of the credit system create relative scarcity of the dollar, it is also what ensures dollars will become less and less scarce on an absolute basis.

Too much debt → Create more money → More debt → Too much debt



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

As is the case with any monetary asset, scarcity is the monetary property that backs the dollar, but the dollar is only scarce relative to the amount of dollar-denominated debt that exists. And it now has real competition in the form of bitcoin. The dollar system and its lack of inherent monetary properties provides a stark contrast to the monetary properties emergent and inherent in bitcoin. Dollar scarcity is relative; bitcoin scarcity is absolute. The dollar system is based on trust; bitcoin is not. The dollar's supply is governed by a central bank, whereas bitcoin's supply is governed by a consensus of market participants. The supply of dollars will always be wed to the size of its credit system, whereas the supply of bitcoin is entirely divorced from the function of credit. And, the cost to create dollars is marginally zero, whereas the cost to create bitcoin is tangible and ever increasing. Ultimately, bitcoin's monetary properties are emergent and increasingly unmanipulable, whereas the dollar is inherently and increasingly manipulable.

Money and digital scarcity

The hardest mental hurdle to overcome, when evaluating bitcoin as money, is often that it is digital. Bitcoin is not tangible, and on the surface, it is not intuitive. How could something entirely digital be money? While the dollar is mostly digital, it remains far more tangible than bitcoin in the mind of most. While the digital dollar emerged from its paper predecessor and physical dollars remain in circulation, bitcoin is natively digital. With the dollar, there is a physical representation that anchors our mental models in the tangible world; with bitcoin, there is not. While bitcoin possesses **far more credible monetary properties** than the dollar, the dollar has always been money (for most of us), and as a consequence, its digital representation is seemingly a more intuitive extension from the physical to the digital world. While the dollar's basis as money is anchored in time and while its digital nature may seem more tangible, bitcoin represents finite scarcity. The supply of the dollar on the other hand has no limits.

Remember that the dollar does not have any inherent monetary properties. It leveraged the monetary properties of gold in its ascent to global reserve status, but in itself, there are no unique properties that ground the dollar as a stable form of money, other than its relative scarcity in the construct of its credit-linked monetary system. When evaluating bitcoin, the first principle question to consider is whether something digital could share the quintessential properties that made gold a store of value (and a form of money). Did gold emerge as money because it was physical or because it possessed transcendent properties beyond being physical? Of all the physical objects in the world, why gold? Gold emerged as money not because it was physical, but instead because its aggregate properties were unique. Most importantly, gold is scarce, fungible and highly durable. While gold possessed many properties which made it superior to any money that came before it, its fatal flaw was that it was difficult to transport and susceptible to centralization, which is ultimately why the dollar emerged as its transactional counterpart.

"As a thought experiment, imagine there was a base metal as scarce as gold but with the following properties: – boring grey in colour – not a good conductor of electricity – not particularly strong, but not ductile or easily malleable either – not useful for any practical or ornamental purpose and one special, magical property: – can be transported over a communications channel" – Satoshi Nakamoto (August 27, 2010)

Bitcoin shares the monetary properties that caused gold to emerge as a monetary medium, but it also improves upon gold's flaws. While gold is relatively scarce, bitcoin is finitely scarce and both are extremely durable. While gold is fungible, it is difficult to assay; bitcoin is fungible and easy to assay. Gold is difficult to transfer and highly centralized. Bitcoin is easy to transfer and highly decentralized. Essentially, bitcoin possesses all of the desirable traits of both physical gold and the digital dollar combined in one, but without the critical flaws of either. When evaluating monetary mediums, first principles are fundamental. Ignore the conclusion or end point, and start by asking yourself: if bitcoin were actually scarce and finite, ignoring that it is digital, could that be an effective measure of value and ultimately a store of value? Is scarcity a sufficiently powerful property that bitcoin could emerge as money, regardless of whether the form of that scarcity is digital?

While money may be an intangible concept, so long as there are benefits from trade and specialization, there is real demand and utility in money. Money is the tool we use to be the arbiter in determining relative value among more abundant consumption goods and capital goods. It is the good that coordinates all other economic activity. The absolute quantity of money is less important than its properties of being scarce and measurable. Scarcity is money's most important property. If supply of the unit of measure were

constantly and unpredictably changing, it would be very difficult to measure the value of goods relative to it, which is why scarcity, on its own, is an incredibly valuable property. While the value of the underlying measurement unit may fluctuate relative to goods and services, stability in the supply of money results in the least amount of noise in the relative price signal of other goods.

Despite being digital, bitcoin is designed to provide absolute scarcity, which is why it has the potential to be such an effective form of money (and measure of value). There will only ever be 21 million bitcoin, and 21 million is a scarily small number in relative and absolute terms. The Fed created $100 billion dollars just last week, with the click of a button. That is approximately $5,000 per bitcoin that will ever exist, created in just a week (and by only one central bank). To provide broader context, the Federal Reserve, the Bank of Japan and the European Central bank have collectively created $10 trillion dollars-worth of new money since the financial crisis, the equivalent of approximately $500,000 per bitcoin. Despite dollars, euro, yen and bitcoin all being digital, bitcoin is the only medium that is tangibly scarce and the only one with inherent monetary properties.

However, it is insufficient to simply claim that bitcoin is finitely scarce; nor should anyone simply accept this as fact. It is important to understand how and why that is the case. Why can't more than 21 million bitcoin be created and why can't it be copied? Why is bitcoin secure and why can't it be manipulated? While there are countless building blocks that collectively allow bitcoin to function with a reliably fixed supply, there are three key columns of security within the bitcoin network which are woven together and reinforced by the economic incentives of the currency itself:

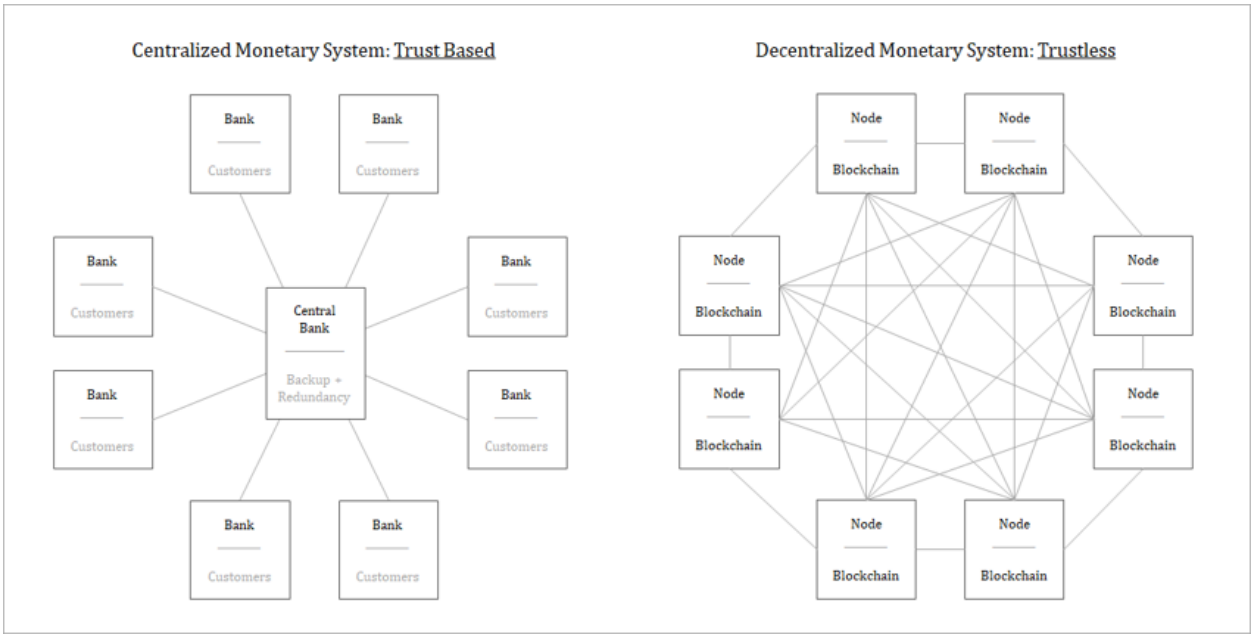
- Network Consensus & Full Nodes: enforce common set of governing rules
- Mining & Proof-of-Work: validate transaction history, anchor bitcoin security in the physical world
- Private Keys: secures the unit of value, ensures ownership is independent from validation

What Secures Bitcoin – Network Consensus & Full Nodes

21 million is not just a number guaranteed by software. Instead, bitcoin's fixed 21 million supply is governed by a consensus mechanism, and all market participants have an economic incentive to enforce the rules of the bitcoin network. While a consensus of the bitcoin network could theoretically determine to increase the supply of bitcoin such that it exceeds 21 million, an overwhelming majority of bitcoin users would have to collectively agree to debase their own currency in order to do so. In practice, a global and

decentralized network of rational economic actors, operating within a voluntary, opt-in currency system would not collectively and overwhelmingly form a consensus to debase the currency which they have all independently and voluntarily determined to use as a store of wealth. This reality then underpins and reinforces bitcoin's economic incentives, technical architecture and network effect.

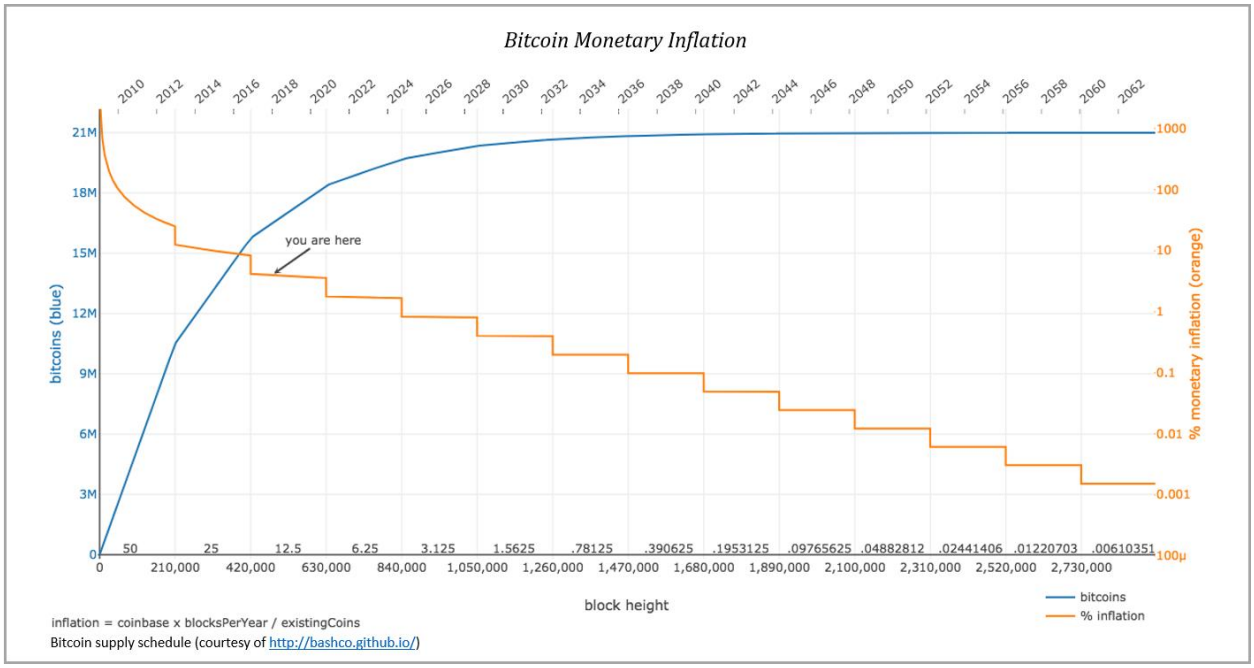
In bitcoin, a full node is a computer or server that maintains a full version of the bitcoin blockchain. Full nodes independently aggregate a version of the blockchain based on a common set of network consensus rules. While not everyone that holds bitcoin runs a full node, everyone is able to do so, and each node validates all transactions and all blocks. By running a full node, anyone can access the bitcoin network and broadcast transactions (or blocks) on a permissionless basis. And nodes do not trust any other nodes. Instead, each node independently verifies the complete history of bitcoin transactions based on a common set of rules, allowing the network to converge on a consistent and accurate version of history on a trustless basis.



This is the mechanism by which the bitcoin network removes trust in any centralized third-party and hardens the credibility of its fixed supply. All nodes maintain a history of all transactions, allowing each node to determine whether any future transaction is valid. In aggregate, bitcoin represents the most secure computing network in the world because anyone can access it and no one trusts anyone. The network is decentralized and there are no single points of failure. Every node represents a check and balance on the rest of the network, and without a central source of truth, the network is resistant to attack and corruption. Any node could fail or could become corrupted, and the rest of the network would remain unimpacted. The more nodes that

exists, the more decentralized bitcoin becomes, which increases redundancy, making the network harder and harder to corrupt or censor.

Each full node enforces the consensus rules of the network, a critical element of which is the currency's fixed supply. Each bitcoin block includes a pre-defined number of bitcoin to be issued and each bitcoin transaction must have originated from a previously valid block in order to be valid. Every 210,000 blocks, the bitcoin issued in each valid block is cut in half until the amount of bitcoin issued ultimately reaches zero in approximately 2140, creating an asymptotic, capped supply schedule. Because each node independently validates every transaction and each block, the network collectively enforces the fixed 21 million supply. If any node broadcasts an invalid transaction or block, the rest of the network would reject it and that node would fall out of consensus. Essentially, any node could attempt to create excess bitcoin, but every other node has an interest in ensuring the supply of bitcoin is consistent with the pre-defined fixed limit, otherwise the currency would be arbitrarily debased at the direct expense of the rest of the network.



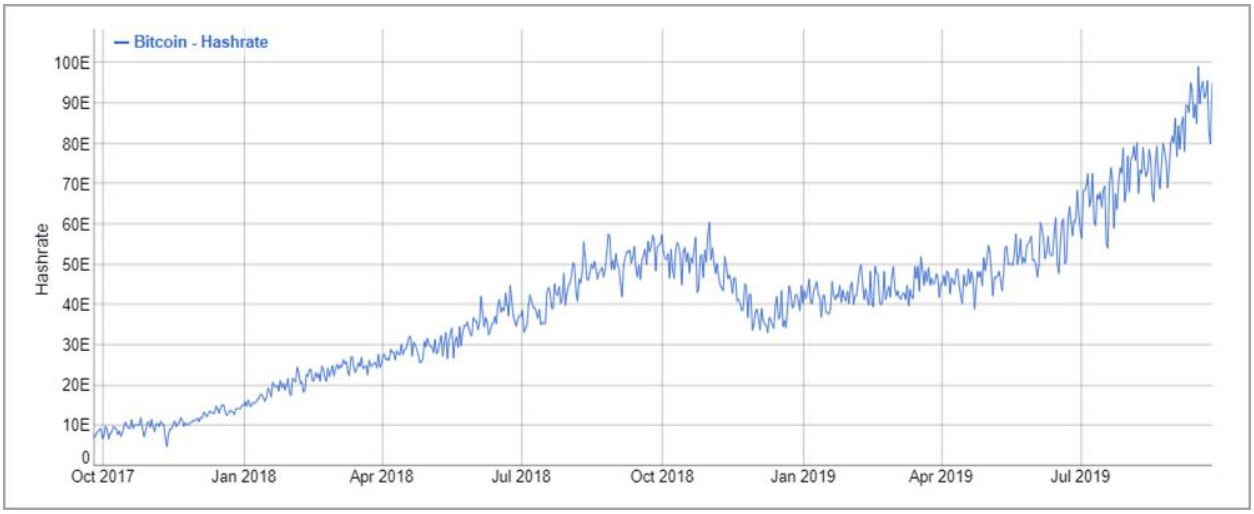
Separately, anyone within or outside the network could copy bitcoin's software to create a new version of bitcoin, but any units created by such a copy would be considered invalid by the nodes operating within the bitcoin network. Any subsequent copies or units would not be considered valid, nor would anyone accept the currency as bitcoin. Each bitcoin node independently validates whether a bitcoin is a bitcoin, and any copy of bitcoin would be invalid, as it would not have originated from a previously valid bitcoin block. It would be like trying to pass off monopoly money as dollars.

You can wish it to be money all you want, but no one would accept it as bitcoin, nor would it share the emergent properties of the bitcoin network. Running a bitcoin full node allows anyone to instantly assay whether a bitcoin is valid, and any copy of bitcoin would be immediately identified as counterfeit. The consensus of nodes determines the valid state of the network within a closed-loop system; anything that occurs beyond its walls is as if it never happened.

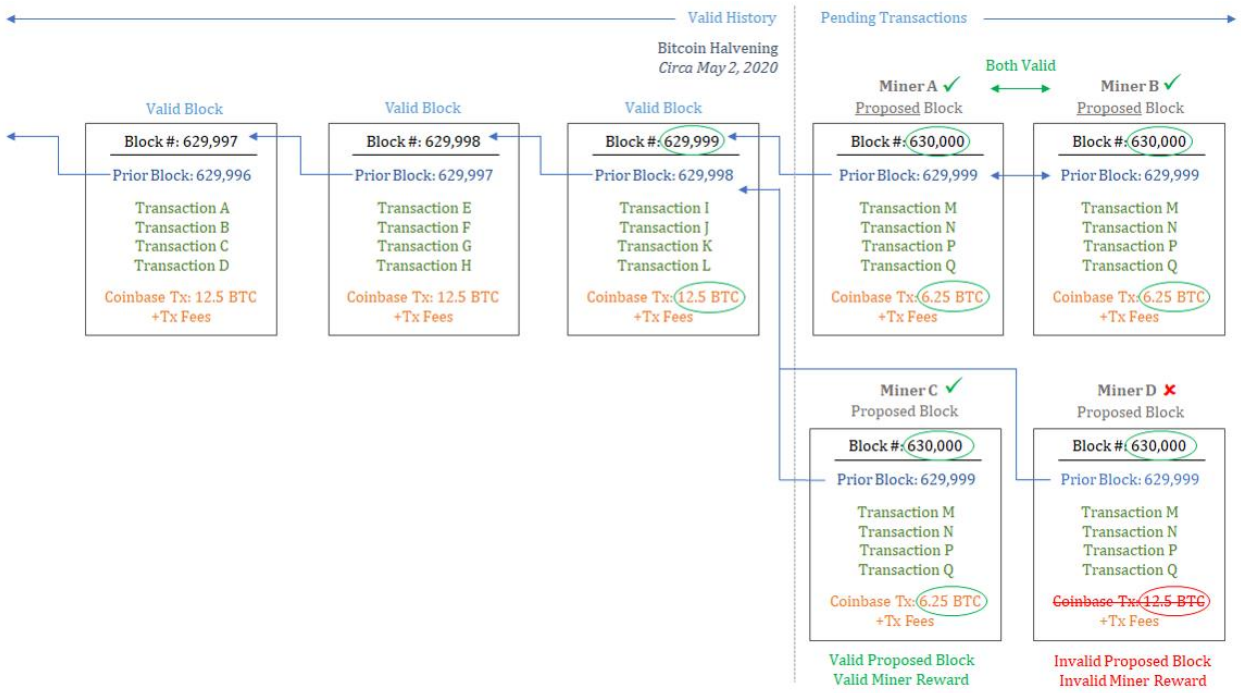
What Secures Bitcoin – Mining and Proof of Work

As part of the consensus mechanism, certain nodes (referred to as miners) perform bitcoin's proof of work function to add new bitcoin blocks to the blockchain. This function validates the complete history of transactions and clears pending transactions. The process of mining is ultimately what anchors bitcoin security in the physical world. In order to solve blocks, miners must perform trillions of cryptographic computations, which require expending significant energy resources. Once a block is solved, it is proposed to the rest of the network for validation. All nodes (including other miners) verify whether a block is valid based on a common set of network consensus rules discussed previously. If any transaction in the block is invalid, the entire block is invalid. Separately, if a proposed block does not build on the latest valid block (i.e. the longest version of the block chain), the block is also invalid.

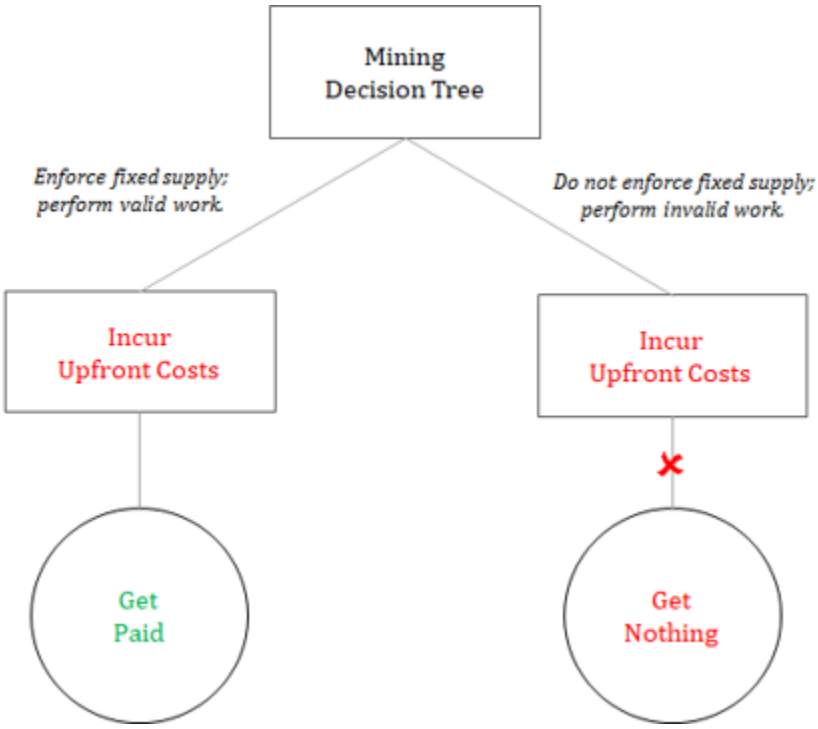
For context, at 90 exahashes per second, the bitcoin network currently consumes approximately 9 gigawatts of power, which translates to ~$11 million per day (or ~$4 billion per year) of energy at a marginal cost of 5 cents per kWh (rough estimates). Blocks are solved on average every ten minutes, which translates to approximately 144 blocks per day. Across the network, each block costs approximately $75,000 to solve, and the reward per block is approximately $100,000 (12.5 new bitcoin x $8,000 per bitcoin, excluding transaction fees). The higher the cost to solve a block, the more costly the network is to attack. The cost to solve a block represents the tangible resources it requires to write history to the bitcoin transaction ledger. As the network grows, the network becomes more fragmented, and the economic value compensated to miners in aggregate increases. From a game theory perspective, more competition and greater opportunity cost makes it harder to collude, and all network nodes validate the work performed by miners, which serves as a constant check and balance.



And recall that a pre-defined number of bitcoin are issued in each valid block (that is, until the 21 million limit is reached). The bitcoin issued in each block combined with network transaction fees represent the compensation to miners for performing the proof-of-work function. The miners are paid in bitcoin to secure the network. As part of the block construction and proposal process, miners include the pre-defined number of bitcoin to be issued as compensation for expending tangible, real world resources to secure the network. If a miner were to include an amount of bitcoin inconsistent with the pre-defined supply schedule as compensation, the rest of the network would reject the block as invalid. As part of the security function, miners must validate and enforce the fixed supply of the currency in order to be compensated. Miners have material skin-in-the-game in the form of upfront capital costs (and energy expenditure), and invalid work is not rewarded.



For a technical example, the valid reward paid to miners is halved every 210,000 blocks with the next halvening (a "technical" term) scheduled to occur at block 630,000 (or approximately in May 2020). At the time and scheduled block of the next halvening, the valid reward will be reduced from 12.5 bitcoin to 6.25 bitcoin per block. Thereafter, if any miner includes an invalid reward (an amount other than 6.25 bitcoin), the rest of the network will reject it as invalid. The halvening is important not just because the supply of newly issued bitcoin is reduced, but also because it demonstrates that the economic incentives of the network continue to effectively coordinate and enforce the fixed supply of the currency on an entirely decentralized basis. If any miner attempts to cheat, it will be maximally penalized by the rest of the network. Nothing other than the economic incentives of the network coordinate this behavior; that it occurs on a decentralized basis without the coordination of any central authority reinforces the security of the network.



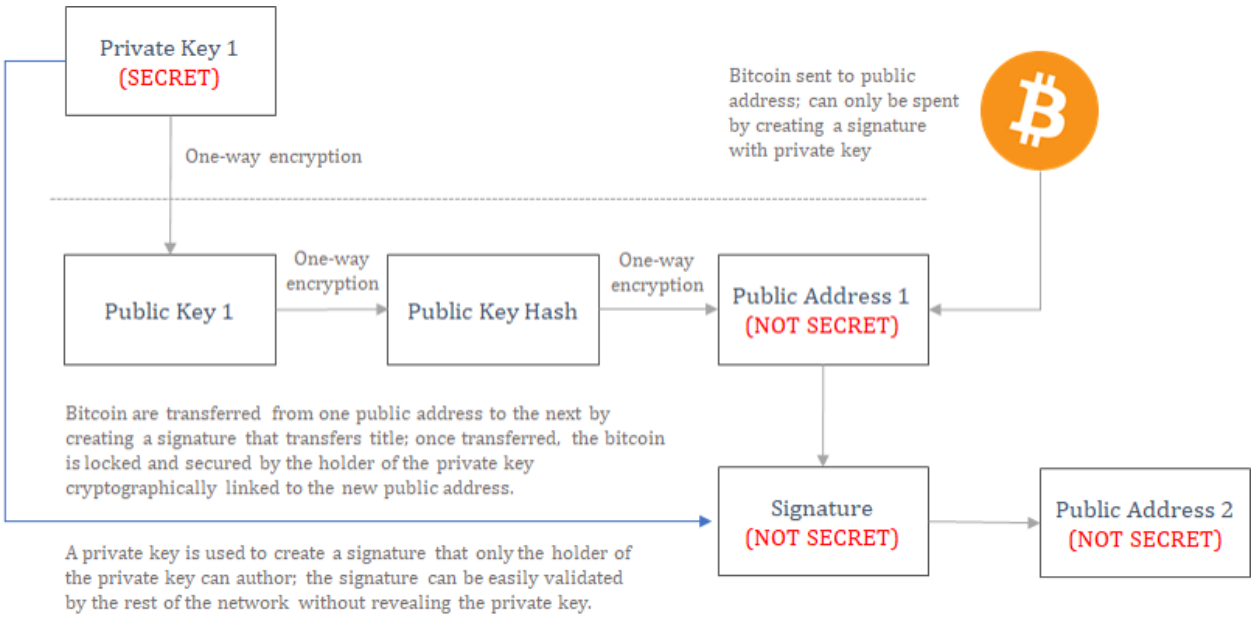
Because mining is decentralized and because all miners are constantly competing with all other miners, it is not practical for miners to collude. Separately, all nodes validate the work performed by miners, instantly and at practically no cost, which creates a very powerful check and balance that is divorced from the mining function itself. Blocks are costly to solve but easy to validate; in aggregate, this is a fundamental differentiator between bitcoin and the monetary systems with which bitcoin competes, whether gold or the dollar. And the compensation paid to miners for securing the network and enforcing the network's fixed supply is exclusively in the form of bitcoin. The economic incentives of the currency (compensation) is so strong and the penalty is both so severe and so easily enforced that miners are maximally incentivized to cooperate and perform valid work. By introducing tangible cost to the mining process, by incorporating the supply schedule in the validation process (which all nodes verify), and by divorcing the mining function from ownership of the network, the network as a whole reliably and perpetually enforces the fixed supply (21 million) of the currency on a trustless basis, while also able to reach consensus on a decentralized basis.

What Secures Bitcoin – Private Keys and Equal Rights

While miners construct, solve and propose blocks and while nodes check and validate work performed by miners, private keys control access to the unit of value itself. Private keys control the rights to the 21 million bitcoin (technically only 18.0 million have been mined to date). In bitcoin, there are no identities; bitcoin knows nothing of the outside world. The bitcoin network validates

signatures and keys. That is all. Only someone in control of a private key can create a valid bitcoin transaction by creating a valid signature. Valid transactions are included in blocks, which are solved by miners and validated by each node, but only those in possession of private keys can produce valid transactions.

When a valid transaction is broadcast, bitcoin are spent (or transferred) to specific bitcoin public addresses. Public addresses are derived from public keys, which are derived from private keys. Public keys and public addresses can be calculated using a private key, but a private key cannot be calculated from a public key or public address. It is a one-way function secured by strong cryptography. Public keys and public addresses can be shared without revealing anything about the private keys. When a bitcoin is spent to a public address, it is essentially locked in a safe, and in order to unlock the safe to spend the bitcoin, a valid signature must be produced by the corresponding private key (every public key and address has a unique private key). The owner of the private key produces a unique signature, without actually revealing the secret itself. The rest of the network can verify that the holder of the private key produced a valid signature, without actually knowing any details of the private key itself. Public and private key pairs are the foundation of bitcoin. And ultimately, private keys are what control access rights to the economic value of the network.



It doesn't matter whether someone has one-tenth of a bitcoin or ten thousand bitcoin. Either and each are secured and validated by the same mechanism and by the same rules. Everyone has equal rights. Regardless of the economic value, each bitcoin (and bitcoin address) is treated identically within the bitcoin network. If a valid signature is produced, the transaction is

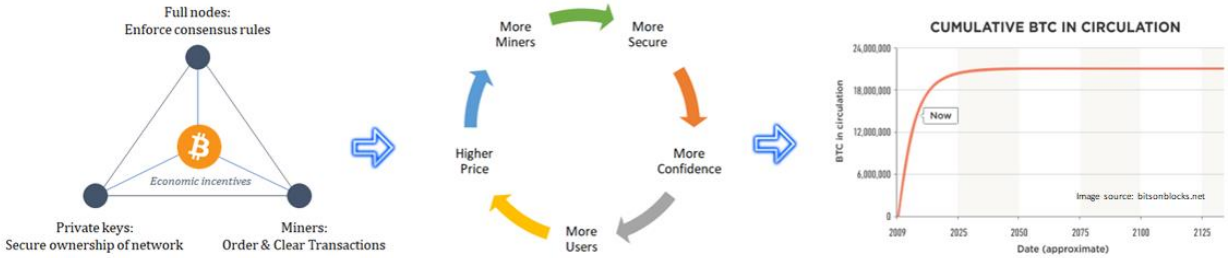
valid and it will be added to the blockchain (if a transaction fee is paid). If an invalid signature is produced, the network will reject it as invalid. It does not matter how powerful or how weak any particular participant may be. Bitcoin is apolitical. All it validates is keys and signatures. Someone with more bitcoin may be able to pay a higher fee to have a transaction prioritized, but all transactions are validated based on the same set of consensus rules. Miners prioritize transactions based on value and profitability, nothing else. If a transaction is equally valuable, it will be prioritized based on a time sequence. But importantly, the mining function, which clears transactions, is divorced from ownership. Bitcoin is not a democracy; ownership is controlled by keys and every bitcoin transaction is evaluated based on the same criteria within the network. It is either valid or it is not. And every bitcoin must have originated within a block consistent with the 21 million supply schedule in order to be valid.

This is why users controlling keys is such a significant ethos in bitcoin. Bitcoin are extremely scarce, and private keys are the gatekeeper to the transfer of every bitcoin. The saying goes: not your keys, not your bitcoin. If a third-party party controls your keys, such as a bank, that entity is in control of your access to the bitcoin network, and it would be very easy to restrict access or seize funds in such a scenario. While many people choose to trust a bank-like entity, the security model of bitcoin is unique; not only can each user control their own private keys, but each user can also access the network on a permissionless basis and transfer funds to anyone anywhere in the world. This is only possible if a user is in control of a private key. In aggregate, users controlling private keys decentralize the control of the network's economic value, which increases the security of the network as a whole. The more distributed access is to the network, the more challenging it becomes to corrupt or co-opt the network. Separately, by holding a private key, it becomes extremely difficult for anyone to restrict access or seize funds held by any individual. Every bitcoin in circulation is secured by a private key; miners and nodes may enforce that 21 million bitcoin will ever exist, but the valid bitcoin that do exist are ultimately controlled and secured by a private key.

Bitcoin versus.

In summary, the supply of bitcoin is governed by a network consensus mechanism, and miners perform a proof-of-work function that grounds bitcoin's security in the physical world. As part of the security function, miners get paid in bitcoin to solve blocks, which validate history and clear pending bitcoin transactions. If a miner attempts to compensate themselves in an amount inconsistent with bitcoin's fixed supply, the rest of the network will reject the miner's work as invalid. The supply of the currency is integrated into bitcoin's security model, and real world energy resources must be

expended in order for miners to be compensated. Still yet, every node within the network validates the work performed by all miners, such that no one can cheat without a material risk of penalty. Bitcoin's consensus mechanism and validation process ultimately governs the transfer of ownership of the network, but ownership of the network is controlled and protected by individual private keys held by users of the network.



Set aside any preconceived notions of what money is, and imagine a currency system that has an enforceably scarce and fixed supply. Anyone in the world can connect to the network on a permissionless basis and anyone can send transactions to anyone anywhere in the world; everyone can also independently and easily validate the supply of the currency as well as ownership across the network. Imagine a global economy where billions of people, disparately located throughout the world, can transact across one common decentralized network, and everyone can arrive at the same consensus of the ownership of the network, without the coordination of any central party. How valuable would that network be? Bitcoin is valuable because it is finite, and it is finite because it is valuable. The economic incentives and governance model of the network reinforce each other; the cumulative effect is a decentralized and trustless monetary system with a fixed supply that is global in reach and accessible by anyone.

Because bitcoin has inherent and emergent monetary properties, it is distinct from all other digital monies. While the supply of bitcoin remains fixed and finitely scarce, central banks will be forced to expand the monetary base in

order to sustain the legacy system. Bitcoin will become a more and more attractive option, as more market participants figure out that future rounds of quantitative easing are not just a central bank tool but a necessary function to sustain the alternate and inferior option. Before bitcoin, everyone was forced to opt in to this system by default. Now that bitcoin exists, there is a viable alternative. Each time the Fed returns with more quantitative easing to sustain the credit system, more and more individuals will discover that the monetary properties of bitcoin are vastly superior to the legacy system, whether the dollar, euro or yen. Is A better than B? That is the test. In the global competition for money, bitcoin has inherent monetary properties that the fiat monetary system lacks. **Ultimately, bitcoin is backed by something, and it's the only thing that backs any money: the credibility of its monetary properties**.

Next week: Bitcoin is Not a Pyramid Scheme

Views presented are expressly my own and not those of Unchained Capital or my colleagues. Thanks to Phil Geiger, Adam Tzagournis and Will Cole for reviewing and for providing valuable feedback.

To subscribe to weekly releases of *Gradually, Then Suddenly*, please click here.

Tweetstorm: We've Built Intermediaries

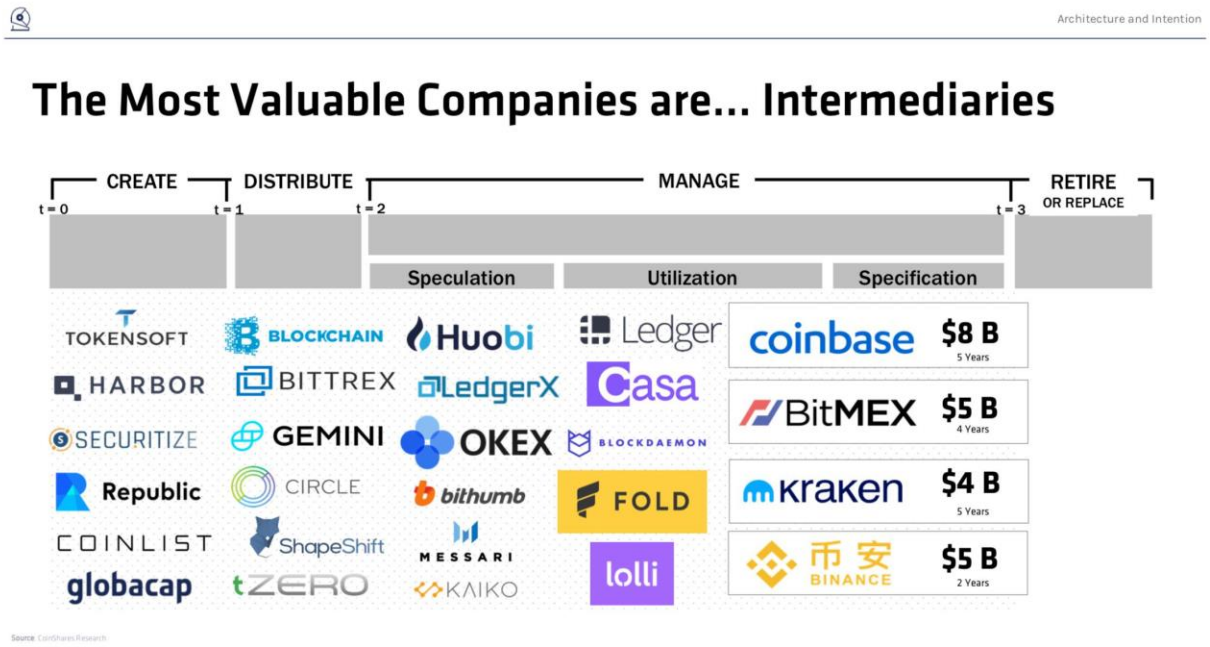
By Meltem Demirors

Posted Septemeber 27, 2019

1/ in the crypto community, we love to talk about things like

- choice and access
- self-sovereignty
- privacy and consent
- removing rent-seeking

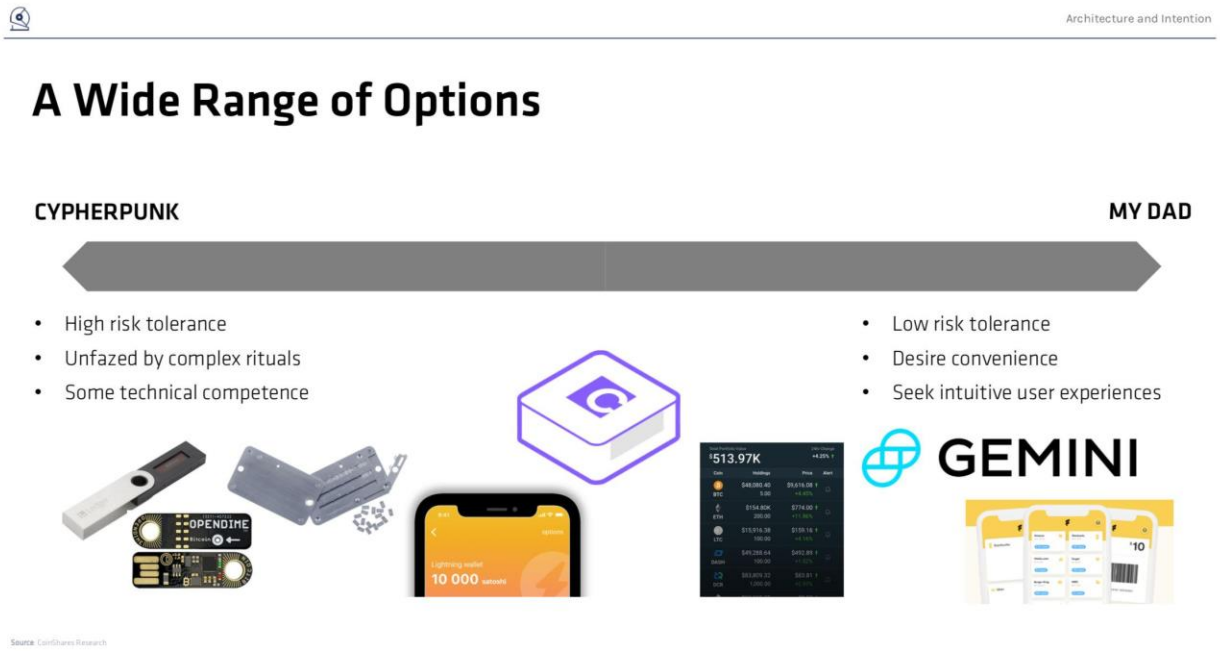
but when we take a hard look at what we've built... the majority of value in our industry is being captured by intermediaries



2/ there are new business models emerging on both the "cypherpunk" end of the spectrum and the "my dad" end of the spectrum... but at the end of the day, it's all about who controls the coins

coin = power

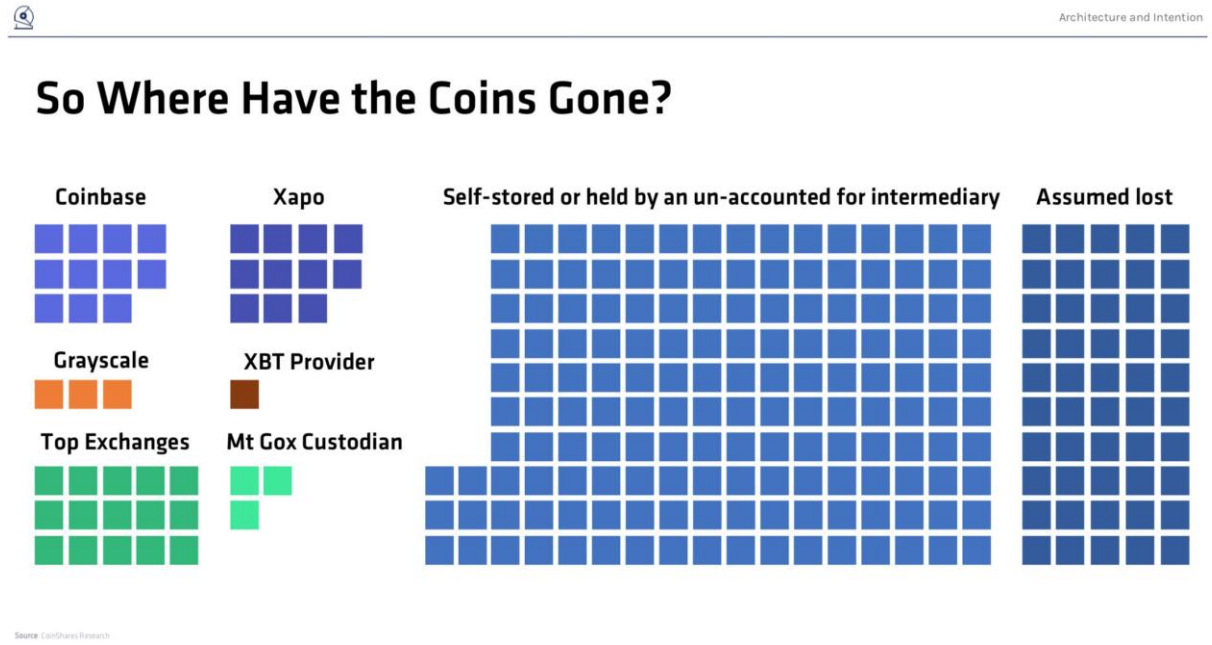
not your keys, not your coins



3/ so where are the coins?

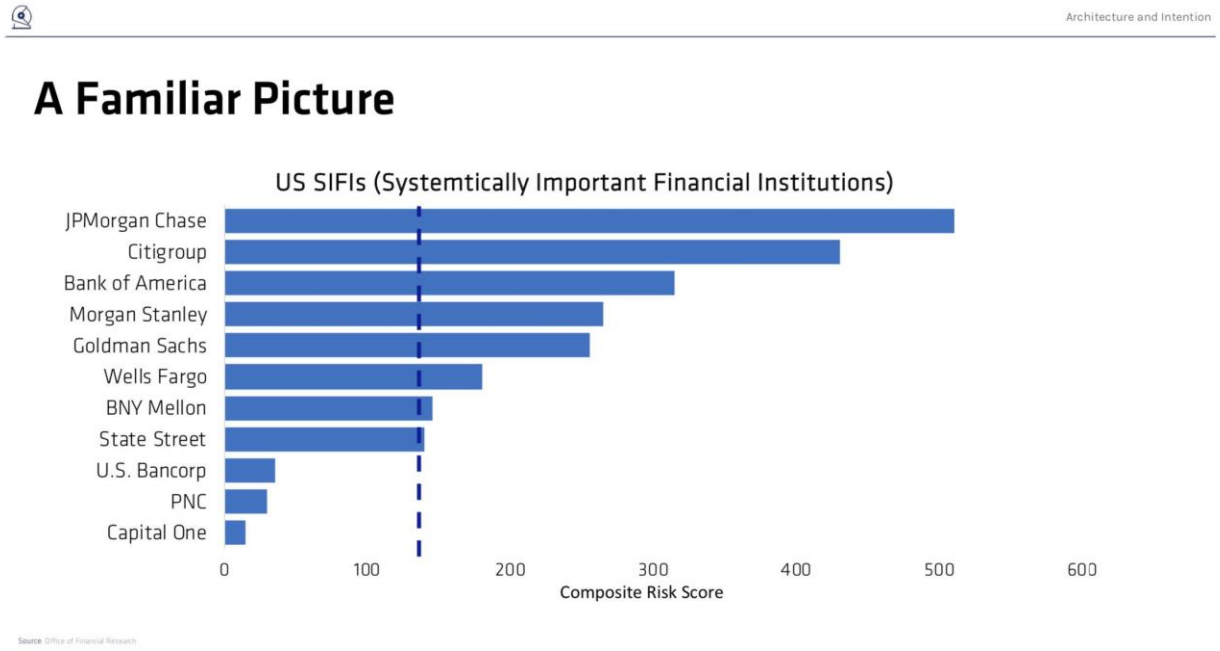
if 100% is all bitcoin mined to date, roughly 17% is in third party custody (although the number is likely higher)

that's pretty significant



4/ why does this matter? well, history usually helps us understand what the future might look like.

in response to the financial crisis, the US government created a new designation for financial institutions - one called a SIFI or systemically important financial institution



5/ when you have a small number of firms holding a large number of assets, you centralize risk

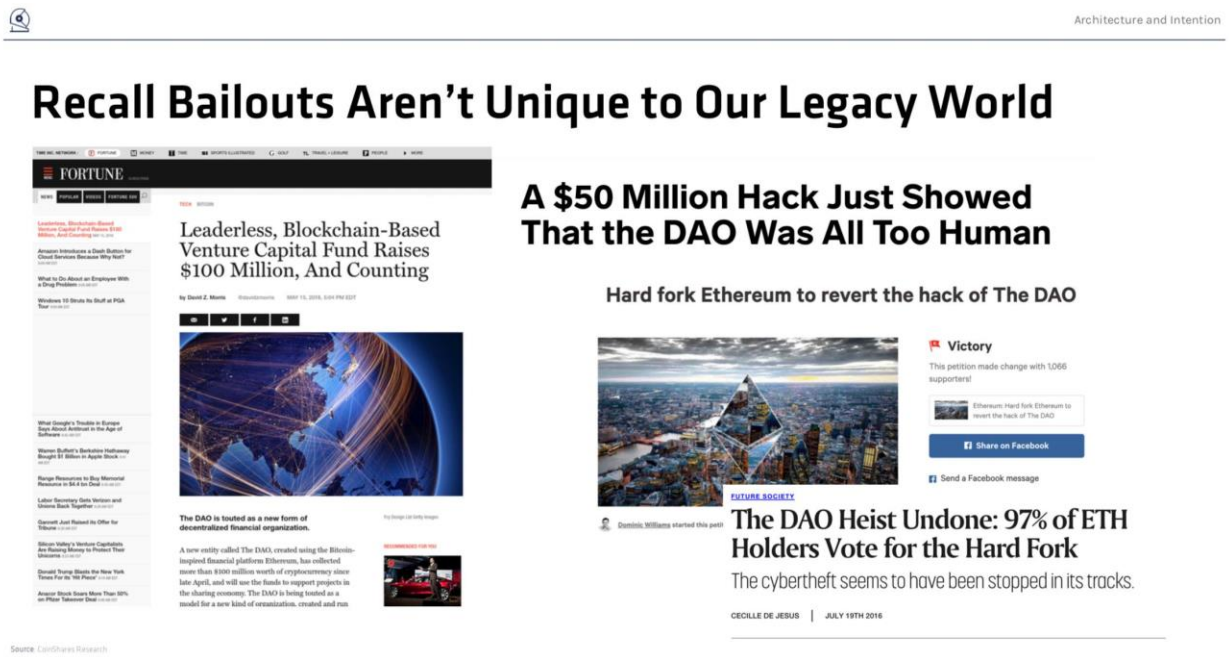
with legacy finance, this is dangerous but not deadly.

with bitcoin, this is both dangerous and potentially deadly. what happens when a large intermediary gets hacked?

6/ well fortunately, we have history as a guide.

bank bailouts are common. crypto bailouts have also happened (see DAO below)

in May, when Binance's hot wallet holding 0.03% of all bitcoin in circulation was hacked, a chain roll-back was suggested and discussed and rejected.



7/ what happens when an intermediary holding 5% of all bitcoin gets hacked? what about 10%?

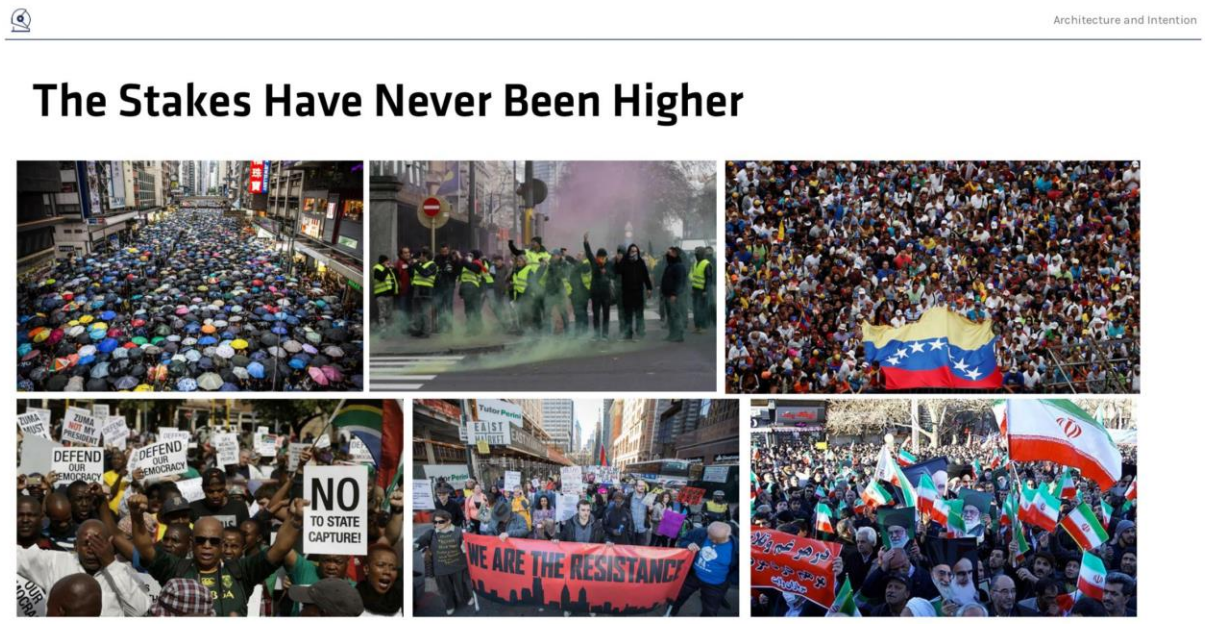
what happens when institutions put bitcoin in cold storage and start trading paper bitcoin depository receipts (BDRs) instead of actual coin?

... is that still bitcoin?

8/ i'm not so sure.

bitcoin is a cultural movement. bitcoin is for people. bitcoin is about principles.

how do we allow for more participation via intermediaries without losing the message? curious to hear what you think.



9/ lastly, these snippets are part of a longer talk on architecture and intentions. will share video link when ready.

you may think you took the red pill, but actually, you're colorblind and it's blue...

enjoy that mental wormhole!

Disclaimer:

WORDS

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

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

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

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

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

DYOR | BTFD | HODL

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

- @_joerodgers