May 2018

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.

The Future of Bitcoin: What Lightning Could Look Like

By Aaron van Wirdum

Posted May 2, 2018

After years of conceptualization and development, the first Lightning implementations are now in beta. As a result, more nodes are appearing online every day, a growing number of users are opening channels with one another, and some merchants even started to accept Lightning payments.

But of course, these are still the very early days of the Lightning Network. While the main implementations are usable and some wallets and other applications are available, Bitcoin's overlay payment network is projected to improve over the next few years in areas ranging from network architecture to security and usability, and more.

These are some of the more important Lightning projects currently in development.

Dual-Funded Channels

The Lightning Network consists of a series of payment channels. Each payment channel exists between two users, allowing funds to be sent back and forth between them.

However, in this early stage of development, payment channels can only be funded by one of the two parties. The funding party must first make a transaction to his counterparty; only then can that counterparty return a payment within the same payment channel.

The Lightning Network white paper, however, proposed dual-funded channels, for which a specification proposal has now also been made by ACINQ, the company behind eclair. As the name suggests, dual-funded channels will let both users partly fund a payment channel by each depositing some bitcoin. This should bring more flexibility to the Lightning user experience, as users can immediately send as well as receive payment after having opened a channel.

Submarine Swaps

In order to make a Lightning payment, users must deposit funds in a Lightning channel. Once in a channel, these funds cannot be sent to regular (on-chain) Bitcoin

addresses (unless the channel is first closed). This means that bitcoin in a Lightning channel is somewhat separated from bitcoin in a regular wallet, not unlike how money in a checking account is somewhat separated from money in a savings account.

But there are solutions to make switching between Lightning and on-chain payments more seamless.

One solution is Submarine Swaps. Developed by Alex Bosworth (but conceptualized by Lightning Labs CTO Olaoluwa Osuntokun even before that), Submarine Swaps essentially let users send Lightning payments to a middleman on the Lightning Network; that middleman will send a corresponding amount of bitcoin to a regular (on-chain) Bitcoin address. It also works the other way around: users can send regular on-chain payments to the middleman; that middleman will then send a corresponding amount of bitcoin to a receiving Lightning node on the Lightning Network.

Importantly, with Submarine Swaps, this conversion is done "atomically." Using a trick that is already embedded in the Lightning Network, the Lightning payment and the on-chain payment can effectively be linked to each other. This makes it impossible for the middleman to steal funds by not forwarding the payment. (In agreement with the users, he could charge a small fee for his service.)

Splicing

Another solution to make the Lightning user experience more seamless is called "splicing." In essence, splicing would let a user "top up" funds in an existing Lightning channel, or "drain" funds from it, potentially while keeping the channel open.

The idea is simple. Any Lightning channel starts with an opening transaction, which ensures that both users consent to moving the funds in the channel. The rest of the Lightning channel consists of a series of subsequent transactions exchanged between the users, which aren't usually broadcast to the Bitcoin network. The funds in the opening transaction don't move until the channel is closed.

When "splicing in," users take the opening transaction to instead send funds to a replacement opening transaction, which includes more bitcoin, from one or both users. Once this new opening transaction confirms on the blockchain, the channel is topped up. Until the new opening transaction is confirmed, the two users can simply update both the old and the new channel at the same time to avoid any "channel downtime."

Conversely, when they "splice out," users take the opening transaction to send funds to a regular (on-chain) address, and potentially keep some of it in the channel using

the same trick. This way, users can make on-chain transactions straight out of a Lightning channel.

Eltoo

Each time a new payment is made, Lightning channels between users are updated to reflect their mutual balances. The trick used to accomplish this currently includes a penalty for users who try to cheat by broadcasting an older balance (presumably because that older balance would pay them more). Cheating users can lose all the funds they have in a channel.

The problem is that the broadcasting of old balances is not always a cheating attempt. There are a number of scenarios in which users can accidentally broadcast an older balance; for example, because of a software bug or a backup gone wrong. In such scenarios, a complete loss of channel funds is quite a heavy punishment.

First published on April 30, 2018, eltoo is the newest proposal featured in this article. Developed by Blockstream's c-lightning development team — Dr. Christian Decker and Rusty Russell — and Lightning Labs' Osuntokun, eltoo updates a channel by building a chain of time-locked transactions, where each transaction spends funds from the previous one to reflect the latest channel balance.

If one user broadcasts an older transaction (representing an older channel balance), her counterparty has some time to broadcast the latest transaction (representing the latest channel balance).

A solution like this could work today, but it isn't practical in cases of failure. It would require that the entire chain of transactions be broadcast and recorded on the Bitcoin blockchain, more or less defeating the purpose of the Lightning Network. Decker therefore proposed a soft-fork change to the Bitcoin protocol to introduce a type of hierarchy in these types of transactions: any newer transaction can override any older transaction without requiring that all transactions in the entire chain be broadcast.

If this soft fork is adopted and activated on the Bitcoin network, Lightning users could create channels in both the current style and by using eltoo, depending on what they prefer.

Compact Client-Side Block Filtering

While the Lightning Network is a second-layer protocol, the Bitcoin blockchain itself is still relevant for Lightning users for security purposes. Specifically, Lightning users must keep an eye on the blockchain to see if specific transactions are included. This can be resource intensive, in particular for mobile users.

A solution for this is called Simplified Payment Verification (SPV) and was described in the Bitcoin white paper. Current SPV wallets use a trick called "Bloom filters " to find out whether any relevant transactions happened.

Unfortunately, Bloom filters are rather privacy-unfriendly, as wallets essentially reveal all of their addresses to nodes on the Bitcoin network. They also have some scaling and usability issues, as each individual SPV wallet takes up resources from at least one full Bitcoin node.

To tackle these issues, Lightning Labs' Osuntokun and Alex Akselrod, along with Coinbase developer Jim Posen, designed a new solution called "compact client-side block filtering," which they are implementing in the Neutrino wallet.

Compact client-side block filtering essentially inverts the trick that current SPV wallets use. Instead of wallets requesting transactions relevant to them by creating and sending out a Bloom filter to full nodes, full nodes create a filter for all Neutrino wallets. The Neutrino wallet then uses this filter to establish that the relevant transaction did not happen — which is really all that users need to know to be sure they are not being cheated. (If the filter produces a match, Neutrino fetches the relevant block to see if the match really concerns the exact transaction instead of a false positive.)

Interestingly, while this trick was designed with the Lightning experience in mind, it could be utilized to benefit regular light wallets as well.

Watchtowers

To avoid being cheated, Lightning users must keep track of potential on-chain transactions that could be relevant to them.

While compact client-side block filtering should make things much easier, users do need to "check in" once in a while to make sure they're not being cheated. If they forget to check, it creates a security risk.

"Watchtowers" are a potential solution that can be traced back to the Lightning Network white paper and has since been improved by Lightning Network white paper co-author and lit developer Tadge Dryja and others. As the name suggests, Watchtowers could let users outsource blockchain monitoring to third parties.

Current Watchtower designs are not set in stone but would roughly work like this. Whenever users update a channel, they send a small data package to a Watchtower. The first part of this package is a "hint" of a transaction they should look out for, as if it were a piece of a puzzle. This hint alone doesn't reveal anything about the content of the transaction that the Watchtower must look out for; users don't give up any privacy in this sense.

However, if the relevant transaction shows up in the Bitcoin blockchain, the Watchtower can use the hint to recognize it. Then, with the transaction data on the blockchain itself, the Watchtower can use the second part of the package they've received to reconstruct the penalty transaction. This penalty transaction sends all funds in the channel to the user that is being cheated. (Or in the case of eltoo, it just broadcasts the correct channel balance.) The penalty transaction can also be designed to let the Watchtower claim part of the funds as a reward, as an incentive to do its job.

Users can outsource channel monitoring to multiple Watchtowers. Even if one fails, another might not, limiting the risk for Lightning users to the point where it's arguably negligible.

Atomic Multi-Path Payments

What makes the Lightning Network a *network* is that the payment channels between users are interconnected. Users can pay across payment channels, through peers on the network that act as "middlemen," to users they don't have a direct channel open with.

However, right now a single payment must be routed over a single route. If one user wants to pay 5 mBTC to another, not only must he have 5 mBTC in a single channel, all the middlemen on the route must also have 5 mBTC ready in a channel to forward. The bigger a payment is, the smaller the odds of this being the case.

Atomic Multi-Path Payments (AMPs) could go a long way of solving this limitation. First proposed by Lightning Labs' Osuntokun and Conner Fromknecht, the idea is simple: Larger payments can be "cut up" into smaller pieces, all of which have their own route from the payer to the payee, through different middlemen.

A challenge to realize this solution is that Lightning payments can fail, which would in this case mean that a payment is made partially. Partial payments can easily be a bigger problem than no payment at all, however: a merchant won't be satisfied with a partial payment, while a customer won't be happy spending any money for nothing.

The solution to this problem is that AMPs use an extension to the hash time-locked contracts, which are already used along Lightning routes and involve passing secret data along a network. Using a trick similar to the one used by deterministic wallets (which generate multiple Bitcoin addresses from a single seed), the smaller pieces of a larger payment can only be redeemed by the payee if all of them are: if some secret data doesn't make it through the route whole, the entire payment fails.

Atomic Swaps

The Lightning Network is designed as a scaling layer for Bitcoin. But since many altcoins are software forks of Bitcoin's codebase(s), it's often not difficult to create similar scaling layers for these altcoins. Already, a small Litecoin Lightning Network exists, and more Lightning Networks are likely to follow.

Interestingly, these networks don't need to remain separated in the future.

Using a fundamental building block of the Lightning Network called "atomic swaps" (first proposed by Tier Nolan and realized on Lightning by Lightning Labs' Fromknecht), payment channels can be linked across different blockchains. In other words, a user can send bitcoin, and as long as a node on the network is willing to make the exchange, another user can receive the payment as litecoin.

Of course, this also means that users can send such payments to themselves: they can send bitcoin and receive litecoin. In effect, the Lightning Network could establish a network of trustless cryptocurrency exchanges. *For more information on this topic, see: "Atomic Swaps: How the Lightning Network Extends to Altcoins."*

Channel Factories

The main benefit of the Lightning Network is arguably its potential to vastly increase the upper limit of bitcoin transactions without burdening the Bitcoin network. As long as two users both have funds in their channel, they can pay each other a virtually unlimited number of times, while only requiring two on-chain transactions: one to open a payment channel and one to close it.

Still, two transactions per payment channel could add up if Bitcoin and the Lightning Network gain more adoption over time.

A proposal by ETH Zurich researchers Christian Decker (also of Blockstream), Roger Wattenhofer and Conrad Burchert called "Channel Factories" could further decrease the average number of on-chain transactions required per payment channel, perhaps significantly.

Loosely based on an earlier Lightning-like proposal by Decker and Wattenhofer from 2015, Channel Factories are a type of payment channel that can exist among many users. Meanwhile, like any payment channel, a Channel Factory only ever requires two on-chain transactions. (If Schnorr signatures are implemented on Bitcoin, these transactions could be quite compact, even if it involves many users.)

The Channel Factories can, in turn, act sort of like "sub-channels" for the Lightning Network. Participants within a Channel Factory can open and close a virtually unlimited number of Lightning channels with each other, without requiring any

additional on-chain transactions. By doing so, they could, in theory, bring the number of required on-chain transactions for the Lightning Network down by a magnitude. *For more information on this topic, see: "This New Scaling Layer Could Make Payment Channels Ten Times More Effective".Thanks to Blockstream developer Christian Decker, Lightning Labs developer Conner Fromknecht, ACINQ CEO Pierre-Marie Padiou and others for information and feedback.*

The Internet's Magna Carta Moment: Bitcoin & The Value of Strong Assurances

By Spencer Bogart

Posted May 20, 2018

Symbolically, the Magna Carta marked a long-standing movement toward broader applicability of rule-of-law (Kings and Nobles not immune to rule of law) and people's rights (rights for everyone, not just the elite).

By providing stronger assurances regarding property rights and rule-of-law, this movement changed economic incentives in favor of investment and growth which ultimately, hundreds of years later, led to the UK's Bill of Rights, the industrial revolution, and a vast improvement in the human condition.

Similarly, highly decentralized networks are providing an open foundation with strong assurances for objective property rights, impersonal rules and consistent enforcement.

An important difference, however, is that with the Magna Carta, the powers on high decided to relinquish some of their privileges and rights — first to nobles and elites and, eventually, to everyone.

In contrast, highly decentralized networks are constructing these rights in reverse — starting from the ground up with the "every-man". These networks don't ask for the king's permission to exist and facilitate the rights they offer — they simply *are.*

A profound implication

A profound implication of some highly decentralized networks is the opportunity, at scale, to deliver stronger assurances than even the largest nation-states today — and in doing so to offer a robust, digital foundation for economic growth.

The Bitcoin network, for example, is a self-contained, rules-based, self-arbitrating court where valid transactions are clearly defined, objectively verifiable, and unerringly enforced by network participants. More on that to follow, but we're getting ahead of ourselves…

WTF are "strong assurances"?

First, what do we mean by "strong assurances"?

Simply put, "strong assurances" means "the rules are the rules" and they will be enforced consistently and objectively. In practice, we're also talking about defining and enforcing property rights: Your exclusive right to determine the use of a good, earn income from the good and to transfer the good to others.

Why strong assurances matter

Overall, property rights and "strong assurances" may sound like a mundane topic, but property rights are a foundational component of economic growth and a primary explanatory variable for understanding differences in growth outcomes between jurisdictions.[1] [2] [3] [4]

Intuitively, it makes sense: Innovators and builders take their ability and ingenuity to where they can build with the least uncertainty. The greater the risk of unexpected outcomes or enforcement (rule-changes, asset seizures, etc), the less inclined builders are to incur the risk of operating on a particular platform or country. This intuition is supported unequivocally by the growth trajectories of countries that have provided the strongest assurances and property rights for participants.[1]

Said differently, strong assurances are valuable in that they de-risk economic activity and, consequently, encourage growth. If it were an actionable trade, investors would have been handsomely rewarded by "going long" jurisdictions that offered strong property rights over the past 100 years — these jurisdictions account for most of the world's economic growth over the same period.

In particular the main transmission channels that lead from strong property rights and consistent rules-enforcement to economic growth include:

1. **Reducing the risk of expropriation**: More likely to invest time, money and labor when the fruits of such efforts are less likely to be seized unexpectedly.

2. **Reducing the risk of unfavorable rule changes**: Investors and operators are more likely to invest and build when the rules of the system are less likely to shift beneath their feet.

3. **Reducing the cost of protecting assets**: If ownership is ill-defined, participants must allocate greater time and resources to engaging in activities that *might* subsequently define ownership (or risk that others will). For example, if private keys define ownership, then users can focus time toward securing private keys (instead of myriad activities that might subsequently redefine ownership).

4. **Increasing the opportunities to realize gains from trade:** With clearly defined and publicly recognizable property rights, owners can engage in contractual arrangements for the asset and more fully utilize the asset to maximize value production.

Strong assurances in a digital, decentralized context

As we move to a world where people increasingly build in the cloud, economic activity will migrate to a digital equivalent: an accessible digital foundation that offers strong assurances and consistently enforces clearly defined (digital) property rights. Such a platform will be increasingly valuable as the frontier of economic activity pushes further into the digital world.

Considering there's billions of dollars and millions of man-hours dedicated to building the parallel world of crypto-finance, the foundational platform(s) — the highly decentralized networks — that underpin it all are mission critical. The networks that attract and retain builders in the medium to long-term will be the ones that deliver a track record of strong assurances — a track record of consistent and objective rule enforcement.

Historically, strong assurances of this sort have only been possible via strong and credible central authorities that commit to defending stated rights and rules with vast resources (e.g. powerful nation states).

Interestingly though, once we depart from a strong centralized authority, strong assurances might only be possible at the other end of the spectrum: via highly decentralized networks. The middle ground — quasi-decentralized networks — will likely be co-opted by economic and social pressures in such a way that they present an inferior option (weak assurances) relative to both centralized and highly decentralized alternatives (more on that here: The Long Game in Crypto- Why Decentralization Matters).

A network of strong assurances: Bitcoin as an institution for digital property rights

Bitcoin, for example, offers a self-contained, reliable foundation for property rights in a digital world. The Bitcoin network is a rules-based, self-arbitrating court — it's likely the fairest, most transparent and most predictable court in the world.

This is due, in no small part, to the fact that the Bitcoin network intentionally limits its scope to enforcing a minimal set of functions. This deliberately limited network scope offers participants greater predictability in the outcome and enforcement of network activity: Valid transactions are clearly defined, objectively identifiable, and unerringly enforced by the network.

In this way, the Bitcoin network is a decentralized institution that defines, monitors, and enforces property rights. It is a reliable foundation of strong assurances on top of which we can efficiently architect arbitrary degrees of complexity and allow innovation and economic growth to flourish.

Tying it all together

Ultimately, strong assurances are fundamental to human progress as most economic growth has gravitated toward and emanated from jurisdictions that offered strong property rights coupled with consistent rules and enforcement.

In the jurisdiction of the Cloud — which is witnessing unprecedented growth in economic activity — highly decentralized networks are taking the notion of strong assurances even further:

· **Global in nature**: The strong assurances offered by highly decentralized networks like Bitcoin are global in nature (whereas, historically, strong assurances have been limited by geography and citizenship).

· **Clearly defined**: The Bitcoin network's rules are clearly defined whereas most historical rights and rule-sets have left ample room for subjective interpretation — an additional element of risk.

· **Perfectly Enforced**: The Bitcoin network enforces its rule-set objectively and unerringly — something every justice system ostensibly seeks to accomplish, but none have delivered on.

In the end, highly decentralized networks like Bitcoin offer a fertile foundation for economic growth in the digital world and will likely be important underpinnings of our increasingly digital economy. Much like how, at the turn of the 20th century, jurisdictions that offered strong assurances for economic activity were at the center of innovation and growth, so too will highly decentralized networks like Bitcoin that offer strong assurances prove to be fruitful for growth and development of the digital world.

Sources:

[1] Claessens Stijn and Luc Laeven. "Financial Development, Property Rights, and Growth." Journal of Finance. 2003 December: 58(6): 2401–2436.

[2] Kerekes, Carrie and Claudia Williamson. Unveiling de Soto's mystery: property rights, capital formation, and development. Journal of Institutional Economics. 2008 December: 4(3): 299–325.

[3] North, D. (1990), Institutions, Institutional Change and Economic Performance, Cambridge: Cambridge University Press.

[4] Acemoglu, Daron and Johnson, Simon and Robinson, James A. "Institutions as a Fundamental Cause of Long-Run Growth". Handbook of Economic Growth, Volume 1A. MIT.

Rethinking Metcalfe's Law applications to cryptoasset valuation

Introducing Network Value to Metcalfe (NVM) ratio and using it to identify and predict price bubbles

By Dmitry Kalichkin

Posted May 21, 2018

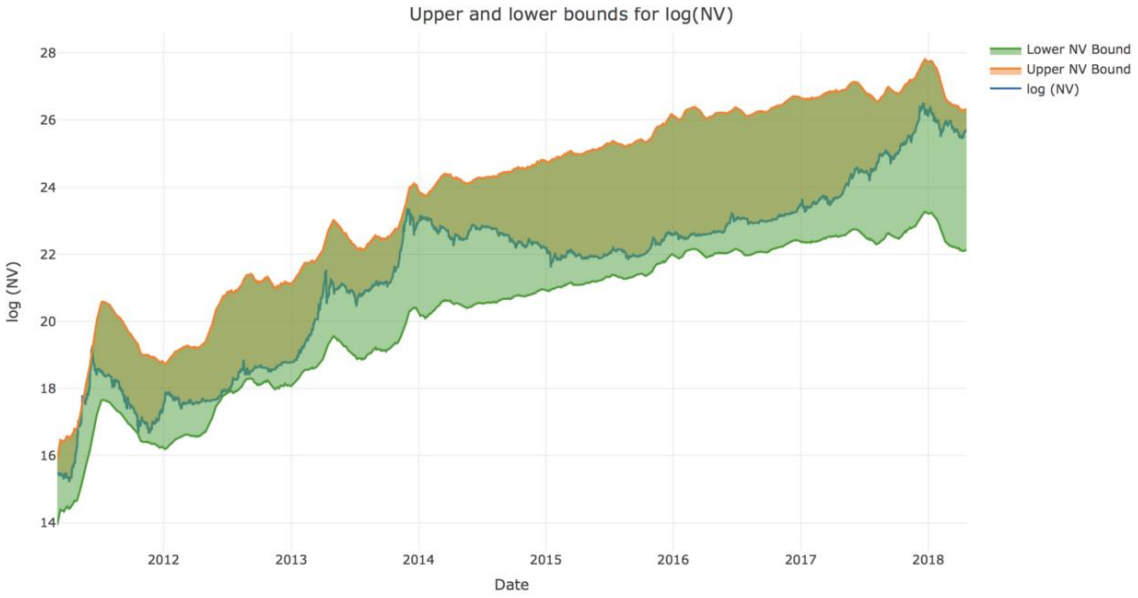
This is the second article from our series on cryptoasset valuation techniques. The first article is Rethinking Network Value to Transactions (NVT) Ratio .

For cryptoasset investors the first quarter of 2018 has been drastically different from 2017. Following a truly remarkable (albeit, not 100% healthy) 60x appreciation in 2017, the crypto market has experienced a strong correction, falling 58.2% from an opening $612bn in total network value on January 1st, to $256bn at the end of Q1. In April, the markets have turned around and regained some of these Q1 losses. Following all this volatility, right now many investors are puzzled by the question as to whether this is the end of price corrections, or just a temporary reprieve.

To answer this question Cryptolab Capital uses a data-driven approach to cryptoasset valuations and looks at the fundamental foundations of asset prices. In our February article *Rethinking Network Value to Transactions (NVT) Ratio* we shared one of the quantitaive metrics that we use. Today I'm excited to tell you about how we use Metcalfe's Law for cryptoasset valuation and investment decisions, and to introduce the **Network Value to Metcalfe ratio (NVM)**.

Summary

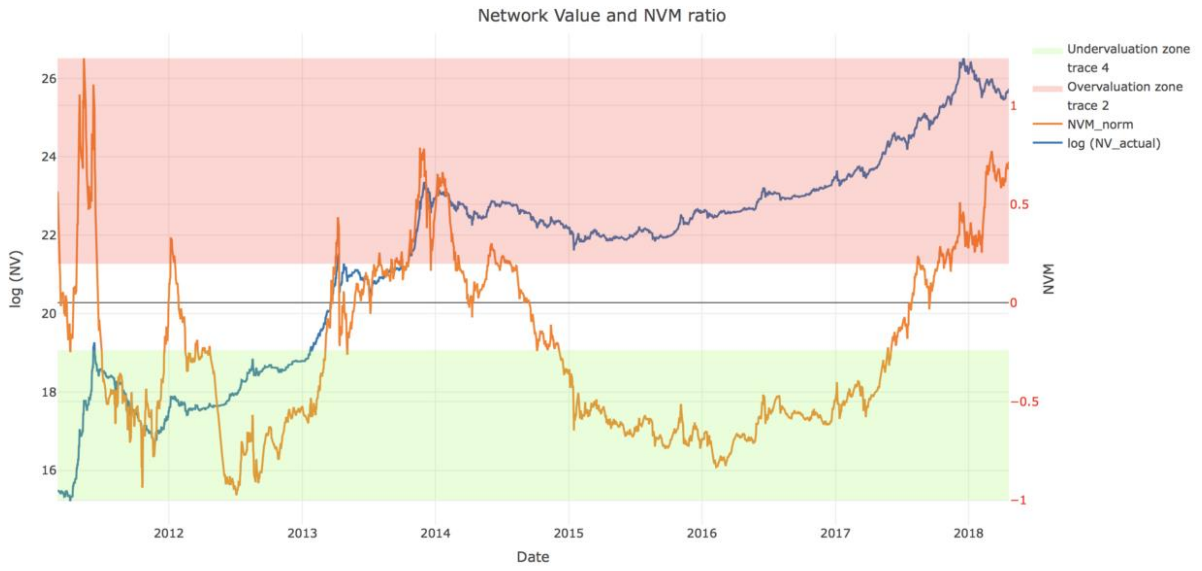
Our goal was to estimate whether current Bitcoin price is supported by activity on the network. To do this we have built robust upper and lower bounds for Bitcoin Network Value, based on a number of Daily Active Addresses (DAA), using different variations of Metcalfe's Law. Using these bounds, we have defined bottom-up valuation of the Bitcoin network as a function of DAA.



When we compared this valuation with actual market Network Value across different time periods, we have found that historically overvaluation can be predicted by Network Value to Metcalfe (NVM) ratio:

$$NVM = ln(NV_{actual}) - ln(NV_{Metcalfe}) = ln\left(\frac{NV_{actual}}{NV_{Metcalfe}}\right)$$

We analyzed current (as of early May 2018) Bitcoin price using this NVM ratio, and came to the conclusion that **despite significant correction in Q1 2018, there might be another bubble (and following correction) on the horizon.**



Having said this, while we see a risk of correction, we stay bullish on Bitcoin price in the long run.

Metcalfe's Law: how it all began

Cryptoassets are networks of users connected in digital space. Users can interact with each other by exchanging information and engaging in transactions. Due to the fact that these networks are digital, always online, and published on the the blockchain, network usage data is more readily available than for other types of networks (telephone, fax, messengers, and social media). Transaction data availability combined with public crypto markets create a unique opportunity to analyze and value these networks in real time.

Nearly four decades ago, Xerox Palo Alto Research Center (PARC) employee Robert Metcalfe proposed arelationship between the value of a network and its size(Metcalfe, 2013). He stated that the value of the network is proportional to the square of the network nodes (users). This relationship is based on the so-called "network effect": a positive effect described in economics and business that an additional user of a product or service increases its value to others. The original Metcalfe's Law has the following form:

$$Network\ Value_t = C * n_t^2$$

The logic behind this formula is the following: the number of unique connections in a network with n nodes can be expressed as ***n(n – 1)/2***, which is proportional to n^2 asymptotically.

Over time, some variations of this law were proposed. For example, Andrew Odlyzko et al. noticed that Metcalfe's Law estimates a number of *potential_connections between users of the network, while, in fact, there are certain limitationsto how many _useful* connections one user can have. He proposed to use ***n * log n*** instead of n^2 for network value estimation for large ***n***. There were multiple other modifications to the original law. Some researchers have successfully applied the law to describe Facebook and Tencent user growth and financial metrics.

Usage in cryptoasset valuation

Over the past year, a lot of research has been done on the topic of valuing cryptoassets using Metcalfe's Law. Cryptolab Capital research on Metcalfe's Law was initially inspired by Thomas Lee of Fundstrat, who has stated back in November 2017 that 94% of Bitcoin price movement can be explained by Metcalfe's Law.

We decided to dig deeper and have found an earlier paper on the topicpublished by Ken Alabiin June 2017. In all these articles the number of network users is usually approximated by the number of **Daily Active Addresses** (DAA). For internet companies with strong network effects, the analogous Daily Active Users (DAU) indicator is one of the most important performance and valuation metrics.

One of the recent articles on the topic by the Clearblocks team explored in detail how well different versions of Metcalfe's Law describe Bitcoin price. Their research revealed 3 candidates for the title of "the most predictive model":

1. Original Metcalfe's Law: NV ~ n^2
2. Generalized Metcalfe's Law: NV ~ n^1.5
3. Odlyzko Law (also called Zipf's Law): NV ~ n • log n

They calculated Pearson correlations for all three of these laws over the period between 2010 and 2018, and based on this analysis chose law #2. They then used it to define Price-to-Metcalfe Ratio by dividing actual Network Value by the one predicted by the law:

$$PMR_{Clearblocks} = ln\frac{Network\ Value}{30\ day\ MA\left(n^{1.5}\right)}$$

where *n* is Daily Active Addresses (DAA), and *30 day MA* is 30 day moving average.

There is an issue here, however: **it is very hard to objectively choose between these three laws,**and the Clearblocks team admits it in the article themselves:

All formulas show near perfect correlation with BTC's USD price, particularly on a natural log scale. In any other field, such a correlation would be considered witchcraft… The differences in correlations are so small they can effectively be considered equal

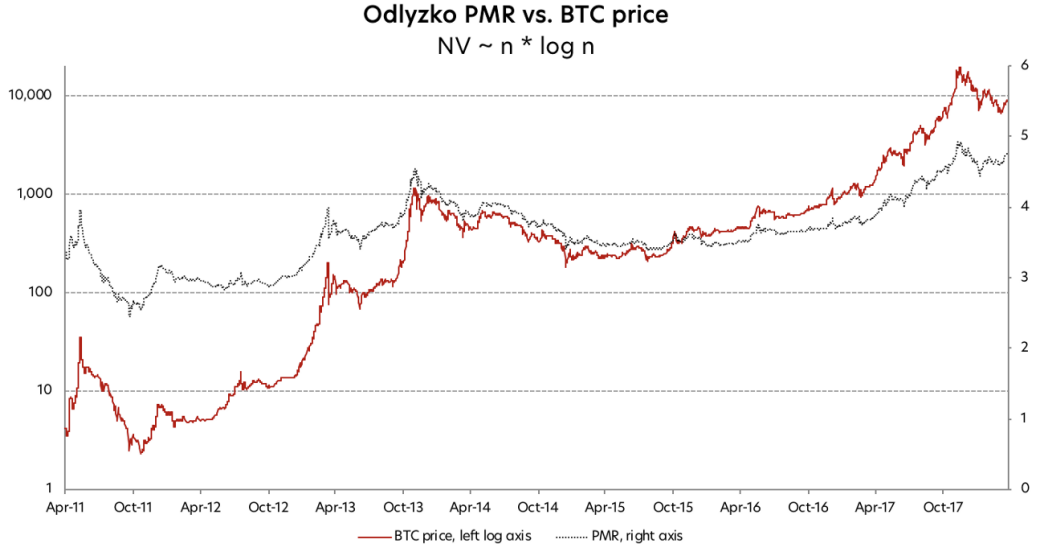
At the same time the value of the ratio (and hence the results of PMR analysis) depends greatly on which law you choose for denominator. **Different values in denominator give you contradicting results when it comes to predicting December 2017 bubble and to describing current BTC price.**

Different laws — contradicting results

If you define the PMR denominator using Odlyzko Law (NV ~ n log n), you will get the following formula:

$$PMR_{Odlyzko} = ln \frac{Network\ Value}{30\ day\ MA\ (n * ln(n))}$$

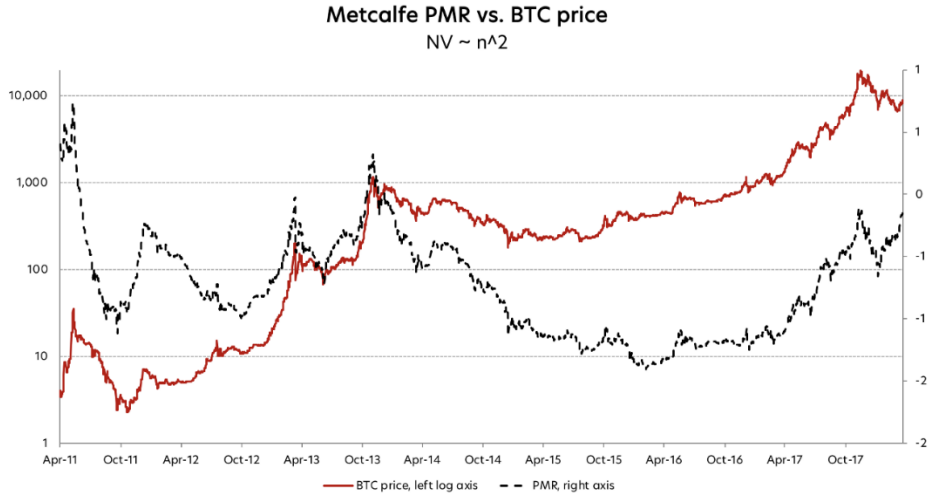
where *n* is DAA. If you then plot the resulting Odlyzko PMR against Bitcoin price, you will get the graph below. Based on this graph, PMR is at its all-time high level of around 5, and we are still in the middle of the worst bubble in Bitcoin history. Corrections in Q1 2018 didn't help much — even at around $6k in February 2018 Bitcoin was still presumably significantly overvalued according to this analysis.



Now let's use the original Metcalfe's Law as the PMR denominator giving the formula below:

$$PMR_{Metcalfe} = ln \frac{Network\ Value}{30\ day\ MA\ (n^2)}$$

If you now plot this PMR against BTC price, you will get very different chart. By closely examining this chart you can see that current PMR value is around 0, which is nowhere close to the bubbles of 2011 and 2013. And at the lowest point of correction in Q1 2018 PMR was around -0.5. Last time it was on the same level in October 2014 and August 2017. As we now know, in both of these cases it was a good time to buy BTC.



As we said above, **PMR analysis gives contradicting results for December 2017 and for May 2018, depending on which law you choose for the PMR denominator.**But it is also impossible to choose between the laws based on their all-time correlations between the actual and predicted Network Values.

Here we asked ourselves 2 questions:

1. Can we come up with a better heuristic for choosing the best law?
2. If not, is there a way to somehow use both of these laws instead of choosing one?

Unfortunately, the answer to the first question is *"no, we can't"*. Those of you interested in the algebra and statistics behind this conclusion can find detailed explanation here.

Luckily, the answer to the second one is yes. **We used both Metcalfe's Law and Odlyzko Law to define extremely robust upper and lower bounds for Network Value, and derived a ratio that is indicative of Bitcoin overvaluation.**

Two laws are better than one

According to the logic behind the Metcalfe's Law, n^2 is a number of *potential_connections between users of the network, and in reality there are limitationstonumber of _useful* connections one user can have. So Metcalfe's Law (Network Value ~ n^2) probably overestimates network value, which is why it's logical to use it as an **upper bound**for valuation of Bitcoin network. At the same time we can use Odlyzko Law (Network Value ~ n • log n) as a**lower bound:**

$$ln(NV_{actual}) < Upper\ Bound = a_1 + b_1 * 30MA[ln(n^2)]$$

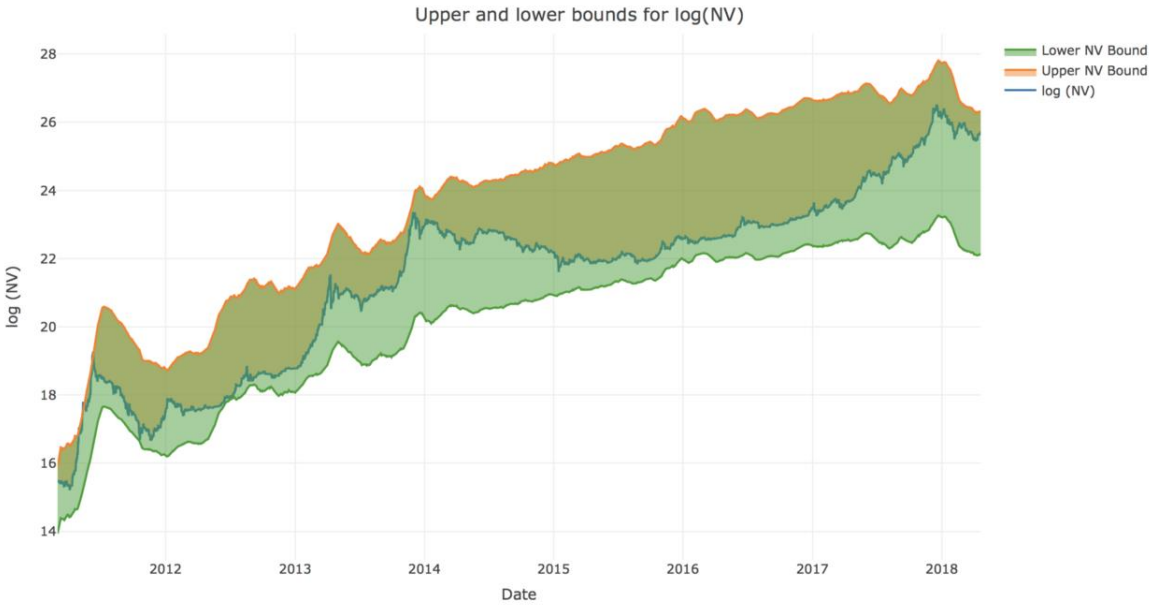
Upper bound based on Metcalfe's

$$ln(NV_{actual}) > Lower\ Bound = a_2 + b_2 * 30MA[ln(n * ln(n))]$$

Law Lower bound based on Odlyzko Law

Constants *a* and *b* for each bound were chosen empirically to have the narrowest corridor possible that still covers all the movements of Network Value. To make sure we didn't overfit and didn't use future information, we used only first 2 years of data to select *a's* and *b's.* After fixing the constants based on this "training" set, we checked that the relationship holds well for the rest of the data ("validation set").

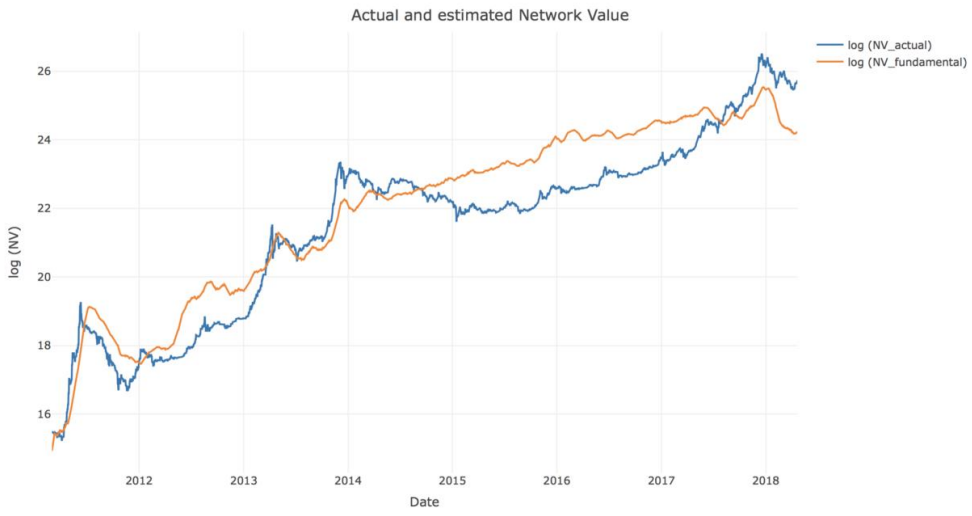
If we now plot the Network Value and respective bounds derived from Metcalfe and Odlyzko Laws, we can see that NV robustly stays within these bounds all time except a few days back in 2011 (and even then it barely crosses the border).



Now that we have robust upper and lower bounds, we can, with confidence, use the halfsum of upper and lower bounds as a bottom-up valuation of the Bitcoin network as a function of DAA:

$$ln(NV_{fundamental}) = \frac{Upper\ Bound + Lower\ Bound}{2} = \frac{(a_1 + a_2) + b_1 * 30MA[ln(n^2)] + b_2 * 30MA[ln(n * ln(n))]}{2}$$

Below is a chart of *actual* and *Metcalfe-estimated fundamental* Network Values. Visually, this relationship is staggering.



Moreover, on the previous chart with the bounds we can clearly see that every time Network Value has approached its upper bound, there was a correction that

followed. And conversely, every instance when Bitcoin Network Value was near the lower border, it was a good time to invest.

Using our newly defined Metcalfe network valuation, we can formalize this logic into a new, refined, indicator that we called **Network Value to Metcalfe ratio (NVM)**:

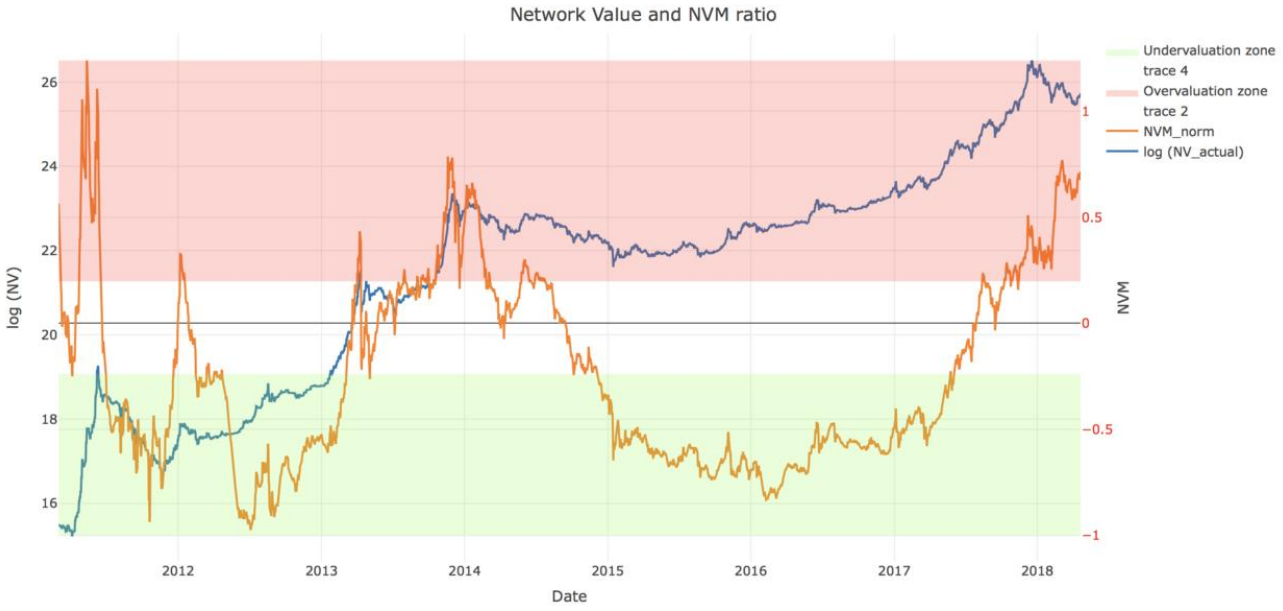
$$NVM = ln(NV_{actual}) - ln(NV_{Metcalfe}) = ln\left(\frac{NV_{actual}}{NV_{Metcalfe}}\right)$$

One last transformation: let's normalize NVM so that it always stays between -1 and 1 no matter how wide the corridor between the bounds is:

$$NVM_{normalized} = \frac{NVM}{\frac{(Upper\ Bound - Lower\ Bound)}{2}}$$

NVM describes Network Value position relative to the upper and lower bounds, and thus quantifies any overvaluation or undervaluation. Normalized NVM of -1 means that Network Value is near the lower bound, and a value of 1 signifies that it has reached the upper bound.

Below is the chart of normalized NVM and Bitcoin Network Value. As can be seen on the chart, high NVM has successfully predicted corrections in 2011, 2012, 2013, 2014, and late 2017.



So, are we in the bubble?

BTC Network Value is close to the upper bound, and NVM is around 0.75. Current NVM value is even higher than it was in December 2017, and is at the same level it was at the height of the 2014 bubble.

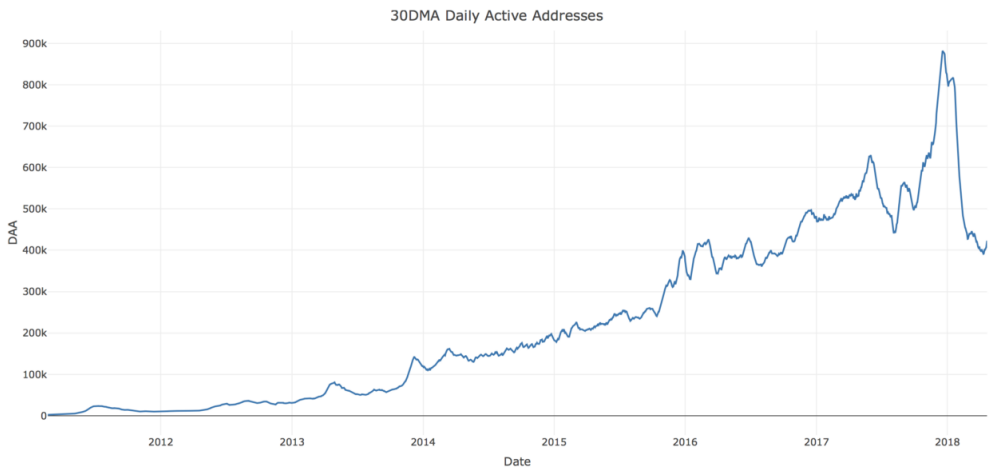
High NVM suggests that Bitcoin is overvalued at the moment, compared to the Metcalfe NV estimation derived from DAA data. According to our model, Metcalfe network valuation is around $33bn, while the actual NV as of May 6th is $162bn. If we take this result at face value, this means that BTC is ~ 5x overvalued, compared to a Metcalfe price of about $2,000. But let's dive one level deeper, and try to analyze *why* NVM is at this level right now.

Let's look for analogies in traditional finance. High PE ratio is usually considered to be a signal of company overvaluation. But it can also be explained by unusually low recent earnings caused by business seasonality or other factors. If low earnings are expected to increase shortly, high PE is not necessarily bad.

Let's try to apply similar logic to NVM. Based on the historic NVM performance, from here it can go one of two ways:

1. **NVM will decrease because of lower numerator.** BTC price correction will bring Network Value closer to(or even below) the Metcalfe-derived valuation. This will be similar to the pattern we saw in early 2014.
2. **NVM will decrease because of higher denominator**. Daily Active Addresses will grow, thus increasing the Metcalfe valuation and bringing it closer to actual Network Value. A similar pattern can be seen in early 201

Let's have a look at number of Daily Active Addresses. The chart below shows there was a significant drop in DAA in Q1 2018.



Let's again compare the current May 2018 situation with December 2017:

- As we noticed before, NVM was high in both cases
- But in December 2017 DAA was unusually high — well above the long-term trend. Given an expected drop in DAA back to the trendline, price correction was the only way to bring Network Value close to fundamental Metcalfe valuation.
- On the contrary, in May 2018 the Daily Active Addresses figure is unusually low
- If DAA to bounces back up to the trendline, it will increase fundamental Bitcoin valuation

Overall, while the current price level is healthier than in December 2017, it is still not 100% supported by fundamentals. Investors should closely monitor the DAA dynamic relative to market Network Value. **If Bitcoin price continues growing further without advancing growth of DAA, there might be another bubble (and another correction) on the horizon.**

Acknowledgements

There were a few people who have contributed to this research, and inspired us to do it in the first place:

- Thomas Lee for the original inspiration to look into Metcalfe's Law applications to cryptoassets
- Haseeb Quereshi,Ivan Bogatyy, and Chris Burniske for feedback on the article
- Professor Susan Athey from Stanford and Professor Christian Catalinifrom MIT Cryptoeconomics Lab for being great mental sparring partners on everything crypto
- Special thanks goes to all the Cryptolab Capital team, and especially to our analyst Roman Skoromnyi who did a lot of data heavy-lifting during this research

Disclaimer: *none of the statements in the article should be considered investment advice. Due to the various risks and uncertainties, actual performance of the assets may differ materially from that reflected or contemplated in forward-looking statements.*

Bitcoin Data Science (Pt. 2): The Geology of Lost Coins

By Dhruv Bansal

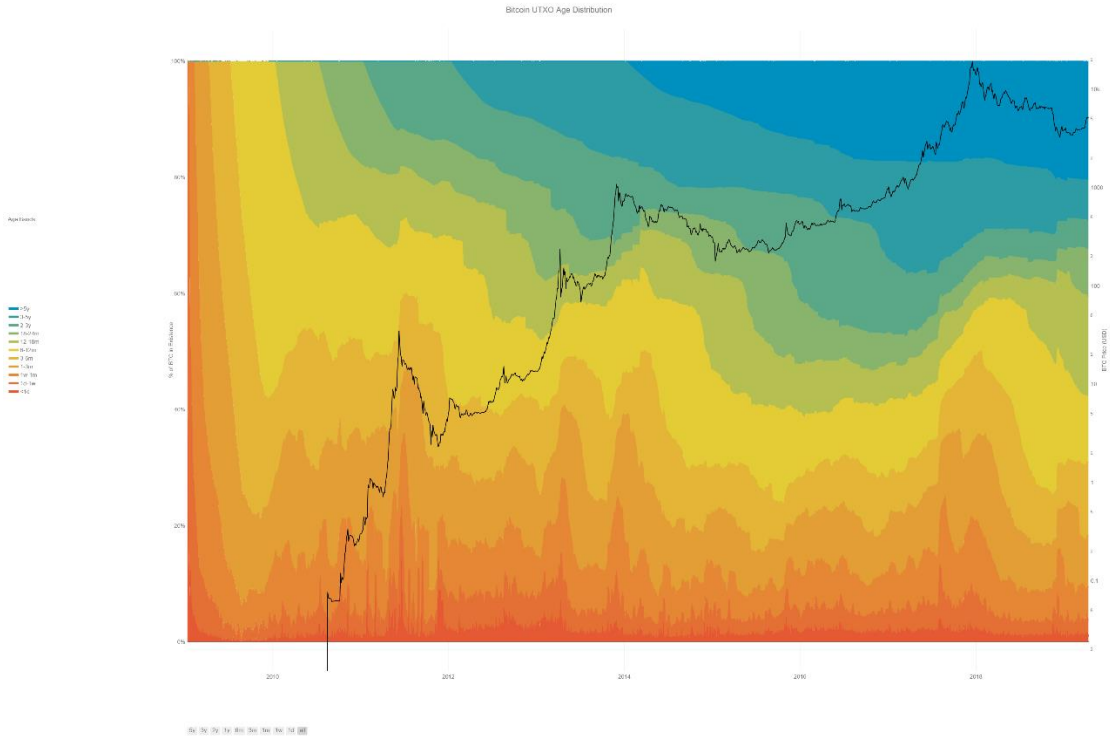
Posted May 29, 2018

This is part 2 of a series

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

There are many stories of people losing BTC in large amounts - especially in the early days - when BTC wasn't worth much, and was easily forgotten on an old hard-drive, USB memory stick, even a scrap of paper.

Is it possible to quantify how much BTC is really lost? Blockchains track their internal data forever, and as we showed in Part 1 of this series, one can visualize Bitcoin's UTXO age distribution to illuminate historical trends in ownership:



The colored bands show the relative fraction of Bitcoin in existence that was last transacted within the time window indicated in the legend. The bottom, warmer colors

(reds, oranges) represent Bitcoin transacted very recently, while the top, cooler colors (greens, blues) represent Bitcoin that hasn't transacted in a long time. Bitcoin's money supply grew from 50 BTC to ~ 17M BTC over this time period, so the chart has been normalized by the BTC in existence at each date (left y-axis). The black line shows the USD/BTC price (logarithmically, right y-axis). Chart lovingly made by Nelson Morrow based on prior work by @jratcliff [Direct Link]

After seeing the UTXO age distribution above, many readers of Part 1 commented, "a large fraction of the oldest coins are probably lost." This is a reasonable intuition. There were many reasons for BTC holders to transact in 2017 & 2018: a price rally and a pullback, the rise of ICOs, the BTC/BCH fork, new segregated witness addresses, etc. Coins which remain unspent for >5 years have a high likelihood to be lost forever. Can we make this intuition more precise?

Despite the richness of blockchain data, it's extremely difficult to measure how much cryptocurrency is truly lost, as lost coins leave no trace in the blockchain. Lost BTC sits idly in the UTXOs of its last transaction, aging quietly as time passes. The problem is that *so much* BTC which is **not lost** looks exactly the same on the blockchain.

Still, the UTXO age distribution does provide insight into how to think about lost BTC. The cooler-colored, older age bands can be thought of as **low-pass filters** which only allow the oldest coins to pass into them. As a result, they experience slower, less volatile changes than the hotter colored, younger age bands.

UTXO age bands are like geological strata: evidence of coins held some time ago, buried beneath layers of more recent transactions. Distinguishing lost coins from those dearly held requires unearthing subtle data from the oldest layers, from the deepest records of the blockchain.

The study of lost bitcoin is geology masquerading as data science.

We believe bitcoin loss occurred over two distinct "cryptogeologic" eras:

1. **Systemic loss**: a large cohort of BTC which was mined together and lost together in the earliest days of Bitcoin by Satoshi and the other first miners. (Bitcoin's *carboniferous period.*)
2. **Incremental loss**: BTC lost by individual users gradually over different periods of time.

We'll show that the era of systemic loss has ended, and demonstrate that we are now in the era of incremental loss. Finally, we'll estimate bounds on how much bitcoin is lost. Let's turn to the data.

Early Systemic Loss

What was happening in Bitcoin in its earliest days in 2009? Answer: Almost nothing.

Satoshi published the original whitepaper in October, 2008 after working on the concept and the code for the prior couple of years. Satoshi mined the genesis block on January 3rd, 2009, and promptly released the first version of the `bitcoind` software (v. 0.1) on January 9th.

Very few people took Satoshi or Bitcoin seriously in those early days. Gwern Branwen's excellent article Bitcoin-is-Worse-is-Better describes some of the initial negative reaction from "professional" cryptographers.

In the first days of Bitcoin, poor Satoshi was mostly mining alone, occasionally joined by other crazy people such as Hal Finney. The result was extremely low hashpower, as the chart below shows. Satoshi and the first miners were unable to exceed the minimum hashrate required to trigger an upward difficulty adjustment till the first days of 2010. The average time between blocks didn't hit the target of 10 minutes until a month later, in February, 2010.

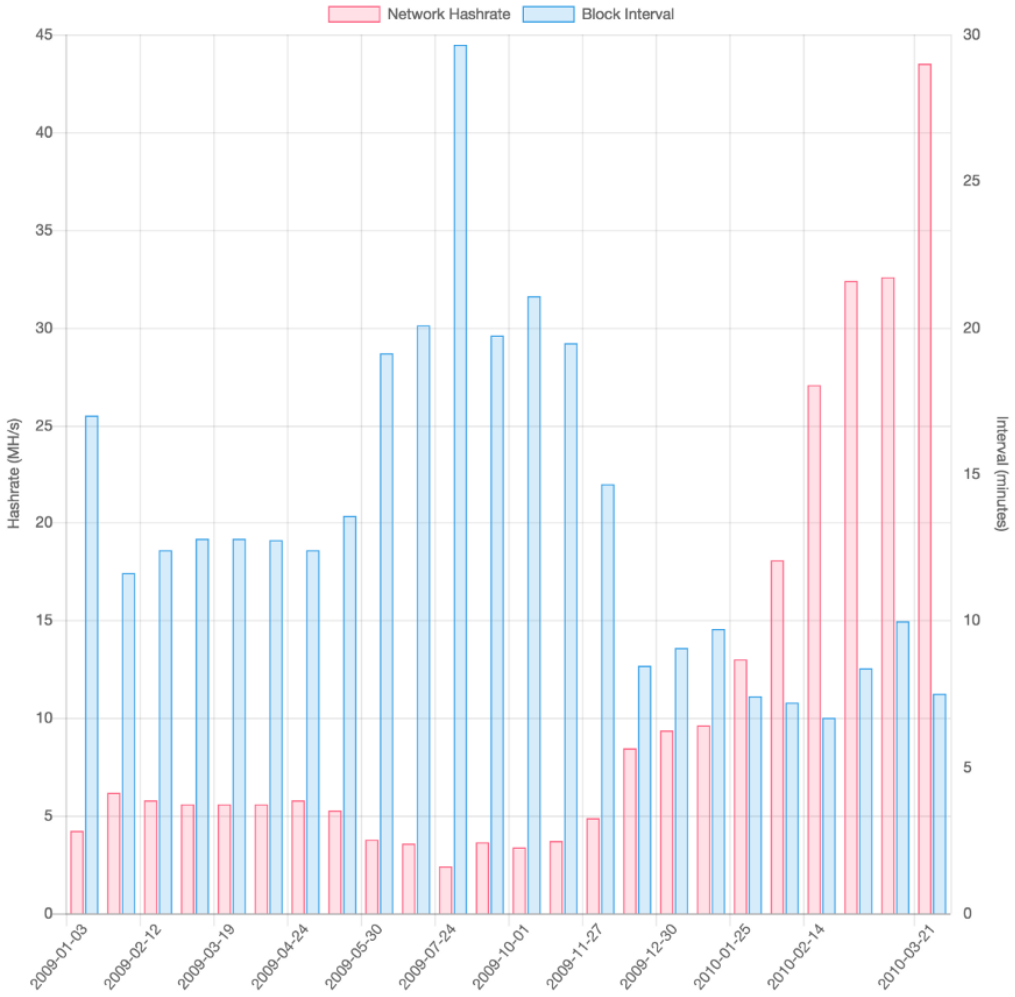
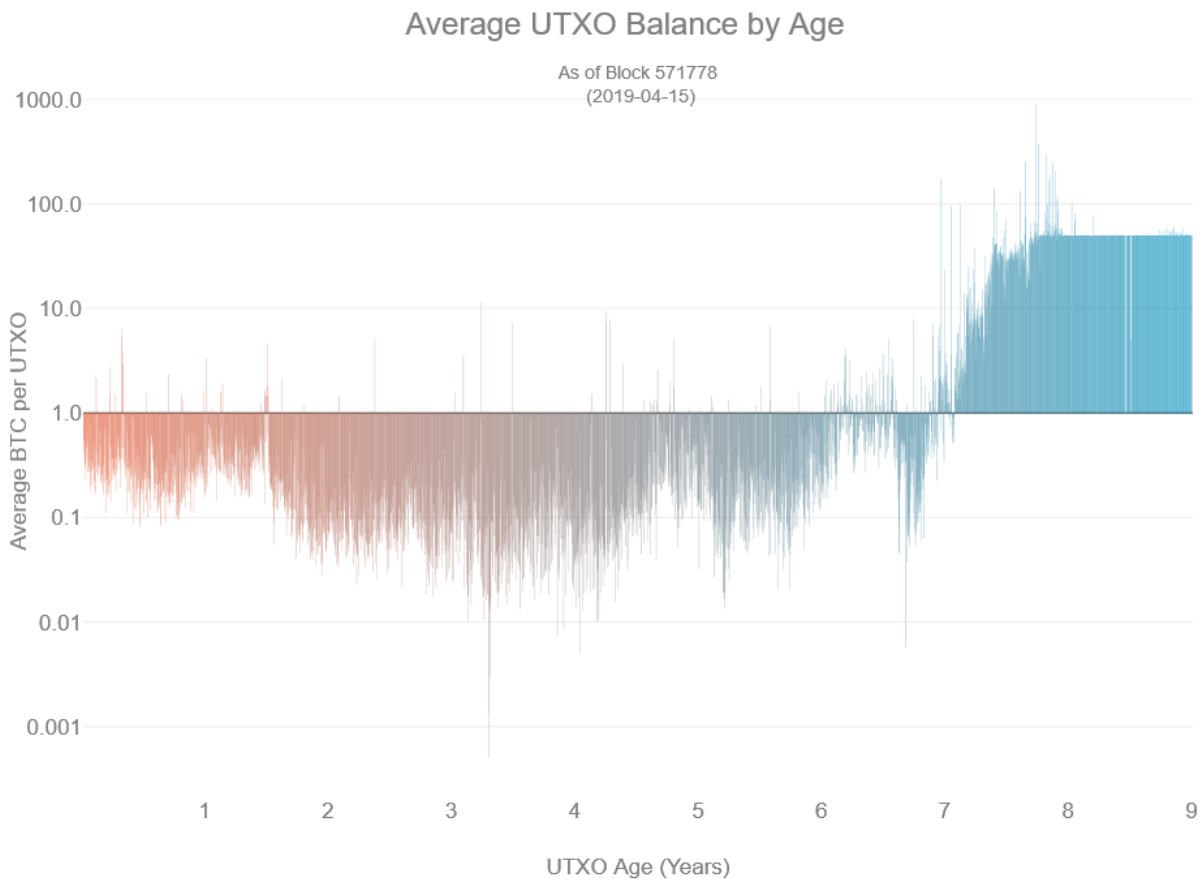


Chart depicting hashrate and the average time between blocks over 2009 and the first quarter of 2010. It's likely that only Satoshi and a few other small groups were mining Bitcoin during the entirety of 2009. Chart originally appeared in an article by Evan Klitzke.

Despite the apparent stagnation above, there were still many, many blocks mined in 2009, and over 5M BTC was produced in this period by Satoshi and the first miners through 2011. That's more than 23% of the all BTC that will ever exist. Where did it go?



This chart groups the current UTXO set by age and then plots the average BTC balance per UTXO at each age group. The cohort of UTXOs older than 7 years (approx. 1.9M BTC), all mined before 2011, is clearly visible as a "shelf" on the right side of the plot, with the average balance sitting at 50 BTC, the coinbase reward in that era.. [Direct Link]

The above plot shows that the oldest 1.9M BTC of UTXOs in existence are a distinct population. They are the cohort of coins mined by Satoshi and the first miners during those early years of Bitcoin. They form a "shelf" at 50 BTC in the chart because the block reward at that time was 50 BTC (and fees were negligible): they are coinbase outputs that were never spent. (Note that the rapid falloff of this shelf between 6.5–7 years ago occurred in 2011. We'll come back to this date below.)

Bitcoin's Carboniferous Period

The carboniferous period occurred about 300M years ago and corresponds to the age in which Earth was covered in trees, but nothing existed which could eat trees. As a result, layers of dead trees accumulated, unable to decay.

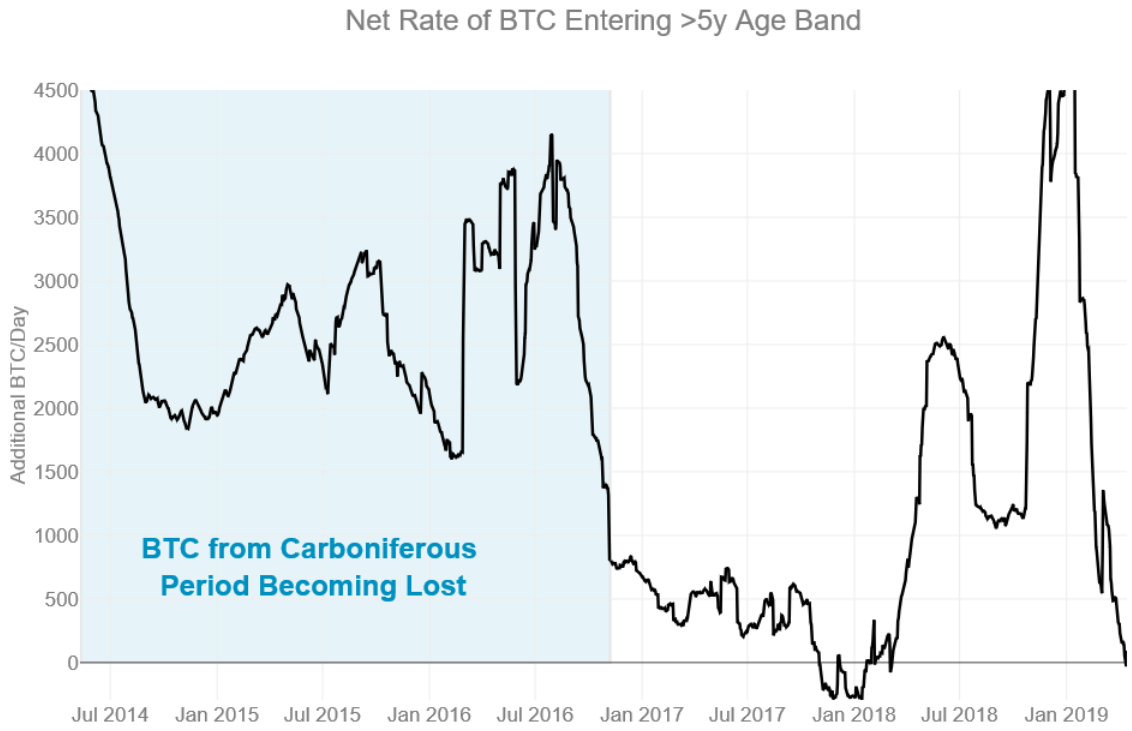
A late 19th century etching of what a forest would look like during the carboniferous period (300–360 Mya). [From Wikipedia]

2009–2011 was Bitcoin's carboniferous period: huge amounts of coins were mined but unused, accumulating in the blockchain, eventually becoming lost, unuseable, and buried.

It's ironic that, eons later, the trees which accumulated in the carboniferous period became coal, the chief energy source used for most Bitcoin mining today :)

Transition to Incremental Loss

Something dramatic happened to Bitcoin in 2011. The cohort of oldest UTXOs noted above diminished rapidly. 5 years later, in 2016, the rate at which BTC was entering the >5 years age band correspondingly diminished. This manifests as an inflection point or "kink" in the >5 years age band of the UTXO age distribution in 2016. One can see the echo of dramatic changes in Bitcoin, 5 years prior, in 2011. This chart shows the net rate-of-change of the amount of BTC >5 years old over time (trailing 90-day average). Between 2014–2016 (highlighted in blue) we see the effect of Bitcoin's "carboniferous period", which occurred 5 years earlier, from 2009–2011, when many coins were being lost. This period ends abruptly in 2016, corresponding to a dramatic change in Bitcoin 5 years prior in 2011. The time-axis of the chart starts in 2014 because this is the first year in which BTC could enter the >5 years age band (the genesis block having been mined in 2009). [Direct Link]



The above plot summarizes this transition. Between 2014–2016 (highlighted in blue) the rate at which BTC was entering the >5 years age band was extremely high. This corresponds to coins which last transacted during Bitcoin's carboniferous period of 2009–2011, when Satoshi and the first miners mined, then subsequently lost, many coins.

A dramatic decrease in the rate of BTC entering the >5 years age band occurs in 2016, corresponding to the end of Bitcoin's carboniferous period in 2011. The real, geological carboniferous period ended when bacteria evolved which could digest wood, preventing dead trees from piling up for eternity. What caused Bitcoin's carboniferous era to end?

Curiosity to Commodity

In June, 2011, Bitcoin experienced its first major rally. Over a couple of short months, Bitcoin's price went from less than $1 to a peak of $33. This created significant wealth for many early miners—at least those who hadn't lost their keys.

Before the sudden price increase to $33, Bitcoin miners may have been lax with the security or safe-keeping of the BTC they were earning. The tragic tales of lost hard drives containing untold digital wealth largely occurred around this time.

Afterwards, anyone mining BTC would have taken note: 1) BTC was valuable, and 2) it could quickly grow in value by orders of magnitude again.

These lessons fostered a radically different attitude towards mining and safeguarding bitcoin. At <$1/BTC, daily mining revenues would be only a few thousand dollars per day, amounting to perhaps ~ $1M per year—a market barely large enough to support a single small business. At $33/BTC, however, daily mining revenues reached almost $250k, creating a yearly revenue stream of >$80M. Bitcoin went from being a curiosity to a commodity, and Bitcoin mining transitioned from a hobby to an industry.

Echoes of the Great HODL?

A remarkable feature of the above chart is the upswing in the rate of BTC entering the >5 years age band in the last couple of months. This upswing represents BTC which last transacted in the middle of 2013, 5 years ago.

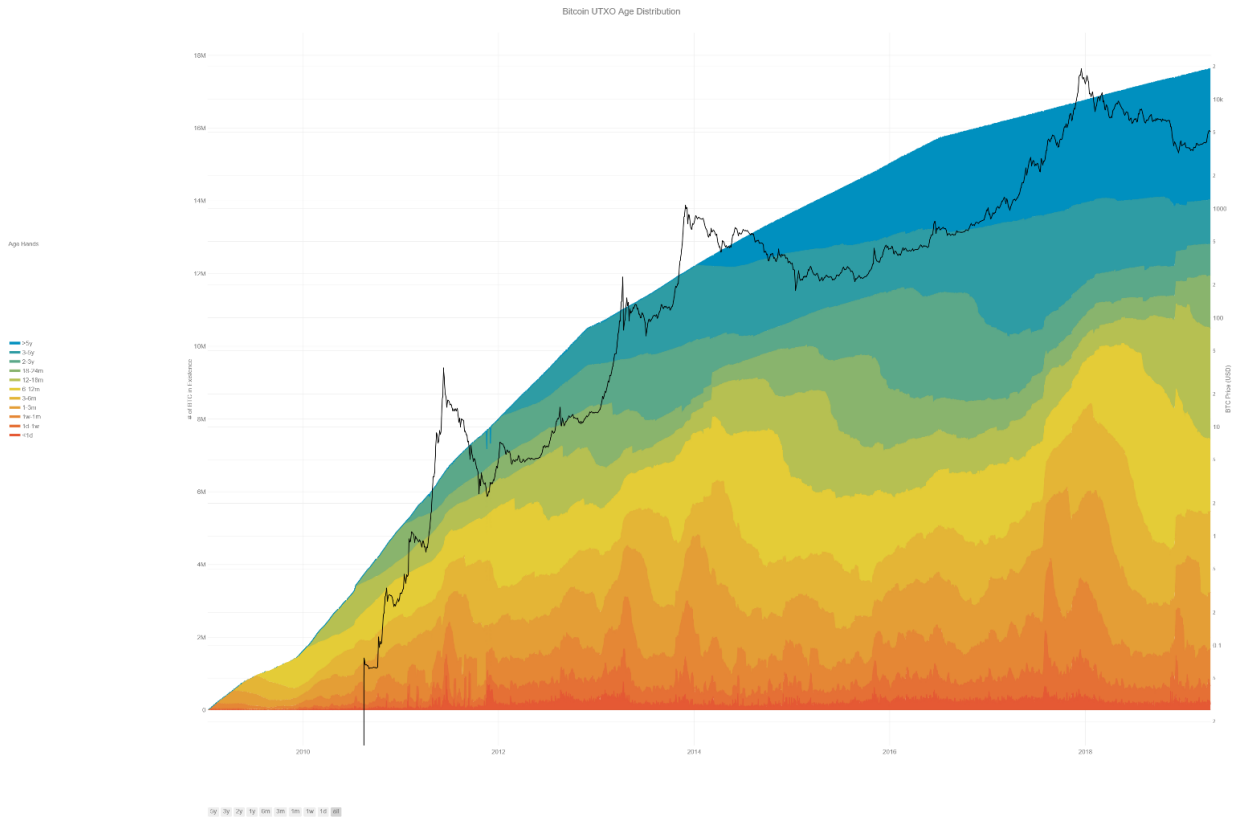
In Part 1 of this series we identified the HODL wave pattern of changes in the UTXO age distribution. This recent upswing in the rate of BTC entering the >5 years age band is the arrival of the leading edge of the Great HODL wave started in 2013/2014, when Bitcoin rallied to $1k/BTC.

We know that the Great HODL wave was disrupted by the 2017 rally to $19k/BTC, so it's unlikely that all the 1.5M BTC in UTXOs which entered the 3–5 age band in 2016 would have survived to enter the >5y age band in 2018; many would have been transacted with during the rally, the fork, SegWit, &c.

So, in distinction to Bitcoin's carboniferous period, we predict this recent upswing to be much smaller and abate more quickly. We estimate <500k BTC should enter the >5 years age band over the next 18 months.

So how much Bitcoin is lost?

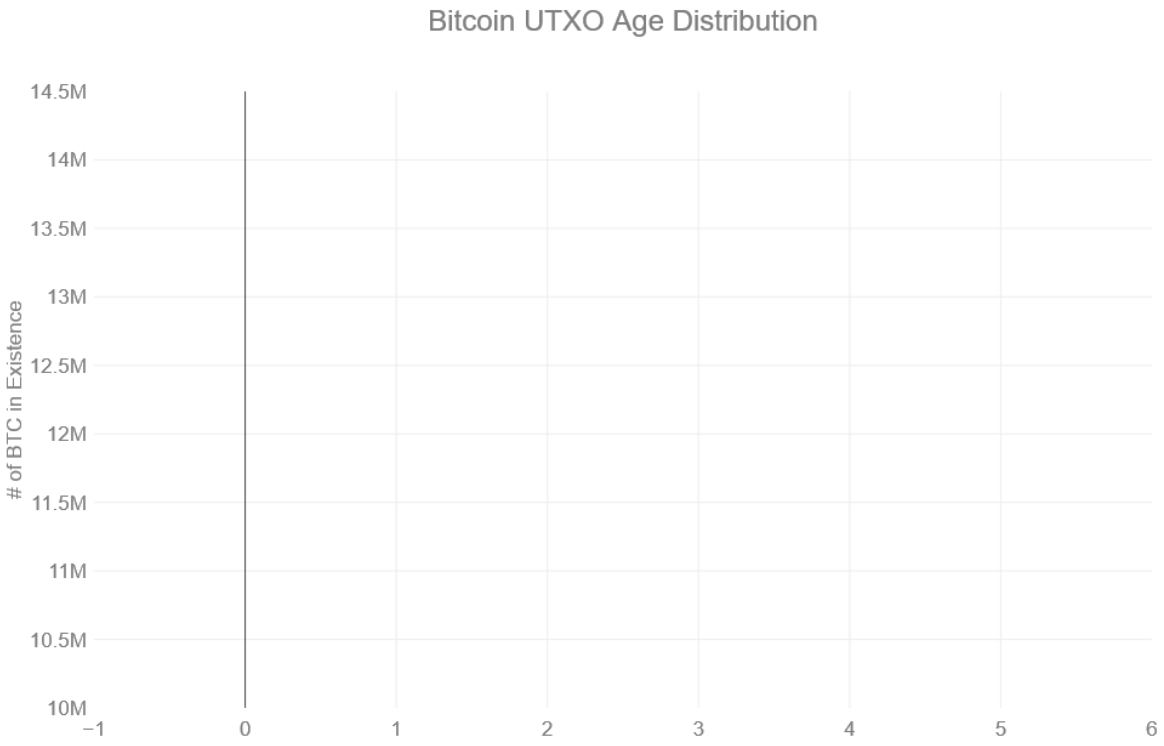
It's impossible to know. But, based on the analysis above, we can make an informed guess at some bounds. This will be easier with an absolute version of the UTXO age distribution:



An absolute version of the UTXO age distribution chart which has not been normalized by the available BTC supply. The two prior halvings are clearly visible as kinks in the overall rate of production (as discussed in the text, hashpower was unstable in 2009, causing a departure from linearity). Due to the vast difference in the BTC supply between 2009 and 2018, the earlier HODL waves are harder to see though the Great HODL of 2013/2014 is still quite clear. [Direct Link]

A conservative lower bound for the amount of lost BTC is the cohort of coins mined in 2009–2011 by Satoshi and the first miners that remain unspent to this day: 1.9M BTC. This is about 2/3 of the BTC in the current >5 years age band. There are certainly many more Bitcoins which were lost in the intervening years since 2011, but can this amount be quantified?

During the 2017 rally, the 3–5 years age band shrinks significantly, **but the >5 years age band barely changes**. This strongly suggests that many coins in the 3–5 years age band are still controlled by someone, but that most coins in the >5 years age band are lost. At some age between 3–5 years, we should expect the former pattern to crossover to the latter pattern. This also suggests a less conservative lower bound of 3M lost BTC—the size of the >5 years age band. A version of the UTXO age distribution "zoomed into" the 3–5 years age band, split into 3-month intervals, covering the rally of 2017. [Direct Link]



This "zoomed-in" version of the UTXO age distribution shows finer-grained detail on the 3–5 years age band, splitting it into several 3-month age bands. A HODL wave is evident as a cohort of coins makes its way through the finer-grained age bands in 3 month periods.

The earlier age bands (36—39 months) are significantly slimmer today than they were in a year ago, indicating that most of those coins are controlled by someone who was able to transact with them during the rally of 2017. The older age bands (57—60 months) show almost no change during the rally of 2017, just like the >5 years age band.

We estimate the boundary between these behaviors occurs between 45 to 51 months. If we make the rough assumption that most coins older than this are lost, it suggests that an upper bound of 3.8M BTC are inaccessible. Our final estimate from looking at the UTXO age distribution is that between 3–3.8M BTC are lost.

A More Precise Estimate

It's difficult to be precise when using just UTXO ages to estimate how much BTC is lost. A better approach would label and track individual UTXOs with external

metadata, which would distinguish the context of different transactions: miners, exchanges, etc. This approach takes after archaeology more than geology.

Happily, our friends at Chainalysis have already made such an analysis. In an excellent Forbes article published last year, they use such an approach and make their own estimate: 2.78–3.79M BTC lost. It is encouraging that our simple approach, based on looking at just UTXO ages, accords with Chainalysis' more sophisticated approach.

Many thanks to Philip Gradwell and Kim Grauer from the Chainalysis Team for helpful discussions. Check out the Chainalysis Blog for more fascinating work from their team.

This post is the second in a series using data science to tell stories about Bitcoin; unearthing the deep geological history of the blockchain, while searching for lost treasure.

You might also enjoy:

- Part 1: In which we describe market cycles with HODL waves.
- Part 3: In which we analyze UTXO dust in the chain.

Unchained Capital has been performing data science on blockchains for years. Discovering the large amount of Bitcoin UTXOs older than 12 months convinced us to start a lending business to help cryptocurrency owners get value from their digital assets today while continuing to hold them into the future.

If you are holding BTC (and soon ETH) and you'd like to borrow against your holdings, please sign up for an account on our website and apply for a loan.

Remember *: Friends don't let friends sell Bitcoin.*

Bitcoin: Past and Future

By Murad Mahmudov and Adam Tache

Posted May 30, 2018

Foreword

This is a follow-up to The Many Faces of Bitcoin, which discussed four schools of thought of Bitcoin. This article will analyze these perspectives by discussing trade-offs, philosophical divides within the community, and expected behaviors of the proposed systems.

Index

Bitcoin As Money

Bitcoin presents us with an opportunity to reinvent gold, or even rethink money for the digital future. A number of economists have suggested that it may be more appropriate to evaluate items based on their degree of *moneyness.* According to this thinking, it isn't that something either is or is not money; on the contrary, many items can play a monetary role and some items can play this role more effectively than others. In a number of ways, bitcoins have a high degree of moneyness. They are more portable, durable, divisible, and scarce than both gold and government fiat currency.

As of today, bitcoins can best be described as digital commodities with monetary properties. According to the Bitcoin Maximalist interpretation of monetary history, it is likely that a new, scarce form of money would evolve roughly along the following lines:

1. Collectible
    2.

- Store of Value
3.
- Medium of Exchange
4.
- Unit of Account.

Proponents of bitcoins as digital cash believe that utility should initially take precedence over store of value, and prioritize attaining the medium of exchange role before store of value by making payments as cheap as possible.

Those who believe bitcoin will become the future global monetary standard ascribe current volatility to the fact that bitcoin is undergoing the process of monetization, and that a global cognitive shift is slowly occurring. In their view, despite great volatility, the long-term parabolic ascent of the price is a testament to more and more people believing in a future world where Bitcoin is widely used.

Crypto-Austrianswho consider themselvesRothbardians, such as authorSaifedean Ammous, believe that bitcoin's disinflationary nature and cap on supply makes it the most sound money ever invented. They believe that bitcoin, with its fixed monetary supply, is the only fair form of money, as well as one which allows for the most efficient capital allocation by individuals and most efficient price signalling by the market as a whole.

Many individuals in this group are against the idea of fractional-reserve banking and consider it to be fraudulent. They believe that a fractional-reserve banking system is unlikely to emerge atop bitcoin, as bitcoins lack the physical centralization of gold, which forced settlements and clearance to necessarily pass through centralized choke-points, allowing governments to have complete control over the money supply, transmission, and the monetary regime at large. The governments had so much control that they were able to get rid of the gold-standard (which was organically chosen by the market over centuries) and introduce their own fiat standards, not backed by any commodity.

These individuals believe that fractional-reserve systems are simply unsustainable in the long run without lenders of last resort, which do not inherently exist in Bitcoin, and that people would be unwilling to accept bitcoin-substitutes in the market.

Those in the "Free Banking" wing of the Austrian school, such as George Selgin and Lawrence White, believe that bitcoin's strictly fixed-supply and lack of lenders of last resort do not technically prevent a competitive system of fractional-reserve banks and entities arising atop bitcoin, or in an economy where bitcoin is the defacto monetary standard.

It is clear that there is a chance that bitcoin can, at the very least, emerge as a mildly volatile digital commodity, a store of value akin to digital gold. However, doubts

remain whether it will transcend the raw store of value role and achieve low enough volatility to become a global medium of exchange and a unit of account.

Some believe that, due to its strictly inelastic supply, bitcoin is unlikely to be stable in its purchasing power anytime soon, if ever, and that people prefer for their day-to-day currency to be stable in purchasing power. These people have expressed excitement about the emergence of cryptocurrencies with more flexible and self-regulating monetary policies built in. For example, stablecoins aim to peg their market value against another form of value, such as the USD or a basket of goods, using an algorithmic central bank.

Othersbelievethat, despite bitcoin's strictly inelastic supply, bitcoin is a perfect solution toJohn Nash'sIdeal Moneyproposal that he worked on for over fifty years. Nash, a Nobel Laureate in Economics,[proposed(http://web.math.princeton.edu/jfnj/texts_and_graphics/Main.Content/IDEAL_MONEY…/Campus_for_Finance_of_2010/?source=post_page———————)that central banks could inflation-target their currencies against an apolitical index to achieve international relational stability of all state currencies. In response to increasing demand for bitcoin, some believe banks will value target their currencies against bitcoin as a basis for the standardization of the value of money.

Deflationary Death Spiral

Mainstream, Keynesian, and Monetarist economists have expressed concerns with Bitcoin's fixed-supply. They fear the possibility of harsh deflationary pressures if bitcoin becomes the predominant currency through the process known as hyperbitcoinization.

Their fear is that the inability to expand the money supply would result in bitcoin's purchasing power growing by 2–3% per annum, roughly in line with the growth rates of global economic output. Some have expressed concerns that deflationary economics might reduce aggregate demand in the present and the near-term, result in excessive savings and hoarding of money, and produce less consumption, investment and entrepreneurial risk-taking by individuals.

Austrian economists believe that the fears associated with a deflationary form of money are overblown and that the 'deflationary spiral' is a myth. Austrian's counter the Keynesian and Monetarists concerns that the delay in spending doesn't last in perpetuity by reminding them that this spending is merely delayed into the future. People will now have a lower time-preference and that instead of buying "useless" things with their "hot potato" decaying money, they will turn their attention to long-term productivity.

They also believe that business profit margins will not be hurt because not only would product prices, but also business costs, deflate at the same rate, leaving the profit margins unchanged. Austrians believe that deflation is absolutely normal, and absent central control on the money supply, both capitalism and technology are naturally deflationary phenomenons. This can be seen in the less-regulated electronics industry, where increased storage/memory/compute capacities are becoming cheaper every year.

According to Austrians, it is the *central bank inflationary fiat printing* that exacerbates recessions and business cycles, as the perpetually-decaying money embeds the citizenry constant anxiety and stress, resulting in not well though-out investments and expenditures, collectively referred to as 'malinvestment'. These malinvestments are typically inefficient allocations of capital, which are unlikely to result in personal gains, societal gains, productivity, or capital stock.

Roles of Full Nodes & Miners in Bitcoin & Bitcoin Cash

The Scaling Debate

The debate over how to scale Bitcoin is very polarizing, and is about scaling throughput, also known as transactions per second (TPS). The main contention is how much it should cost to run a full node, and what the role of full nodes and miners should be in the the system.

In July 2010, Satoshi Nakamoto, the creator of Bitcoin, supposedly added a 1 MB maximum block size limit as an anti-DoS (Denial of Service) prevention mechanism. This 1 MB block size limit stood in place, and until transaction volume increased heavily in 2017, the blocks were never close to full capacity. When this limit was introduced, 1 MB was hundreds of times the size of an average block.

In August 2017, an update called Segregated Witness (SegWit for short, see dedicated section below) was activated, which increased the amount of data that could be stored in a block to above 1 MB. Taking many by surprise, at around the same time, on August 1, a fork of Bitcoin (BTC) named Bitcoin Cash (BCH) spawned from users dissatisfied with the BTC developers' scaling roadmap and emphasis on bitcoins as digital gold. The developers of this fork quickly implemented 32 MB blocks and are planning to increase the limit much further, which would allow for more on-chain transactions per block and cheaper fees but make it more expensive to run a full node.

Factors that influence the cost of running a full node include required bandwidth, the size of the UTXO set (see this primer on Bitcoin transactions if you're not familiar with the UTXO concept), and required CPU, RAM, and disk space, which are all impacted by the block size.

Those who favor small blocks view them as essential to maintain decentralization of the system by allowing any user to afford validation using a full node, and to develop a fee market in order to guarantee miner compensation as the block reward decreases.

The proponents of Bitcoin Cash, "big blockers," view a block size limit as an artificial limit maintained through a centralized planning mechanism in the form of consensus rules. Many prefer miners selecting the size of blocks they are willing to create based on market conditions. There are other blockchain projects where this is the case, such as Ethereum where miners can vote to adjust the gas limit, which is analogous to the block size in Bitcoin, a certain factor each block.

The perspective of "small blockers" (Bitcoin project)

Full nodes relay transactions and blocks and do full verification of the data they relay to other members of the (full node) network, enforcing consensus rules and serving as watchful eyes against potentially malicious miners. Bitcoin's value arose from the system eliminating trust in third-parties, having resilience to state-level attacks, and its censorship-resistant nature. All users having the ability to run a full node is essential to maintain these characteristics. As the cost of running a full node increases, a smaller percentage of users can afford validation and enforce consensus rules, and a greater percentage of users are forced into using Bitcoin in a trusted manner, relying on others to be honest, rather than the robustness of the system as a whole. Massive blocks will eventually result in full nodes residing only in data centers, which increases centralization by putting consensus in the hands of a limited number of entities, puts Bitcoin at a greater risk of getting shut down, and degrades privacy by requiring users to connect to other nodes. SPV (Simple Payment Verification) clients, which are lightweight clients that can prove a transaction is included in a block without downloading the entire blockchain, are incapable of trustless and complete validation.

At this time, even low-end computing devices such as a Raspberry Pi can serve as a functioning full node. Many desire a future where even smartphones can serve as full nodes.

In order for a full node to perform validation, it must propagate the entire UTXO set that it derived by processing the entire chain. The UTXO set can shrink by users and companies consolidating outputs, but it has been shownto steadily increase over time and can grow infinitely in size.

By primarily using the blockchain as a settlement layer for off-chain transactions and optimizing space efficiency through technological improvements, the UTXO set is managed much more efficiently, block propagation latency and initial blockchain syncing times are reduced, and the amount of bandwidth, CPU power, RAM, and disk space required to run a full node are minimized.

Off-chain payment-channels (like the Lightning Network) are being developed, which will be able to settle thousands or millions of transactions in a single transaction on the Bitcoin blockchain.

Although miners are the only entities that can produce new candidate blocks, economic full node operators signal and provide the incentive for miners to create valid blocks by rejecting invalid ones. If a miner were to produce an invalid block, such as one with differing consensus rules than those defined by the rest of the network (e.g. tampering with issuance rate of new bitcoins or altering the maximum number of bitcoins), full nodes would automatically ignore it even if a majority of the hash power accepted the block as valid.

The ability for full nodes to reject invalid blocks and trustlessly verify transactions leads to the saying "Don't Trust, Verify" — and this is why full nodes are deemed the network that miners are being paid to serve.

This is not to say that miners don't have any control at all. Both full node operators and miners power aspects of the system, despite having differing roles. Miners can choose what transactions they include in blocks (profit-maximizing miners will likely include ones with higher fees) and create new blocks, whereas merchants and other full node operators (including mining pool node operators) determine validity of blocks and transactions, enforcing consensus rules.

A User Activated Soft Fork (UASF) event in 2017 demonstrated that users operating full nodes were able to push miners to activate SegWit despite only a minority of miners initially signaling that they were in favor of the update.

The perspective of "big blockers" (Bitcoin Cash project)

Bitcoin Cash proponents look to scale toward unlimited block size and do not believe in the importance of full nodes being cheap to run for all. They claim the best version of Bitcoin was outlined by Satoshi Nakamoto in his original whitepaper,

blog posts, and emails. They believe Satoshi only considered miners to be the network and that consensus should be handled purely through hash power.

Some big blockers believe that users simply transacting never need to run full nodes, but some recommend incrementally increasing the block size in accordance to Nielsen's Law of bandwidth to allow users with "reasonable" computers and internet connections to continue to run full nodes.

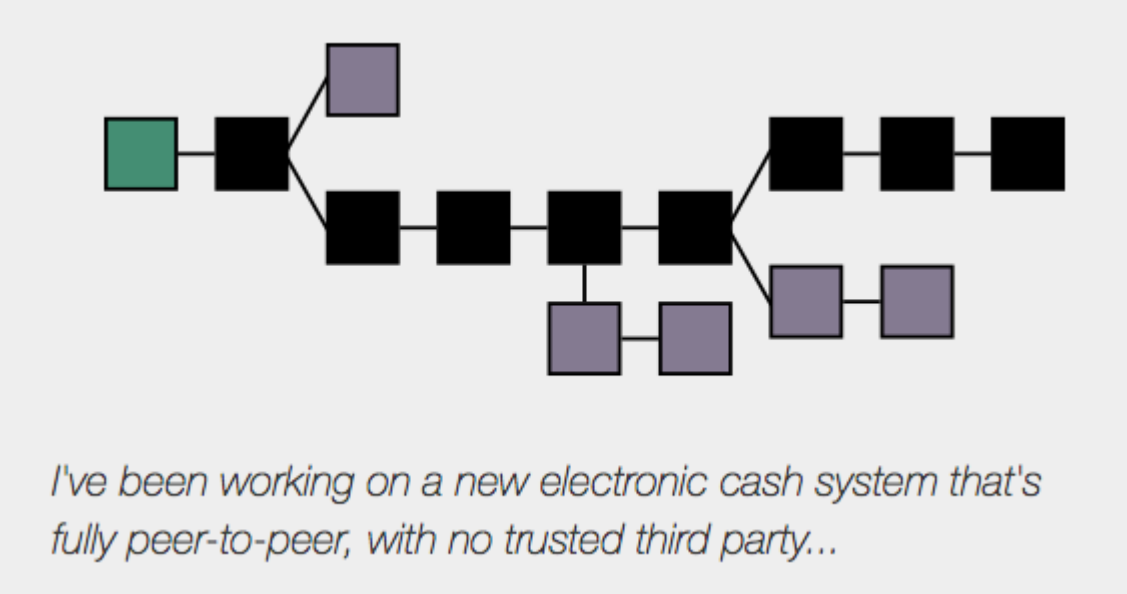
Miners are held accountable through profit-maximization and game theoretic market incentives. Miners will never collude as they are in direct competition with one another to find new blocks and get bitcoins as a reward. The security model of SPV is good enough for end-users, and full nodes are powerless, passive observers to the mining network. Full nodes are only needed by firms such as payment processors to provide services such as 0-confirmation transactions and serving merkle-branch proofs to SPV clients. There is nothing sacred about non-monetary Bitcoin consensus rules, which should be allowed to emerge through a market process.

From Mark Wilcox:

"The whole point of the Proof of Work game is that nodes cannot be trusted. The only thing we can trust is the difficulty of solving the problem, and the economic interests of everyone involved. This means that, quite crucially, 'everyone is responsible' is different from 'everyone must do everything'. We collectively need to protect the network. But the whole point of rewarding nodes that contribute hashpower is to free everyone else of the burden of having to worry about attacks on monetary policy or denial of service."

BCH proponents equate decentralization to competition and the network topology of miners instead of full node cost. They rejected SegWit, and Bitcoin Cash was their response. They encourage on-chain applications, such as the social network Memo, which small blockers would likely view as spam and encourage to be developed on upper-layer systems instead.

Addressing "Satoshi's Original Vision"



The perspective of "small blockers" (Bitcoin project)

BTC proponents believe that appealing to Satoshi's words is a logical fallacy of appealing to authority, and that Satoshi should no longer matter.

"If you see the Buddha or a Buddha, kill him."

They generally refer to BCH proponents as whitepaper "religious fundamentalists" who are unable to accept that Bitcoin has organically evolved since its inception. They view BTC as a far superior and more decentralized system than BCH due to the ability for full nodes to serve as a p2p network governance mechanism(**not** a democracy).

Many view BCH as a fraudulent project guided by leaders attempting to take over the Bitcoin brand and establish a centralized, miner-controlled system that requires trust in third-parties.

BTC proponents also mention that Satoshi laid the groundwork for the Lightning Network through a high-frequency trading payment channel design.

Satoshi's last words about block size were written in December 2010 during a discussion about BitDNS, a proposal to use Bitcoin for domain name issuance which led to the creation of a merged-mined blockchain called Namecoin.

"BitDNS users might be completely liberal about adding any large data features since relatively few domain registrars are needed, while Bitcoin users might get increasingly tyrannical about limiting the size of the chain so it's easy for lots of users and small devices."

Here, Satoshi alluded to the scaling debate and suggested limiting the size of the blockchain might gain consensus.

Bitcoin Cash did not receive social consensus to be called Bitcoin based on the User Activated Soft Fork, market cap, and hash rate. Instead, Bitcoin Cash hard forked to create a new network, whereas Segregated Witness was an update to the original Bitcoin network in which old software still functions.

The perspective of "big blockers" (Bitcoin Cash project)

BCH proponents pronounce that "Bitcoin Cash is Bitcoin" as they believe Bitcoin was designed to scale on-chain without 'non-mining full nodes' limiting the throughput of the system. They note that Satoshi referred to miners as 'nodes' in his writings.

From Satoshi Nakamoto:

"Only people trying to create new coins would need to run network nodes. At first, most users would run network nodes, but as the network grows beyond a certain point, it would be left more and more to specialists with server farms of specialized hardware." "The current system where every user is a network node is not the intended configuration for large scale. That would be like every Usenet user runs their own NNTP server. The design supports letting users just be users. The more burden it is to run a node, the fewer nodes there will be. Those few nodes will be big server farms."

BCH proponents feel small blockers co-opted the Bitcoin project to create a settlement network with high on-chain fees when blocks are full. Some believe Core developers succeeded at changing people's understanding of Proof-of-Work (PoW) game theory, as they interpret Satoshi's descriptions of PoW as mining being the only consensus mechanism.

12. Conclusion

We have proposed a system for electronic transactions without relying on trust. We started with the usual framework of coins made from digital signatures, which provides strong control of ownership, but is incomplete without a way to prevent double-spending. To solve this, we proposed a peer-to-peer network using proof-of-work to record a public history of transactions that quickly becomes computationally impractical for an attacker to change if honest nodes control a majority of CPU power. The network is robust in its unstructured simplicity. Nodes work all at once with little coordination. They do not need to be identified, since messages are not routed to any particular place and only need to be delivered on a best effort basis. Nodes can leave and rejoin the network at will, accepting the proof-of-work chain as proof of what happened while they were gone. They vote with their CPU power, expressing their acceptance of valid blocks by working on extending them and rejecting invalid blocks by refusing to work on them. Any needed rules and incentives can be enforced with this consensus mechanism.

BTC proponents stronglyobjectto the contention that miners ever controlled consensus rules. They note that even in theoriginalnode software, the longest PoW chain rule only applied to resolving disputes between multiple chains using the same consensus rules, and nodes had the option to generate coins or not.

Role of SPV

In contrast to full nodes, the type of software for lightweight Bitcoin clients is SPV (Simple Payment Verification). SPV clients allow a user to connect to one or more nodes (i.e. from a smartphone), determine the latest block with longest PoW chain, and request block headers (80 bytes each) from the node(s).

As described in section 8 of the whitepaper, a user can obtain the merkle branch which confirms their transaction is inside a block with a valid block header and proof of work. Further confirmations (new blocks on top of the other block) demonstrate further work was done.

SPV clients cannot validate blocks or consensus rules themselves, so they must trust the validation of the node(s) they are connected to.

A theoretical way to increase SPV security, among others, was proposed by Satoshi in the whitepaper. It would allow nodes to alert SPV clients when invalid blocks are detected. Fraud proofs could prove the existence of these invalid blocks with minimal resources required. Although fraud proofs are not implemented today, SegWit enables them to be integrated into Bitcoin with a soft-fork, which is a change that is backwards compatible with old clients and tightens or adds new rules.

Segregated Witness

A 2017 soft-fork to BTC called Segregated Witness, or SegWit for short, was activated as the result of a multiple year scaling debate. It was primarily a bug fix to an issue involving the malleability of transactions, but also adds more space for transactions and enables easier future updates and extensions through soft forks.

What is malleability?

Before SegWit, there were malleable (changeable) parts of transactions. For example, a node relaying a transaction or a miner including it in a block could add extra bytes to the transaction's signature. This changes the ID, which is a cryptographic hash of the entire transaction, including the signature.

Although there is malleability in other computer software, in the case of Bitcoin, changing the transaction ID after the transaction propagated to the network prevented wallet software to track transactions by ID, users from performing certain types of transactions, and developers from creating certain types of smart contracts.

For example, a valid transaction can spend an unconfirmed output (not yet included in a block) as an input to another transaction in the same block. If the transaction ID of the unconfirmed output was malleated, the first transaction would be confirmed

as it's still valid, but the second transaction would be invalid because the transaction data would include aninvalid *Previous tx* attribute.

Miners, full nodes, and users can choose to use SegWit or not, since it was a soft fork. As of May 2018, transactions with SegWit inputs make up approximately 35% of transactions, and SegWit nodes are at approximately 99% distribution.

The rest of this section is fairly technical, so feel free to skim or skip to the "Bitcoin Maximalism" section if you are a beginner.

Witness data refers to signatures and unlocking scripts. With SegWit, miners "segregate the witness" by placing the witness data in a separate merkle tree (the data structure inside a block that holds transactions) called the witness merkle tree, which mirrors the transaction tree. The witness root hash is stored in the coinbase transaction, which is the transaction that miners use to pay themselves newly minted bitcoins. Therefore, signatures for SegWit transactions are still included in blocks, since the coinbase transaction affects the merkle root hash that is stored in the block header of a block.

If miners choose to not update to SegWit, then they can't mine blocks with SegWit inputs, as to them these are non-standard transactions. They can still receive SegWit transactions with the witness structure stripped.

The SegWit update(for more detail see SegWit benefits) **:**

- Phases out block size in favor of block weight. Currently, blocks can have at most 4 million weight units (WU). A byte in the original block structure weighs 4 WU, whereas a byte in the witness structure only weighs 1 WU. For more, see "Understanding Segwit Block Size."
- Reduces the UTXO size for SegWit transactions by the size of witnesses, which is around 60–75% of the data. The discount on weight units for the witness structure was introduced to incentivize more responsible growth of the UTXO set by lowering fees.
- Increases the amount of data that can be stored in blocks as the percentage of SegWit transactions increases. The largest block we have seen is 2.1MB.
- Allows payment channels, such as the Lightning Network, to take advantage of the malleability fix.
- Fixes quadratic scaling of Sighash operations.
- Enables the checksummed Bech32 address format.
- Introduces Script versioning to allow for easier soft-forks in the future for features such as SPV Fraud Proofs, Schnorr signatures and Signature aggregation and MAST which compress data and further aid on-chain scaling, and Confidential Transactions.
- Makes covert ASICBoost ineffective (though some dispute the relevance of ASICBoost in the first place).

The following are arguments against SegWit:

- Some users prefer that Bitcoin developers change Satoshi's codebase as little as possible.
- SegWit and the Lightning Network do not solve the scaling debate because users will always have disagreements over how much it should cost to run a full node.
- SegWit technically used a mandatory extension block making it an "Evil Fork" or "Forced Fork."
- Pushing the new Bech32 address format onto users invalidates the network effect that was built upon the original address format over the last nine years.
- It is technically possible for miners to censor SegWit transactions in an anti-UASF movement by not including any transactions involving SegWit inputs.
- Jihan Wu, the CEO of Bitmain which is the largest mining ASIC manufacturer, called SegWit transactions "unfairly cheap" due to the discount on witness data.

Bitcoin Maximalism

There are different flavors of Bitcoin Maximalists, but they all believe that Bitcoin is the best and most secure blockchain which has the strongest network effect, most desirable monetary policy, and a highly-capable scripting language built which allows for future development.

Bitcoiners generally believe the idea of a 'token economy' reveals a deep misunderstanding of monetary systems as a whole and view tokens as snake oil. They strongly reject a future world of 10,000 currencies, seeing it as no different to barter — the very problem that money is supposed to eliminate. They believe that value accrues to the money held, not necessarily the one transacted with, and the long tail of 'tokens' will suffer from extremely high velocity, rendering them with

little to no value accrual and serving as unnecessary friction even if abstracted away from the end user.

Upper-Layer Systems and Alt-Coins

Many Bitcoiners view alt-coins as testing grounds for features that may eventually be integrated into Bitcoin if desirable by users.

It is theoretically possible to copy almost any blockchain, even a giant block one, and put it on a Bitcoin sidechain. Paul Sztorc's Drivechain project, which is currently under development, would allow these blockchains to inherent Bitcoin's mining security, although it requires a soft-fork and is awaiting more extensive peer review.

There are three main categories of changes that would (likely) never be integrated into Bitcoin's base layer.

- Alternative **consensus mechanisms** to replace Nakamoto Consensus, such as Proof-of-Stake (Tendermint, Ethereum's Casper, DFINITY's Threshold Relay), Chia's Proof-of-Space, EOS' Delegated Proof-of-Stake, Algorand's Weighted Proof-of-Stake, or Ripple and Stellar's Federated Byzantine Agreement.
- Alternative data structures to replace the **blockchain**, such as Coda's succinct blockchain, DAGlabs and HashGraph's DAG, or Nano's block-lattice.
- Alternative **governance mechanisms** to replace full node p2p network governance, such as Decred or Tezos' on-chain governance, DFINITY's Blockchain Nervous System AI governance, or Bitcoin Unlimited's miners voting.

Bitcoiners generally take issue with Proof-of-Stake (PoS) where validators propose and vote on blocks instead of solving energy-intensive cryptographic puzzles. They believe Bitcoin software should be handled with the same respect as nuclear reactor software, and discount PoS due to its "subjective" nature, which means participation in the network requires subjective information like social information. This contrasts to PoW objectivity where nodes necessarily arrive at the current state by observing the heaviest PoW chain.

Many view PoS as a digital version of the fiat-money system, with PoS validation being anti-competitive in comparison to mining and lacking any ties to real-world value (energy).

Meanwhile, PoS advocates have "learned to love" weak subjectivity and aim to simulate the security of PoW through threats of economic penalties for validators (slashing dishonest actors by taking away deposits) instead of burning physical energy. They deem PoW as energy wasteful, and think it's possible to design a PoS

protocol that is more secure, decentralized, offers faster block times, and is more flexible than PoW, which is "limited" by physics.

In distributed systems terms, Nakamoto Consensus favors liveness (availability) over safety (consistency) and achieves probabilistic finality of transactions that increases with the number of new blocks.

Currently, with Casper's PoS, for example, economic finality is to be achieved once validators fully commit to a block and comes at the cost of some availability. Because finality requires some upper-bound synchrony asumption, extraordinary events could theoretically partition a significant portion of the network or shut down the entire network for a greater amount of time than this upper-bound validator response time.

This could cause either some partitions to lack the majority of votes needed to come to consensus or the lack of ability for the network to choose a canonical chain when the partition or shut down ends. This could end with liveness or safety faults requiring human action, whereas with PoW, network partitions create temporary forks, which are necessarily resolved through the heaviest chain once the partition is resolved.

There is overwhelming consensus that there should be no experimentation and as little changes made as possible to the base BTC layer, and that payment channels and sidechains should not weaken the security of the base layer. Some users are enthusiastic about the potential of upper-layer systems to bootstrap further utility on Bitcoin.

The main philosophy is to have a hyper-decentralized, hyper-secure base layer that is used to bootstrap security for slightly more insecure protocols on top layers.

Lightning Network

Proponents of the Lightning Network consider it to be the most feasible solution to the current Bitcoin scalability problem, allowing people to transact nearly without limits using peer-to-peer payment channels and smart contracts, while using the *main* Bitcoin chain for occasional settlement purposes.

Despite only being conceptualized three years ago, and only being in beta for several months, the Lightning Network is already seeing a wave of innovations, such as Dual-Funded Channels, Submarine Swaps, Channel Splicing and Factories, Watchtowers, Eltoo, Atomic Swaps, and more all covered here.

One common concern about second-layer solutions is that they will negatively impact miners revenue by taking more transactions off-chain.
Initial research, presented at Scaling Bitcoin 2017, estimated that miner revenue

could increase after 20 million users were using the Lightning Network, although decrease under that threshold.

It is important to note that Lightning Network is an extremely new, unproven and immature system. However, many developers believe that it will greatly improve the scalability of Bitcoin and enable cheap micro-transactions, paving a way for Bitcoin to potentially be used as an effective medium of exchange and true global currency.

At the very least, Lightning Network occupies a niche, which will be valuable in itself. And at the most, we haven't even scratched the surface of the upside, potential, and capabilities enabled by the Lightning Network, such as third-layer projects.

Conclusion

Bitcoin is the original, longest-lasting cryptocurrency with the highest levels of hashpower, network effects, liquidity, market capitalization, and arguably the highest amount of "HODLers of last resort." This article attempted to outline the so-called 'small blocker' and 'big blocker' positions on the most notable changes, milestones and debates throughout Bitcoin's past and its near-term future.

The open-source, global and decentralized nature of these digital money-forms makes the governance of these systems complex and even minor changes contentious and controversial. Almost 10 years into its history, Bitcoin and other cryptocurrencies as an asset class are beginning to challenge monetary metals as the defacto store of value assets of the future, as well as challenge existing global payment rails and mechanisms. We believe that the future is bright for Bitcoin and its spiritual brethren.

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