CRYPTO WORDS

CY19 Q2 April

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

Contents

Goals and Scope

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

History

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

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

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

Bitcoin: An insurance policy against the largest monetary and fiscal policy experiment in human history

By Travis Kling

Posted April 1, 2019

Quick Take

- The world is in the midst of the largest monetary and fiscal policy experiment in human history
- That 'experiment' is now 10 years old and facing daunting challenges, because risk assets are now entirely reliant on cheap money
- Every fiat currency in history has completely failed in its ability to maintain purchasing power
- It would be naïve to think this 'experiment' is going to end without significant market stress. A bet on Bitcoin is opting out of this experiment
- Bitcoin is a better long term store of value than both fiat currency and gold

The following piece is a contributor essay from Travis Kling, the Chief Investment Officer of Ikigai Asset Management, a crypto asset hedge fund. Prior to founding Ikigai,Travis spent 10 years in traditional finance, most recently as a portfolio manager at Point72. Disclaimer: This is not investment advice.

More than a decade ago, on the back of the global financial crisis, the world began the largest monetary and fiscal policy experiment in human history: globally-coordinated quantitative easing while running massive deficits on top of increasingly untenable debt levels. That 'experiment' is now 10 years old and facing daunting challenges, because risk assets are now entirely reliant on cheap money.

In 2017 the Fed slowly began shrinking its bloated $4.5 trillion balance sheet and raising rates. By late 2018, this tightening put risk assets globally under significant stress. In late January, on the back of market stress and President Trump chastising the Fed on Twitter, the Fed capitulated. They made a complete U-turn from quantitative tightening and a hawkish stance to an openness to further easing and a decidedly dovish stance.

This dovish stance was confirmed by Chairman Jerome Powell on 60 Minutes on March 10 and solidified by the FOMC statement on March 21. On March 26 Stephen Moore, the President's recent nominee for the Fed board, publicly lobbied for his nomination by stating he would demand a 50bps rate cut if appointed. The Fed,

billed as an independent organization unaffected by the political machine of Washington, has unequivocally become politicized.

Over the last several months, commentary and actions from the ECB, BoJ, PBoC and RBA have echoed the Fed's dovish capitulation. Global central banks have resoundingly taken their stand – rather than attempting to unwind the 'experiment', central banks and governments globally look likely to keep printing money at a breakneck pace.

To frame the current environment, the US dollar has only existed as a fiat currency for 48 years. In 1861, the U.S. treasury printed its first paper currency and for 110 years, those dollars could be redeemed for gold. When Nixon abolished the gold standard in 1971, the U.S. dollar became a fiat currency. Fiat currencies have been around since 11th century China and, without exception, every one has failed in its ability to maintain purchasing power.

As an alternative to this relentless devaluation, civilizations have been using gold to store value for ~ 5,000 years. Ten years ago, a new store of value emerged, based on computer science, cryptography and game theory. And after a tremendous price run-up in 2017 and subsequent crash in 2018, Bitcoin appears to have found a bottom. Over that time, Bitcoin has also been finding its identity – a non-sovereign, hard-capped supply, global, immutable, decentralized, digital store of value. It is Gold 2.0, and a compelling argument can be made that bitcoin is better at being gold than gold.

Similar to gold, much of bitcoin's value is derived from its limited supply. Gold's annual supply increase has historically been 1-2%, giving holders confidence that its purchasing power won't be diluted. Bitcoin's supply is the most predictable ever – there will only ever be 21 million. When compared to gold, Bitcoin more effectively satisfies the six characteristics of money: durable, divisible, portable, uniform, scarce and accepted. The world has a new, arguably better form of money.

Does the world need a new form of money? We have an interesting backdrop for a non-sovereign, hard-capped supply, digital form of money to gain mass adoption. The increasingly erratic U.S. president is yelling at an irresponsible central bank to act even more irresponsibly with its monetary policy, while running a $1 trillion deficit for the second year in a row. Bitcoin is a risk asset right now, but it is a risk asset with a specific set of investment characteristics. The more irresponsible monetary and fiscal policies are, the more attractive those characteristics become.

It would be naïve to think this 'experiment' is going to end without significant market stress. A bet on Bitcoin is opting out of this experiment. Whether it's 1%, 5% or 25% of a portfolio, a bet on Bitcoin means there's a chance this experiment could go very wrong, and portfolio protection from that downside scenario is warranted.

Bitcoin prices have been understandably volatile. It makes complete sense that the world is having a hard time understanding, and in turn valuing, Bitcoin. A new form of money doesn't come around very often. It is in fact exceedingly rare for an entirely new and superior store of value to emerge. Ancient civilizations used seashells, salt, and heavy rocks for thousands of years to store value – each eventually failed to maintain purchasing power. Then gold was discovered, deemed superior, mass adopted and propelled to be the global monetary standard. Today global gold supplies are valued at $8 trillion. If the world decides Bitcoin is a superior store of value to gold, the price of Bitcoin will likely increase significantly from current levels. In the meantime, central banks and governments around the world are proving the profound need for a non-sovereign, hard-capped supply, global, immutable, decentralized, digital store of value.

Managing Bitcoin and Private Keys

By Thib

Posted April 1, 2019

Owning a bitcoin means controlling the underlying private key that secures it.** If lost, no recovery is possible. No third-party can help. It's irrevocably gone.

Private keys must be kept secret and protected at all times. This is non-trivial for most users, with many severe financial losses in the past attesting to such unfortunate reality (here, there, over here and more there).

Private keys govern how bitcoins are spent (or moved between UTXOs, to be precise). Bitcoins are securely stored on a globally distributed ledger. The ledger is replicated and synced across anyone who wants access to it to verify how bitcoins are moved within the network. This is usually done by running a full node (more on that later). Private keys unlock bits of this ledger, called addresses (or UTXOs), where bitcoins are stored.

Managing private keys

A Bitcoin private key is a 256-bit data unit, often represented as an hexadecimal string, which can be understood as a digital bearer asset with intrinsic financial value.

It is code with a price tag. Money is now pure software. Anyone in possession of a private key is deemed the rightful owner of the associated bitcoins.

From generation, to storage and utilization, private keys deserve delicate care and extreme caution for Bitcoin to be utilized securely as a global value communication protocol on the Internet.

Generating new Bitcoin private keys requires randomness to ensure no one can easily guess what it is. Once it is created, it must be stored securely, sometimes offline, to reduce the possibility of loss or theft. When used to approve or sign Bitcoin transactions, private keys must be cautiously managed to avoid introducing risks of loss. Secure backups may also be used with additional security to recover compromised or lost private keys.

This is an oversimplification of private key management, applied to Bitcoin.

Security issues are real

Exclusive control of private keys, echoing with rightful ownership, is primordial for bitcoin owners. But self-managing private keys brings an unusual responsibility that can be problematic to most people. Cutting trusted third parties, such as banks for credential recovery, requires full accountability over private key management. Not an easy feat for most.

In many countries, consumers are legally protected from any liability in traditional banking as most transactions are traceable and reversible. Bitcoin transactions while traceable are irreversible, leading to permanent losses with no legal recourse to authorities or financial protections.

Users who manage their own bitcoin private keys rely on setups that often require technical skills, an advanced dedication for security and a high risk tolerance as simple errors are still quite common.

Over the last decade, multiple improvements were released by individuals, open source projects and companies, making bitcoin private key management much easier and minimizing safety trade-offs, while ensuring users retain full control of their funds in the best cases.

Full control means bitcoin owners can be sovereign in how they manage their wealth, independently from trusted third-parties, which is essential for bitcoin's long-term morphing from a value communication protocol on the Internet into a global peer-to-peer economic system.

Custodial wallets

Today, most bitcoin owners still leave private keys on online custodial wallets such as exchanges after having acquired bitcoins, delegating full control of their private keys to trusted third parties.

There isn't comprehensive data on the third-party custodied proportion but it is public knowledge that Coinbase, a popular cryptocurrency exchange, recently announced they possess 5% of bitcoin's circulating supply under custody, drawing attention to the large portion of bitcoin holders giving away full control of their assets.

Exchange platforms make it ridiculously easy for people to acquire and store bitcoins, reducing the anxiety that comes with the self-custody responsibility. They are one of the most essential and valuable products to onboard new users. But simplicity is often mistakenly associated with security.

Multiple custodial exchanges have lost customers' bitcoins in the past due to hacks, as they turn into honey pots for hackers or internal collusion jobs. User credentials have been stolen, 2-factor authentications have been spoofed and private keys were compromised with no recourse for affected users. Mt. Gox is the obvious illustration with 850,000 BTC lost, but there was also Coincheck with over $500M stolen, and most recently QuadrigaCX that lost $190M of customers' funds. Lots of other cases (here, there or here) have happened, totalling hundreds of millions of customers' funds that are gone forever.

Many web, mobile and desktop wallets also have full custodial control of their users' bitcoins, which introduces similar risks as with exchanges. Aesthetically-pleasing user interfaces with highly usable experiences lure users into trusting them.

Often these products are developed by small teams of developers or early-stage companies with light governance, fragile security models and no credit history, making these counterparties highly risky to delegate full control of your funds.

Some custodial wallets may let users control a portion of their private keys but still force users to rely on trusted third-party full nodes to verify Bitcoin transactions. More on that later.

Non-custodial wallets

Self-custody of bitcoin private keys is therefore the most advisable alternative to eliminate reliance on unproven third parties. "Not your keys, not your bitcoins" is being thrown around over and over in the community but it often takes some time (rightfully so) to fully grasp why that concept truly matters.

Efforts in the Bitcoin community, such as the Proof Of Keys movement initiated by Trace Mayer, are attempts to make more people care about controlling their own keys to protect their bitcoins, asking bitcoin holders to withdraw their private keys from custodial exchanges into the non-custodial alternatives described below.

Bitcoin's architecture design using public key cryptography allows users to be sovereign by self-managing their wealth in an effort to cut the overwhelming dependence on trusted financial institutions such as banks.

With that principle in mind, non-custodial wallets have been developed to help users safekeep bitcoins on their computers, mobile devices, specialized hardware and even paper.

Non-custodial desktop wallets can be "lightweight", meaning they need to be connected to a full-node of the Bitcoin network to verify transactions.

Full nodes are used in Bitcoin to transparently verify the transactions that are happening in the network, without trusting an intermediary to report information. All the Bitcoin transaction history since the network was born on the Internet on January 3rd, 2009 are stored and accessible in any active full node.

Using Simple Payment Verification (SPV), non-custodial desktop wallets ask full nodes to verify specific transactions, which diminish privacy if done with a trusted third-party full node, but is fine if it is user-owned. Using this method, bitcoin holders are truly sovereign in how they manage their private keys and verify that their transactions went through.

Lightweight desktop wallets include Electrum or Wasabi, which rely on their corporate servers to verify user transactions as trusted full nodes, reducing user privacy.

For lightweight desktop wallets that don't rely on third-party full nodes, users need to set up and operate their own Bitcoin full node and have the patience to perform the initial block download from the genesis block to today, which may take several days or weeks depending on technical limitations such as bandwidth and processor speed.

This makes desktop wallets easier to use for regular users who may not have sufficient computer disk space to store the entire Bitcoin blockchain history directly on their computer, or enough network bandwidth to download the 215GB of transactions. Some companies such as Nodl, Casa and Samourai's Dojo are making full node plug-and-play products to help onboard less tech-savvy users.

Other desktop clients have "full-verification nodes," which requires users to download Bitcoin's entire blockchain transaction history without requiring any external full node for verification.

Besides the technical specifications required for the computer to perform such operations (at least 500GB of disk space as Bitcoin's blockchain is 215GB now and growing, with high network bandwidth and reasonable CPU), users need to have this wallet connected to the Internet constantly.

This is to prevent the in-app full node from disconnecting from the network and having to re-sync to download the latest blocks, which introduces delays until the full node is fully synced again to the tip of Bitcoin's blockchain.

Full node desktop clients include Armory or Electrum. Unfortunately, hardware failure risk and Internet connectivity via Wi-Fi for desktop computers and laptops make users prone to a wide range of online security risks on desktop wallets.

Mobile

Similar to desktop clients, mobile wallets store private keys on user devices, which are connected to the Internet via Wi-Fi and cellular networks such as LTE. They are available on either Android, iOS or Windows Phone.

Bringing better usability, mobile wallets are by default "lightweight" wallets due to the hardware memory and bandwidth constraints tied to mobile devices. Mobile wallets also use SPV and either rely on trusted third-party servers providing transaction verification (which isn't favorable) or connecting to user-owned full nodes.

As noted, SPV wallets can introduce privacy concerns for users when there is a trusted third-party full-node involved in providing transaction verification. For users operating their own personal full node, privacy concerns using SPV are diminished.

Mobile devices are reasonably more secure than desktop computers with data encryption but still face hardware failure risks, social engineering and physical losses. Strikingly, they are ubiquitous and can be useful in other multi-party configurations that we will cover later on.

Mobile wallets using trusted third-party full-node servers include Mycelium and Blockstream Green. Some rely on one core corporate server, which is the least favorable option for privacy and security, while other configurations randomly select verification servers from a trusted list, which reduces privacy concerns.

Other mobile wallets connecting to user-owned full nodes include BRD Wallet and Zap on iOS, Electrum Wallet with Samourai Wallet on Android. HODL Wallet is

available on both iOS and Android and lets advanced users choose between connecting to their own full-node or using their third-party server.

Specialized hardware

Dedicated companies have developed specialized hardware products to make it safer and easier for owners to store their bitcoins independently of any trusted third parties, while reducing risks of traditional desktop and mobile wallets.

Hardware wallet providers such as Trezor, Ledger and Cold Card Wallet are the most popular manufacturers. Specialized hardware in the form of USB-like devices store private keys offline to reduce the potential attacks from hackers that users may face but require users to trust the hardware providers and their full-node APIs to verify transactions.

Specialization of hardware devices is an attempt to prevent physical extraction of private keys. Hardware wallets are either connected to desktop or mobile apps to execute operations in tandem with a trusted interface built-in on the device. Users need to have these specialized devices physically each time they want to move funds to and from their wallet, which is not the most convenient.

Even with added security features, multiple cases of losses and thefts occurred in the past due to people buying reused hardware wallets (always buy directly from verified manufacturers) or loosing the device with its recovery (here or here).

In case of physical loss or destruction, hardware wallets have backups that need to be stored separately to recover the private keys they contained.

Physical backups

Backups of private keys must be stored by users who are advised to write them down on a piece of paper. Backups, also called seed, recovery or mnemonic phrase, are the ultimate option for users to recover funds in case private keys get lost or compromised via a web, mobile, desktop or hardware wallet.

Storing backups is a responsibility that is outside the scope of hardware, web, mobile or desktop wallet providers. This introduces potential user errors and likely loss events if backups are lost or compromised. It is the ultimate recovery material. If lost or compromised, there are no recourse.

Backups must be stored offline to minimize risk exposure to theft and loss, which involves operational and physical security. Preventive measures must be considered to avoid physical theft of recovery material, which would lead to the compromise of the entirety of the associated private keys and funds.

Floods, fires, earthquakes and other catastrophic events may very well destroy the backups users are storing in their homes or workplaces. Companies such as Cryptosteel, Hodlinox or Billfodl are developing heat-resistant steel plates to prevent long-term degradation of backups.

Redundancy of backups across geographies is advisable, which introduces other risks and dependencies. Sharding, or splitting, backups into multiple sub-parts help reduce the likelihood of a malicious actor compromising the funds. Vault providers can help store redundant or partial copies of backups for maximum security but introduce third-parties.

Operational complexity and cognitive burden rise dramatically as a direct cost of extended security measures. Today this is the state-of-the-art for backups and recovery of bitcoins.

Open-source frameworks

Open-source software and procedures, such as Glacier, a protocol for high-security bitcoin storage have been released by the community in an attempt to create an industry standard. It is a highly-involved operational procedure, which require redundant, quarantined and special-purpose hardware.

Physical dice are used to generate true randomness that algorithms on computers aren't capable of creating properly. Combined with purpose-limited offline computers, truly random private keys are generated, and stored on offline paper wallets.

This is a deep cold storage, which involves machines that have never been connected to the Internet and never will with one-time disposable hardware that gets burned after having generated private keys.

All these operations must happen in a faraday cage to nullify the exposure to potential radio-wave side attack channels. Not a procedure for your casual user securing his bitcoins. Minimum expense for that configuration is roughly $600 and takes 5-7 hours of initial set up.

Institutional custodians

With the rise of Bitcoin's market cap in 2017, institutions have showed interest in the safekeeping of bitcoins with novel configurations. As fiduciaries, institutions are forbidden to self-custody bitcoins and are required to hold funds using dedicated third-party custodians that are regulated under the appropriate regulatory regimes, licenses and supervising entities.

With the segregation of duties between investing and custody, custodians have emerged as a quality interim solution to bring institutional liquidity in the market

until regulations and technology mature sufficiently to have reliable non-custodial infrastructure deployed mass market.

Custodians often provide bespoke governance, internal controls, proof of reserves and insurance guarantees for fiduciaries with multi-party authorizations, where many signatories are registered to collectively approve transactions on bespoke governance rules.

Multiple companies are working towards getting a share of the market, with notable entities such as ICE's Bakkt (still pre-launch), Fidelity Digital Assets, Anchorage, Xapo or KNØX.

Multi-signature

Multiple signing authorities can be required to execute Bitcoin transactions. Multi-signature is a built-in feature of Bitcoin's P2SH (pay-to-script hash) at the base protocol layer that has been available since the early days. This design reduces single points of failure and enable bespoke transaction governance rules based on amounts, time locks and specific use cases.

Multi-signature schemes, where 2 authorizers out of 3 registered would be required to execute on a transaction, allow users to retain full control of their bitcoins, controlling 2 keys, while ensuring continuity in case of loss with other parties controlling the remaining key. The architecture of such system is non-trivial to design and implement securely while abstracting away the complexity from the end-user experience.

Companies such as Casa has recently released multi-signature wallets for users, letting consumers store keys across their devices, and a few with Casa creating a "seedless" configuration, where users can get their private keys recovered using other keys securely held by Casa in case of loss events. BlockstreamGreen has been updated recently with a new multi-signature mobile wallet for consumers using "2-of-2 multisig by default, with one key held on the device, and one key held on Blockstream's servers." BlockstreamGreen send pre-signed transactions to users, which only need the user signature to be treated as valid transactions. Muun is the another multi-signature mobile wallet for Bitcoin. "As a non custodial service, Muun helps users fulfill Bitcoin's be-your-own-bank promise, and protect their funds from trusted third parties, attackers and human error [...] transactions are protected with 2-of-2 multisig and theft detection. A personal key is stored in your phone. Muun holds a co-signing key."

On the institutional side, Unchained Capital has recently announced their "collaborative custody" product, as "a superior approach to security that combines the control of self-custody with the benefits of a managed financial service. Ledger

Vault was released in 2018 as a "multi-authorization cryptocurrency wallet management solution enabling financial institutions to safekeep their funds [...] looking for convenience and streamlined operations with zero compromise on security." Ciphrex, is an open-source, free to use multi-signature desktop wallet. "It supports the best security practices in the industry and is rated amongst the most secure wallets by bitcoin.org." MuSig, was released by Blockstream earlier in 2019, as a new multi-signature standard to offer "provable security, even against colluding subsets of malicious signers, and [producing] signatures indistinguishable from ordinary single-signer Schnorr signatures." Blockstream has proposed their code implementation to be deployed into Bitcoin development environments, which may happen later on should it pass community standards.

An ongoing quest...

Multiple developments are currently happening for bitcoin private key management in an effort to blend security with usability and user sovereignty. A peer-to-peer, country-agnostic and economic system built on Bitcoin deserves novel solutions to onboard the next millions of consumers and businesses without introducing reliance on trusted third parties.

It has only been 10 years since Bitcoin's birth so the industry still deserves additional infrastructure development for Bitcoin private key management. Safekeeping private keys and utilizing public key cryptography has proven to be a non-trivial but ever-evolving endeavour.

Perhaps in 10 years, most Bitcoin hodlers will be able to securely manage their private keys without knowing how the system operates in the back-end, collectively storing a portion of the world's growing Bitcoin wealth.

Owing a lot to Antoine, Ben, Allen who reviewed early draft versions of this writing, and specifically to Sun and Zane with whom we're trying to make bitcoin private key management better for us three. Learning everyday from the best, who are helping us shape a better understanding of Bitcoin, for private key management, security, privacy, usability and so many other important things: @JackMallers @giacomozucco @francispouliot_ @LukeDashjr @lopp @starkness @valkenburgh @nic__carter @fernandoulrich @LarryBitcoin

---

The case for a small allocation to Bitcoin

By Wences Casares, CEO of Xapo

Posted April 11, 2019

Why most portfolios should allocate up to 1% to Bitcoin

Summary

Bitcoin is a fascinating experiment but it is still just that: an experiment. As such it still has a chance of failing and becoming worthless. In my (subjective) opinion the chances of Bitcoin failing are at least 20%. But after 10 years of working well without interruption, with more than 60 million holders, adding more than 1 million new holders per month and moving more than $1 billion per day worldwide, it has a good chance of succeeding. In my (subjective) opinion those chances of succeeding are at least 50%. If Bitcoin does succeed, 1 Bitcoin may be worth more than $1 million in 7 to 10 years. That is 250 times what it is worth today (at the time of writing the price of Bitcoin is ~ $4,000).

I suggest that a $10 million portfolio should invest at most $100,000 in Bitcoin (up to 1% but not more as the risk of losing this investment is high). If Bitcoin fails, this portfolio will lose at most $100,000 or 1% of its value over 3 to 5 years, which most portfolios can bear. But if Bitcoin succeeds, in 7 to 10 years those $100,000 may be worth more than $25 million, more than twice the value of the entire initial portfolio.

In today's world where every asset seems priced for perfection, it is hard, if not impossible, to find an asset that is so mispriced and where the possible outcomes are so asymmetrical. Bitcoin offers a unique opportunity for a non-material exposure to produce a material outcome.

It would be irresponsible to have an exposure to Bitcoin that one cannot afford to lose because the risk of losing the principal is very real. But it would be almost as irresponsible to not have any exposure at all.

What is interesting about the Bitcoin Blockchain?

Throughout this essay I refer to the "Bitcoin Blockchain" when I am referring to the Bitcoin platform as a whole, including the Bitcoin Blockchain and the Bitcoin currency. Many different systems for different use cases may one day run on top of the Bitcoin Blockchain. When I refer to "Bitcoin" I am referring to Bitcoin the currency, that can be bought, sold, sent, received, held, etc. You can think of the Bitcoin currency as the first system to run on top of the Bitcoin Blockchain.

The current state of the Bitcoin Blockchain is similar to the state of the Internet in 1992. Back then the Internet was very nascent and experimental. Just like with the early days of the Internet there are many bold claims about how the Bitcoin Blockchain will revolutionize the world and solve so many problems. Many of these claims are exaggerated or wrong. Even though right now most of us feel like we do not fully understand the Bitcoin Blockchain, over time we will all does not get any value from having a sovereign platform can you be correct to assume that the Bitcoin Blockchain electricity consumption is an enormous waste.

Bitcoin miners secure the Bitcoin Blockchain because they get paid in bitcoins to do so. The Bitcoin Blockchain is secured, to an important degree, by the bitcoins that the miners earn. If you were to remove the bitcoins, most miners would stop mining and, therefore, the Bitcoin Blockchain would not be very robust and not very sovereign. In corporate circles, especially in financial institutions, it has become fashionable to say "I am interested in the Blockchain but not in Bitcoin", which is the same as saying "I am interested in the web but not interested in the Internet" (remember Intranets?), not understanding that the web could not exist without the Internet. The only innovation of the Blockchain is it's sovereignty, the only sovereign Blockchain so far is the Bitcoin Blockchain and the fuel that keeps it sovereign is the Bitcoin currency. It is like a boa eating its own tail.

If a group of people wanted to take away the Bitcoin Blockchain sovereignty today they would not only need an extraordinary amount of capital and the capacity to develop specialized mining hardware in very large quantities, but they would also need access to the equivalent of the United States largest hydroelectric dam for an extended period of time. That would be hard to do but not impossible. Every day that goes by it gets even harder to "break" the Bitcoin Blockchain sovereignty. The Bitcoin Blockchain sovereignty has been attacked in the past (in fact, one of those attacks found me on the wrong side of history and that is how I painfully learned many of these lessons, but that's another story...) and so far it has always survived intact. We can expect the Bitcoin Blockchain sovereignty to come under attack from more and more resourceful bad actors, coalitions of bad actors or even from nation states eventually. Only time will tell if Bitcoin is truly sovereign or not.

Where can a sovereign platform add value?

It is a lot easier to see where the Bitcoin Blockchain will NOT add any value. For any Blockchain to add value it has to be the ultimate arbiter of truth: nothing has to be able to contest it or change it. For any use case in which the Blockchain information can be contested or changed by a government, by a registrar of deeds, by a court, by the police, by the SEC or by any other authority it does not make sense to use a Blockchain. Claims that the Blockchain can solve property titles, securities settlement, supply chain management, the authenticity of works of art and many

other similar cases are misplaced. It is true that the systems that we are using today in all of those cases are old, antiquated and inefficient. And it is true that all of those cases involve many stakeholders that use different data formats and transaction protocols that are often proprietary, but all of those problems would be better solved if those stakeholders agreed to use open standards and if they used better technology. Most often the word “Blockchain” is being waved frantically by consultants who want to scare their corporate customers into buying new technology projects, or by executives at those corporations who do not yet understand the Blockchain but understand that they may get the budget they want if they say their project is using “Blockchain”, or by entrepreneurs who think they are more likely to get the funding or press coverage they want if they add the word “Blockchain” to whatever they are doing.

So, where does a sovereign platform add value? As an example, an identity system may benefit from a sovereign platform. We would rather not keep all of our identity information (full name, social security #, date of birth, name of our parents, name of our spouses and kids, our address, passport information, payment information, etc.) on our phone which can be easily hacked, but we also do not want to give all that information to Google or Facebook or to our government. A sovereign system that no one can corrupt or control that will keep our information safe and will ask us every time someone wants a piece of our information may make sense. With this example we are simply trying to be creative and guess one possible use case, I am sure we will be surprised by creative and revolutionary entrepreneurs coming up with uses cases that take full advantage of a sovereign platform and that we cannot imagine right now.

But there is a use case that makes a lot of sense and, in fact, it is already working quite well. That is to use this sovereign platform to run a global system of value and settlement which is what Bitcoin, the currency, may become. Similar to what gold was for 2,000 years and similar to what the US dollar has been for the last 70 years. Bitcoin is potentially superior to gold and to the US dollar as a global non-political standard of value and settlement because there will never be more than 21 million bitcoins and because Bitcoin is open and uncensorable. There will never be more than 21 million bitcoins because it runs on a sovereign platform so no one can change or inflate that number. Additionally, Bitcoin is uncensorable because it runs on a sovereign platform so no one can change the transactions that already exist in the system and no one can keep the system from accepting new transactions. This allows for unprecedented economic freedom in the same way the internet allowed for unprecedented freedom of information. Gold has the advantage that it is tangible and many people (especially older ones, who tend to have more capital) strongly prefer something that they can touch. Gold also has in its favor that it has been around for over 2,000 years, and it may be impossible for Bitcoin to match that

history and reputation. The dollar has the advantage that it is already easily understood and accepted globally and it is a platform with remarkable network effects. These qualities may be too much for Bitcoin to overcome. Or it may be that we collectively come to appreciate the advantages of a digital unit that cannot be inflated or censored. Only time will tell.

Bitcoin is not an asset. It does not produce earnings or dividends and it does not generate interest. And Bitcoin has no intrinsic value. Bitcoin is simply money and most forms of good money have no intrinsic value. Gold, the US dollar and national currencies do not have any intrinsic value either but because they have had a monetary value for a long time most people perceive them as being intrinsically valuable, which is a big advantage. The main hurdle Bitcoin has to clear to become successful is to develop a similar widespread social perception of value and achieving that is quite an ambitious goal.

What does a world in which Bitcoin succeeded look like?

If Bitcoin succeeds it will most likely not replace any national currency. It may be a supranational currency that exists on top of all national currencies. If Bitcoin succeeds it may be a global non-political standard of value and settlement.

The world already has a global non-political standard of measure in the meter, and a global non-political standard of weight in the kilo. Could you imagine a world in which we changed the length of the meter or the weight of the kilo regularly according to political considerations? Yet that is what we are doing with our standard of value. Today we use the US dollar as a global standard of value which is much better than nothing but quite imperfect: it has lost significant value since inception, it is hard to know how many dollars will be outstanding in the future and, increasingly, the ability or inability to use it as a platform depends on political considerations. The world would be much better off with a global non-political standard of value.

The same is true for a global non-political standard of settlement. Only banks can participate in most settlement networks (like SWIFT, Fedwire, ACH in the US, CHAPS in the UK, SEPA in Europe, Visa and Mastercard, etc). Individuals, corporations and governments can only access these settlement networks through banks. Using these settlement networks takes time

(sometimes days), the process is opaque and costly and, increasingly, the ability to use them is determined by political considerations. Imagine an open platform where any individual, corporation or government could settle with any other individual, corporation or government anywhere in the world, in real time and for free, 24/7 and 365 days of the year. This would do for money what the Internet did for information.

In a world in which Bitcoin succeeds all currencies may be quoted in satoshis (the smallest fraction of a Bitcoin). When your granddaughter asks what is the price of the New Zealand dollar she may receive an answer in satoshis: the New Zealand dollar is 72 satoshis today. And the price of the Turkish Lira? 21 satoshis today. The US dollar? 107 satoshis today. A barrel of oil? 5,600 satoshis today. Global GDP? 97,356,765 bitcoins. The GDP of Indonesia? 1,417,007 bitcoins. The reserves of the South African Reserve Bank? 53,230 bitcoins. You get the idea. Then all of these values would be easily comparable across time and across geographies.

When your granddaughter asks “Grandpa, how did you guys keep track of all these things when you did not have Bitcoin?” your answer will be “We used the US dollar”. Then she may ask

“Really? But isn’t that the currency of the United States?” after you say yes she may ask “And how did you keep track of the US dollar?” to which you will say “Well… mostly in Euros, sometimes in Yen, Swiss Francs or other currencies depending on what we were talking about”. She may think we were weird.

Why not another cryptocurrency instead of Bitcoin?

There are about 1,000 cryptocurrencies that have at least one transaction a day. So why Bitcoin and not any one of those other ones? Over 60 million people own Bitcoin and over 1 million people become new owners every month. The other 1,000 cryptocurrencies have less than 5 million owners combined, so Bitcoin will add more users in the next 5 months than those 1,000 cryptocurrencies added in their combined history. Bitcoin is moving over $1 billion a day which is also more than all the other cryptocurrencies combined.

The most important metric of all, though, is how much can we trust these platforms or how sovereign they are. The measure of how sovereign these platforms are is the square of the computing power they have. If we use electricity consumption as a proxy of the computing power each of these platforms have, all of those 1,000 cryptocurrencies combined have less than 1% of the Bitcoin Blockchain processing (mining) power so none of them is (yet) really sovereign and in many cases their code is controlled by a person or a small group of people. New technologies may achieve sovereignty without relying on processing power and that may seriously challenge the Bitcoin Blockchain. But if those technologies do not get developed or it takes too long it may be difficult to unseat the Bitcoin Blockchain.

The Bitcoin Blockchain is a open protocol, not a company. The history of protocols is very different than the history of companies. In the history of companies there is a lot of change, disruption and churn (Microsoft-Apple, eBay-Amazon, Altavista-Google, MySpace-Facebook, etc.). However, the history of protocols is very different. Once a protocol gets established it almost never changes. For example, we are using IP

(Internet Protocol, or just “the Internet” colloquially) for almost all transport of data (until the late 90s cisco routers used to route dozens of protocols, today they only route IP). We are using only one web protocol and only one email protocol. The email protocol, for example, is quite lousy. At the protocol level there is no way for me to know if you received my email, much less if you read it, there is no way for you to verify my identity when you receive my email, there is no way to handle spam and many, many other things that could be fixed at the protocol level. I am sure some people have already developed much better email protocols, but we never heard about them and most likely we never will: once a protocol gets established it becomes the only protocol for that use case and it is not possible to displace it with a better protocol. Right now it looks like the standard protocol for a sovereign platform will be the Bitcoin Blockchain.

Many interesting technologies and applications that are being tested with other cryptocurrencies and other Blockchains and, if they are successful, they may be implemented on top of the Bitcoin Blockchain. It is not efficient to invest massive amounts of new hardware and electricity to replicate sovereignty when we already have a most solid and robust sovereign Bitcoin Blockchain. It is more efficient to simply build on top of it. For example, the Bitcoin Blockchain is limited in that it can only process approximately 3,000 transactions every 10 minutes, you have to wait 10 minutes for the transaction to be recorded in the Blockchain and up to 1 hour if you want to make sure it is irreversible. And you have to pay anywhere from 5 cents to 50 cents in transaction fees for the miners to process your transaction. The Lightning Network takes advantage of the robustness of the Bitcoin Blockchain and it works as a “Layer 2” solution on top of the Bitcoin Blockchain, enabling thousands of transactions per second of as little as 1 satoshi ($0.00004), for free and in real time. Similarly, other early examples of Layer 2 solutions that work on top of the Bitcoin Blockchain are RSK which enables the full functionality of Ethereum but on top of the much more robust Bitcoin Blockchain. Liquid is an open source wholesale settlement network developed by Blockstream that operates on top of the Bitcoin Blockchain. There are many more examples of technologies being developed to take advantage of the sovereignty and robustness of the Bitcoin Blockchain and enhance its capabilities by building on top of it.

How can Bitcoin fail?

Bitcoin can fail in many different ways. It could be taken over by a bad actor. It could be displaced by a better platform. It could be hacked. And Bitcoin can probably fail in many ways that we cannot imagine yet. Because Bitcoin does not have any intrinsic value, and because it’s value depends on a social consensus which is a sort of collective delusion, in my opinion, the most likely way in which Bitcoin could fail is a price panic. If we all decide at the same time that we think Bitcoin is worthless, then

it will be worthless. It is a self-fulfilled prophecy. If the price of Bitcoin were to plummet to zero or near zero, even if the platform remained intact, its reputation would suffer immensely and it could take a generation to rebuild that credibility. This could happen if people buy amounts of Bitcoin they cannot afford to lose, for example if people invest their retirement funds or their kids' college funds into Bitcoin, and as the price goes does down they are forced to sell, pushing the price further down and forcing others to sell. So, in my opinion, the biggest risk to Bitcoin is people investing amounts they cannot afford to lose.

Most of the capital invested in Bitcoin today seems to be capital that people can afford to lose. That is not because people are wise, or because the regulators have been very effective or that the industry has been prudent. The only reason why most people today do not have an amount of Bitcoin they cannot afford to lose is because of Bitcoin's price volatility. Ironically Bitcoin's price volatility is the best insurance against Bitcoin's biggest risk. If Bitcoin ever begins to be perceived as a safe asset before it has matured and people begin to allocate capital they cannot afford to lose we should be concerned. This happens to some degree during every Bitcoin price rally but, fortunately, so far each rally has corrected without destroying Bitcoin, but one day that could not be the case.

After 10 years of Bitcoin working well without interruption more concerning than a complete failure is a scenario where Bitcoin does not fail but it becomes irrelevant. Something similar to what happened to the BitTorrent protocol, which still exists but is less and less relevant as the real revolution in digital file sharing and entertainment happened through Dropbox, Spotify, Netflix, and many others. Similarly, there is a chance that Bitcoin does not fail but that it never becomes mainstream, that is only used by a group of believers and fanatics but not much more beyond that. That could happen because financial institutions, governments, and regulators manage to keep Bitcoin separate and ostracized from the rest of the financial world, like a non-convertible currency, but it could also happen even if financial institutions, governments, and regulators keep going on their current path of enabling Bitcoin to be fully connected to the financial world. If Bitcoin never becomes mainstream bitcoins will still have a price but most likely lower than what it is today. In my (subjective) opinion the chance of this happening is 30%.

Bitcoin's price action

Bitcoin launched in January 2009 but it did not have a price until July 2010 when it began to to change hands informally at $0.05 cents per bitcoin. In November 2010 Bitcoin had its first price rally that took the price to a peak of $0.39 cents to then "crash" to $0.19 cents. The price was at its peak of $0.39 cents only very briefly and the volume on prices near $0.39 cents was negligible, for most casual observers the rally simply took the price of Bitcoin from $0.05 cents to $0.19 cents, an increase of

280%, but most of the commentary at the time focused on the Bitcoin "crash" of over 50% from $0.39 to $0.19 cents. This exact same story has repeated itself 6 times in Bitcoin's history so far. There have been 6 of these rallies in Bitcoin's 10-year history and in between the rallies the price of Bitcoin has traded sideways or downward for months or years at a time. During most of Bitcoin's 10-year history, the press has been commenting and worrying about Bitcoin's latest "crash". How can something that constantly crashes go from

$0.05 cents to $4,000 you ask? If you want something to go from $0.05 cents to $4,000 and fool everybody into believing that it is failing, do it with as much volatility as possible.

The second Bitcoin price rally happened in February 2011 and it took the price of Bitcoin over $1.00 for the first time to then "crash" to $0.68 cents. The third rally happened in August 2011 and it took the price of Bitcoin to $29 to then "crash" to $2. The fourth rally happened in April 2013 and it took the price to $230 to then "crash" to $66. The fifth rally happened in December 2013 and it took the price to $1,147 to then "crash" to $177. The 6th (and currently last) rally happened in December 2017 and it took the price of Bitcoin to $19,783 to then "crash" below $3,200 (and until this bear market is over we don't know how low it may go).

The Bitcoin price rallies are the most important feature of how Bitcoin propagates, how people spread the word and how more people want to own it. It is a risky mechanism, so far it has worked well but it could lead to a disaster one day. The Bitcoin price rallies are Bitcoin's best moments but they are also it most dangerous and vulnerable moments.

Every Bitcoin bear market is about working out the excesses of the rally. During the rally too many people buy too many bitcoins thinking that they will be able to sell them for a big gain very soon and that usually does not happen. Imagine a fruit tree that has some good fruit and some rotten fruit. The Bitcoin bear markets resembles a period in which the tree is shaken until all the rotten fruit has fallen to the ground. Every time the tree is shaken some rotten fruit falls to the ground. The Bitcoin tree is shaken by the price going down and by letting time pass by. The more the price goes down and the more time passes without another rally the more people give up their original expectations, they sell, they adjust their exposure and their expectations. Eventually, no matter how much you shake the tree there is no more fruit to fall to the ground and the market may be getting ready for another rally.

If Bitcoin succeeds it is likely that the price will do another 6 of these rallies over the next 7 to 10 years. Anyone who tells you that they know what the price of Bitcoin will be next week, much less next year is either ignorant or outright lying to you. It is not possible to know when the price will hit bottom or when the next rally will come and

the penalty for trying to time the bottom or the top and getting it wrong can be much higher than the money you were trying to save. If you decide to buy Bitcoin simply decide what is the amount of money you can afford to lose (ideally less than 1% of your net worth), deploy it at market and at once and forget about it for 7 to 10 years. I have been giving this advice for 6 years and, by watching what people do with this advice, I can tell you that "Forget about it for 7 to 10 years" is the most difficult part of the simple recipe I am proposing. This lack of discipline destroys a lot more value than you would anticipate. The price volatility rattles people and makes them trade. If the price goes down a lot they want to buy more to reduce their average their cost, they buy more and now they have more than they can afford to lose so they care even more about the price volatility. Even worse: when the price goes up 10 times they decide to sell to rebalance because now Bitcoin represents too much of their net worth and it is too risky (it is hard to double your portfolio with a 1% exposure if you rebalance it every time it multiplies by 10). If you think this may happen to you, I suggest you invest in two buckets: keep one bucket that you will not trade for 7 to 10 years, and another bucket that you will trade as much as you want (but be responsible and be sure that both buckets combined add to an amount then you can afford to lose).

Why do I believe 1 Bitcoin may be worth $1 million in 7 to 10 years?

How much a Bitcoin may be worth if Bitcoin succeeds is pure speculation. Today Bitcoin is worth a total of ~ $70 billion (~ 17.5 million bitcoins in circulation x ~ $4,000 per Bitcoin). If Bitcoin ever becomes the world's standard of value and settlement it may have to be worth more than gold and less than the world's narrow supply of money. All the gold that was ever been mined is worth ~ $7 trillion the world's narrow supply of money is ~ $40 trillion. If Bitcoin is ever worth as much as gold each Bitcoin would be worth ~ $300,000, and if Bitcoin is ever worth as much as the world's narrow supply of money it would be worth ~ $2 million.

My preferred way of guessing how the price of Bitcoin may evolve is much more prosaic. I have noticed over time that the price of Bitcoin fluctuates around ~ $7,000 x how many people own bitcoins. So if that constant maintains and if 3 billion people ever own Bitcoin it would be worth ~ $21 trillion (~ $7,000 x 3 billion) or $1 million per Bitcoin.

In closing

This essay is focused on making the case for a small allocation to Bitcoin and, therefore, it focuses on the possible financial gain to be had if Bitcoin succeeds. But if Bitcoin does for Money what the Internet did for information the prospect of unprecedented economic freedom is much more exciting than any possible financial gain.

I grew up in Patagonia, Argentina, where my parents are sheep ranchers. Growing up I saw my family lose their entire savings three times: the first time because of an enormous devaluation, the second time because of hyperinflation and the last time because the government confiscated all bank deposits. It seemed like every time we were recovering, a new and different economic storm would wipe us out again. My memory of these events is not economic or financial but very emotional. I remember my parents fighting about money, I remember being scared, I remember everybody around us being scared and returning to desperate, almost animal like behavior. I also remember thinking how unfair it was that these crises hit the poor the hardest. People who had enough money to get some US dollars protected themselves that way, people who had even more money and could afford to buy a house or apartment protected themselves that way, and people who had even more money and could have a bank account abroad protected themselves that way. But the poor could not do any of those things and got hit the hardest. When I saw the emergence of the Internet I was young and idealistic and I sincerely thought the Internet was going to democratize money and fix money forever. But it has been 30 years since the Internet was created and it has fixed many problems but increasing economic freedom is not one of them. I was about to give up hope for the Internet to fix this problem when I ran into Bitcoin by accident. At first I was very cynical but the more I learned about it the more curious I became, after six months of studying and using Bitcoin I decided to dedicate the rest of my career, my capital and my reputation to help Bitcoin succeed. Nothing would make me prouder than to be able to tell my grandkids that I was part one of a very large community who helped Bitcoin succeed. And that because Bitcoin succeeded now billions of people can safely send, receive and store any form of money they want as easily as they can send or store a picture. So that what I saw happen to my parents and countless others can never happen again. Wences Casares is the CEO of Xapo, a Bitcoin wallet that helps individuals and institutions buy, sell and store Bitcoin. If you want to learn more about Bitcoin or if you are interested in buying Bitcoin do not hesitate to reach out to him at wences@xapo.com

Further reading:

➔ "Shelling Out: The Origins of Money" by Nick Szabo. Essential background on the nature of money.

➔ "An (Institutional) Investor's Take on Cryptoassets" by John Pfeffer. Bitcoin analysis from an investor's perspective

➔ "The Bitcoin Standard" by Saifedean Ammous. Non technical explanation of Bitcoin and what it may become.

➔ "Mastering Bitcoin" by Andreas Antonopoulos. Technical explanation of Bitcoin for non-technical people.

➔ "Programming Bitcoin" book by Jimmy Song. Technical explanation of Bitcoin for technical people and programming guide.

Crypto - Time to Take it at the Flood

By Rayne Steinberg

Posted April 4, 2019

The recent collapse in crypto assets from their high in December of 2017 has caused many to question the viability of crypto and blockchain, generally, and Bitcoin specifically. The overall market cap of the crypto ecosystem peaked at around $800 billion in January of 2018 and recently set a low of $100 billion in December of 2018. This is an 87% decline from peak, and a catastrophic result for any asset class. But what should investors make of it? And how should one approach it from here?

Source

First, we have to contextualize the performance of crypto as an asset class. For these discussions, I will use Bitcoin as a proxy for the broader crypto market as it has the only meaningful return set.

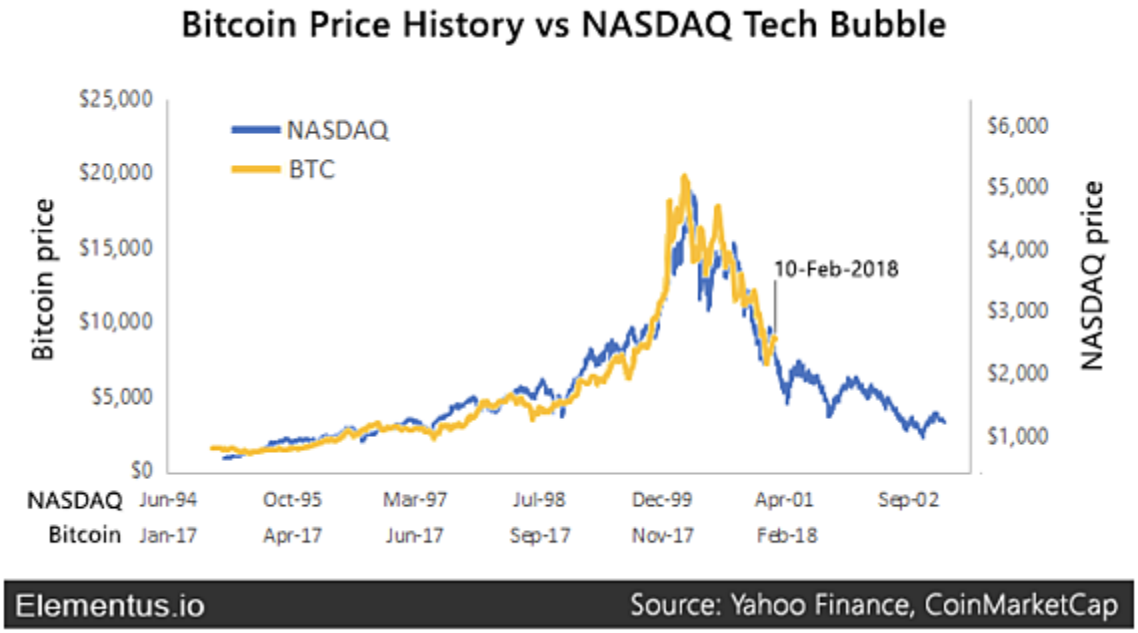
Bitcoin - What Is It?

Let's look at the Bitcoin boom-bust cycle through the lens of previous historical experiences. In order to do that, we have to determine what crypto/blockchain/bitcoin is. Bitcoin has attributes that overlap many areas. It has some qualities that are akin to a financial instrument, and others that compete more with currencies. Also, it is a new and disruptive technology. Also, it is an idea that advances decentralization and is a potential remedy for a financial system that is losing trust.

Bitcoin - The Asset Bubble

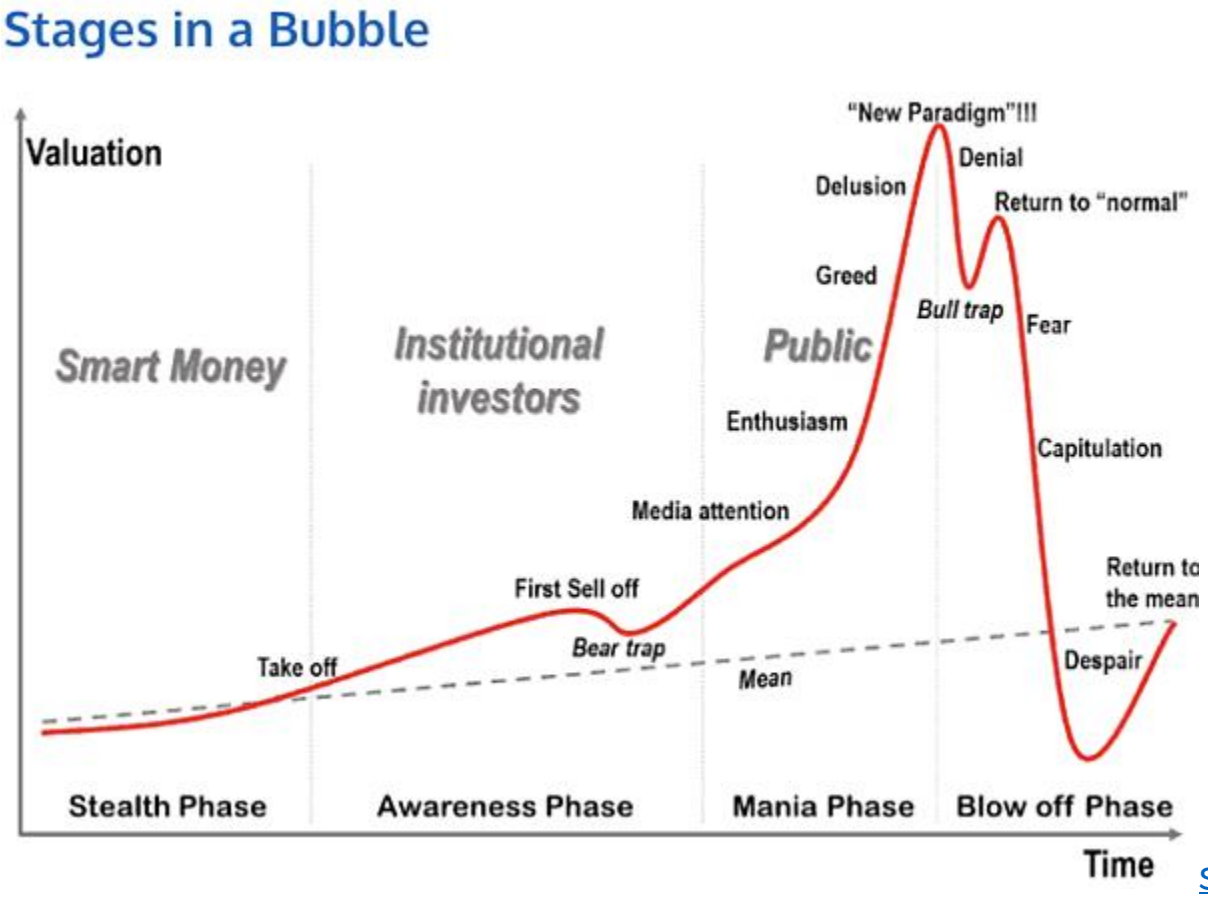
When we look at Bitcoin as an asset class, we can view the recent run-up and subsequent collapse in prices like any other financial bubble. Many have compared it

to the technology stock bubble of the late 1990s. And the trends look remarkably similar:



Source

This is interesting but does not really tell us that much. There is a broad pattern that bubbles follow:

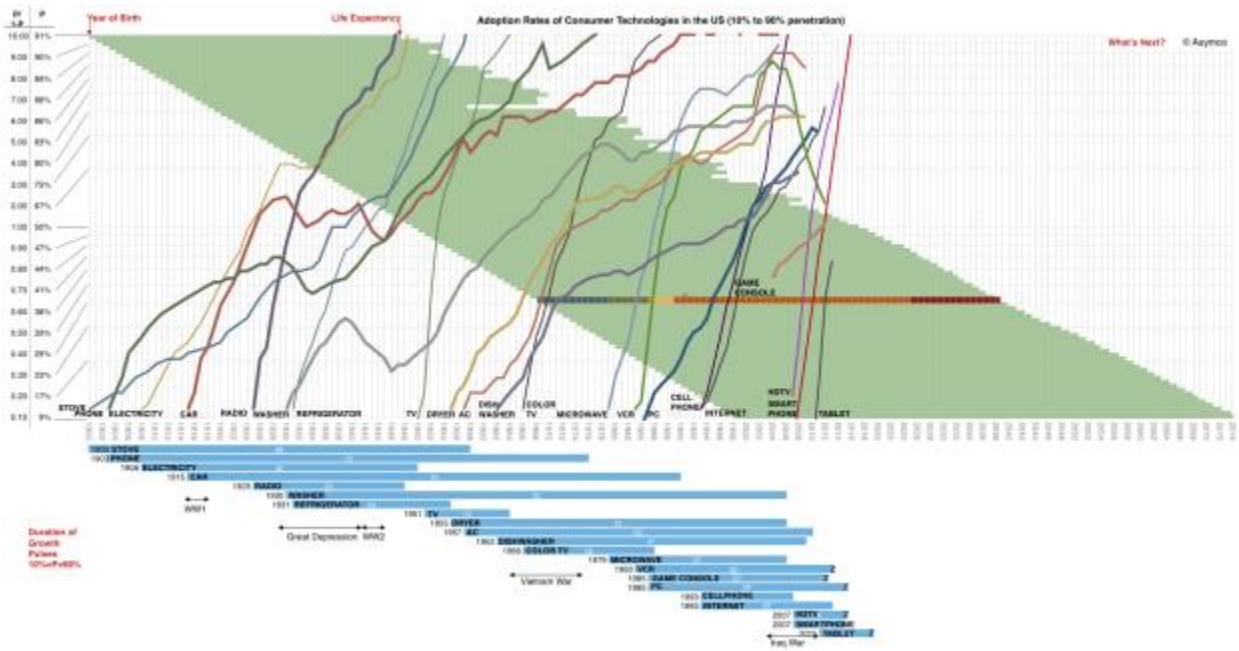


Source

There have been many financial bubbles throughout history that have followed this pattern. If the recent volatility in Bitcoin was just a run of the mill asset bubble, we could dismiss it and move on. Bitcoin would have just now entered the end of the Blow Off Phase. But Bitcoin is more than just an asset class; it is a new and disruptive technology.

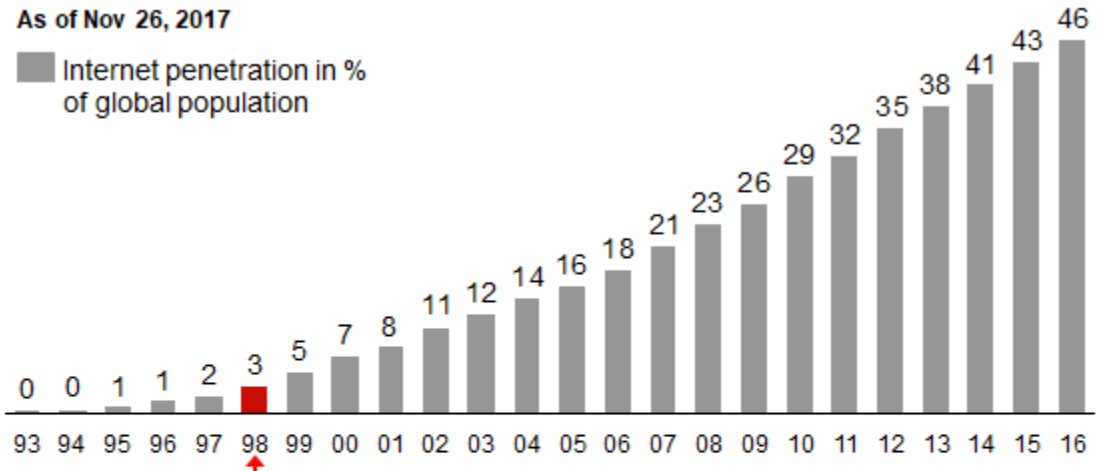
Bitcoin - The Disruptor

When we treat Bitcoin as a disruptive technology, there are many corollaries for us to consider. Asymco outlines the adoption cycle of all major innovations in the US from 1900 on:



Source

If blockchain is a revolutionary technology, it is important to know where it is in its life cycle. By most accounts, it is still, incredibly early innings. This comparison contextualizes it in relation to the internet and its rate of penetration:

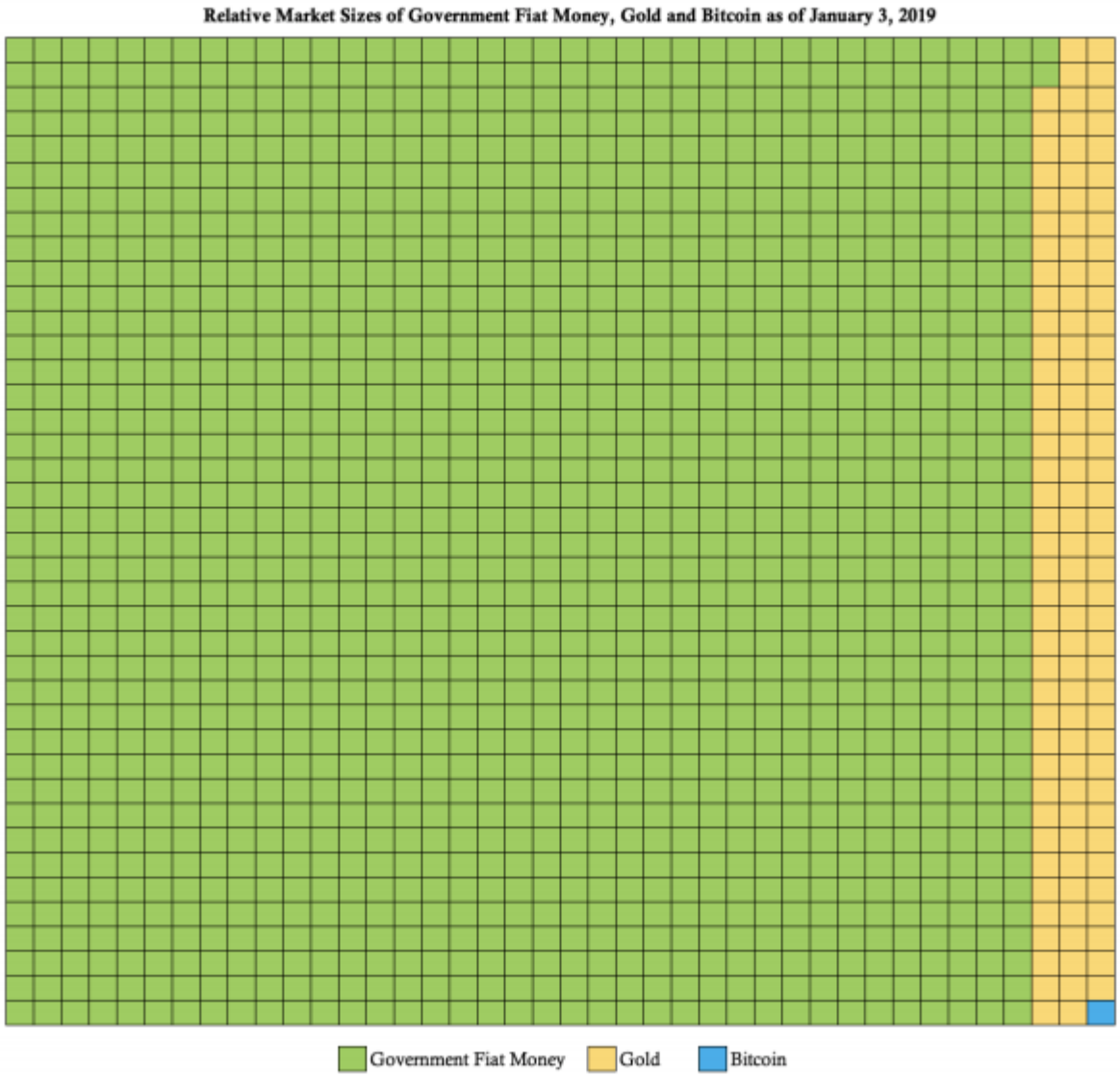


Number of Coinbase Accounts	13.3m
Coinbase as % of bitcoin trade	5%
Implied # of total crypto exchange accounts	266m
Assumed # of accounts / household	4
Total number of unique crypto Households	**66.5m**
As % of total world wide households	**3.5%**

Sources:
- internetlivestats.com
- Coinbase data (@alistairmilne on Twitter)
- Wikipedia Household information

Source

One can argue it is even earlier, as the above analysis is estimating user adoption where it mainly takes into account retail adoption. As Bitcoin is potentially a replacement for currency one could argue that the total market for Bitcoin is that of government fiat + gold. When looked at this way, Bitcoin is only 0.07% of that addressable market:



Source

By any of these measures, Bitcoin is at the beginning of its adoption cycle, not the end. In addition to the technology, what is even more fundamental, is the animating idea behind it.

Bitcoin - The Idea

The idea of Bitcoin is more basic than its asset class and technology-like attributes. Robert Breedlove says Its "a momentous Innovation of the digital age. As such, it has

many unique characteristics, properties and capabilities never before seen in a monetary technology:"

- Immutable Monetary Policy
- Digital Scarcity
- Absolute Scarcity
- Global Final Settlement System
- Self-Sovereign Network
- Stateless Money
- Revolutionary Social Contract Implementation
- Global Consensus
- Global Energy Buyer of Last Resort
- A New Form of Life
- Adaptive Security
- Adaptive Functionality
- Programmability

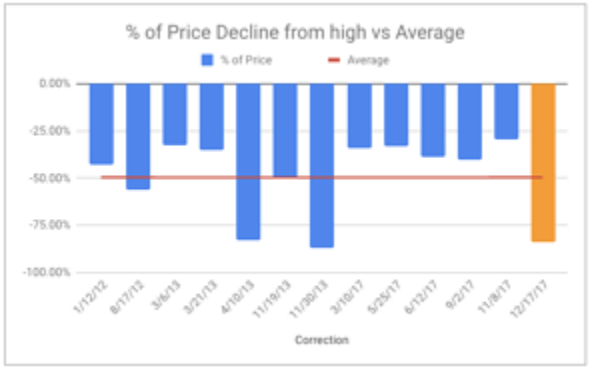
The revolutionary and society-changing nature of this idea is what makes it incredibly powerful and disruptive. This is the first technology that has the ability to halt, and perhaps reverse, our relentless drive towards centralization while still affording us of its benefits. And as an idea, it came into existence in response to the overreach of banks and governments during the financial crisis. The same policies that spawned it are being continued and amplified today. The idea of Bitcoin is much more similar to a sea-change in societal thinking, like the spread of a major religion or the reaction to one. And when thought of like that, it is incredibly early and it will take a long time for that idea to work its way around the globe.

What Do You Do?

If the above is true, what does that mean in regards to the current price level of Bitcoin? Should we be buying or selling? Even if we agree with the thesis that this is a transformative technology and we are at the earliest stages, no one wants to suffer through more downside volatility than they have to. Let us contextualize this bear market as it relates to other Bitcoin downdrafts. I used Solomon Stavis piece From Bear to Bull, a Look into the Cycle of Bitcoin Prices as a place to start. From January of 2012, there have been 13 corrections of more than 30% in Bitcoin (including our current correction):

Bitcoin Price Corrections - January 2012 to April 2019 (30% or more correction)										
Correction Start Date	Correction End Date	# of Days in Correction	Price Recovery End Date	Bear Market # of Days in Recovery	Bitcoin High Price	% Change of Previous High	Bitcoin Low Price	% Change of Previos Low	% of Price Decline	$ Difference in Price Decline
1/12/12	1/27/12	15	7/12/12	182	$7		$4		-43%	-$3
8/17/12	8/19/12	2	1/21/13	157	$16	129%	$7	75%	-56%	-$9
3/6/13	3/7/13	1	3/18/13	12	$49	206%	$33	371%	-33%	-$16
3/21/13	3/23/13	2	3/25/13	4	$77	57%	$50	52%	-35%	-$27
4/10/13	4/12/13	2	11/6/13	210	$259	236%	$45	-10%	-83%	-$214
11/19/13	11/19/13	0	11/22/13	3	$755	192%	$378	740%	-50%	-$377
11/30/13	1/14/15	410	2/23/17	1181	$1,163	54%	$152	-60%	-87%	-$1,011
3/10/17	3/25/17	15	4/30/17	51	$1,350	16%	$891	486%	-34%	-$459
5/25/17	5/27/17	2	6/6/17	12	$2,760	104%	$1,850	108%	-33%	-$910
6/12/17	7/16/17	34	8/5/17	54	$2,980	8%	$1,830	-1%	-39%	-$1,150
9/2/17	9/15/17	13	10/12/17	40	$4,980	67%	$2,972	62%	-40%	-$2,008
11/8/17	11/12/17	4	11/16/17	8	$7,888	58%	$5,556	87%	-30%	-$2,332
12/17/17	**12/15/2018**	**363**	**4/4/2019**	**473**	**$19,666**	**149%**	**$3,233**	**-42%**	**-84%**	**-$16,433**
Average		**66**		**184**		**106%**		**156%**	**-50%**	
Median		**4**		**51**		**86%**		**69%**	**-40%**	
Max		**410**		**1181**		**236%**		**740%**	**-30%**	
Min		**0**		**3**		**8%**		**-60%**	**-87%**	

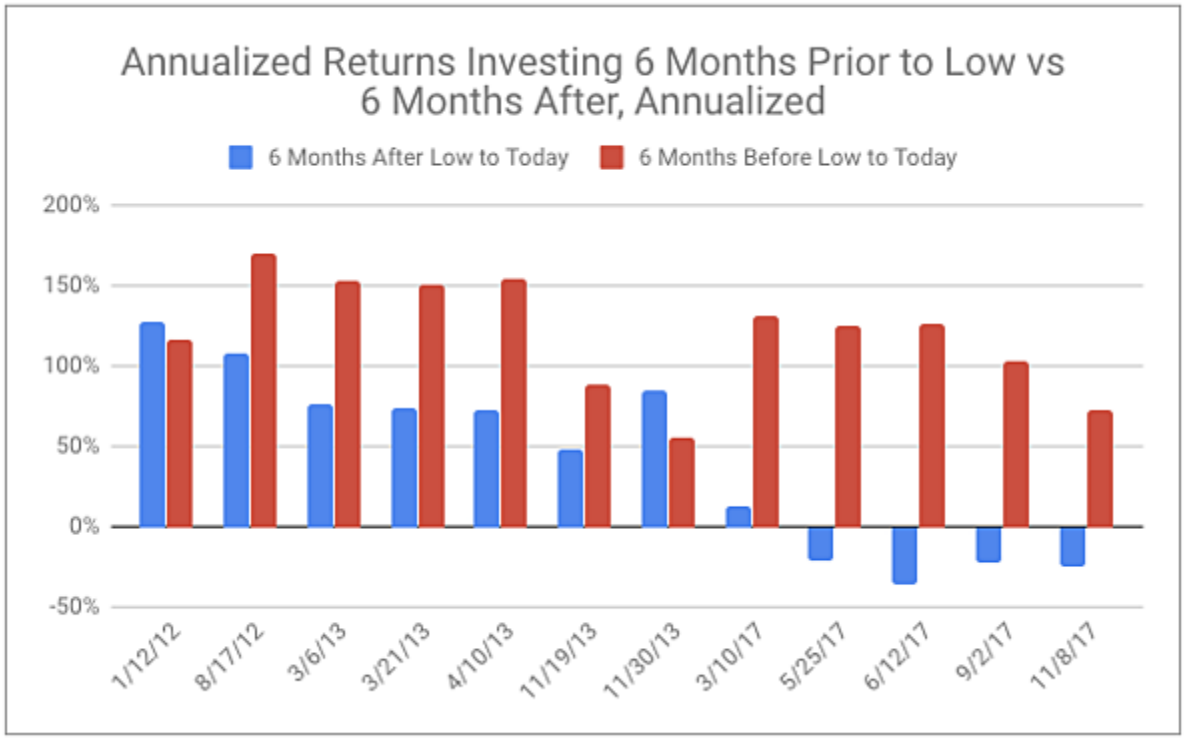
If we did put a bottom in on 12/15/2018 at $3,233, then this correction would have lasted 363 days with a max drawdown of 84%. This compares to an average length of 66 days for bear markets and an average 50% decline.



Source: Yahoo Finance, data as of 4/2/2019

In both duration and severity, this correction is near the previous extremes.

And what we are trying to determine is if this really is the bottom, or do we have more to drop? A better question is, is it better to be early or late. And by that I mean, if you feel you are near a bottom, would you prefer to invest before it bottomed or after? To add some color around this, I examined if you had invested 6 months before each of the previous lows, or if you waited until six months after.



Source: Yahoo Finance, data as of 4/2/2019

The average annualized return for the after low set is 41%, an unimaginable return in any other asset class. The average annual return for the before the low investment is, however, an eye-popping 120%. When you look at the growth of a dollar invested at these respective rates, over 5 years, late grows to $4, and early grows to $38.

Source: Yahoo Finance, data as of 4/2/2019

In this case, the early bird really does get the worm.

While this analysis is rudimentary, and the time series is short, the data does suggest its better to be early than late. As of 4/2/2019, Bitcoin is up 54% from the low on 12/15/18. If you believe the overall thesis for Bitcoin specifically and the crypto and blockchain space generally, you may not get another opportunity to enter at such an opportune time.

If Shakespeare's Brutus were transported to a pension's investment committee meeting where they are considering making an allocation to crypto, his famous words of action might be the best advice they could get:

There is a tide in the affairs of men, Which taken at the flood, leads on to fortune. Omitted, all the voyage of their life is bound in shallows and in miseries. On such a full sea are we now afloat. And we must take the current when it serves, or lose our ventures.

Technological Teachings of Bitcoin

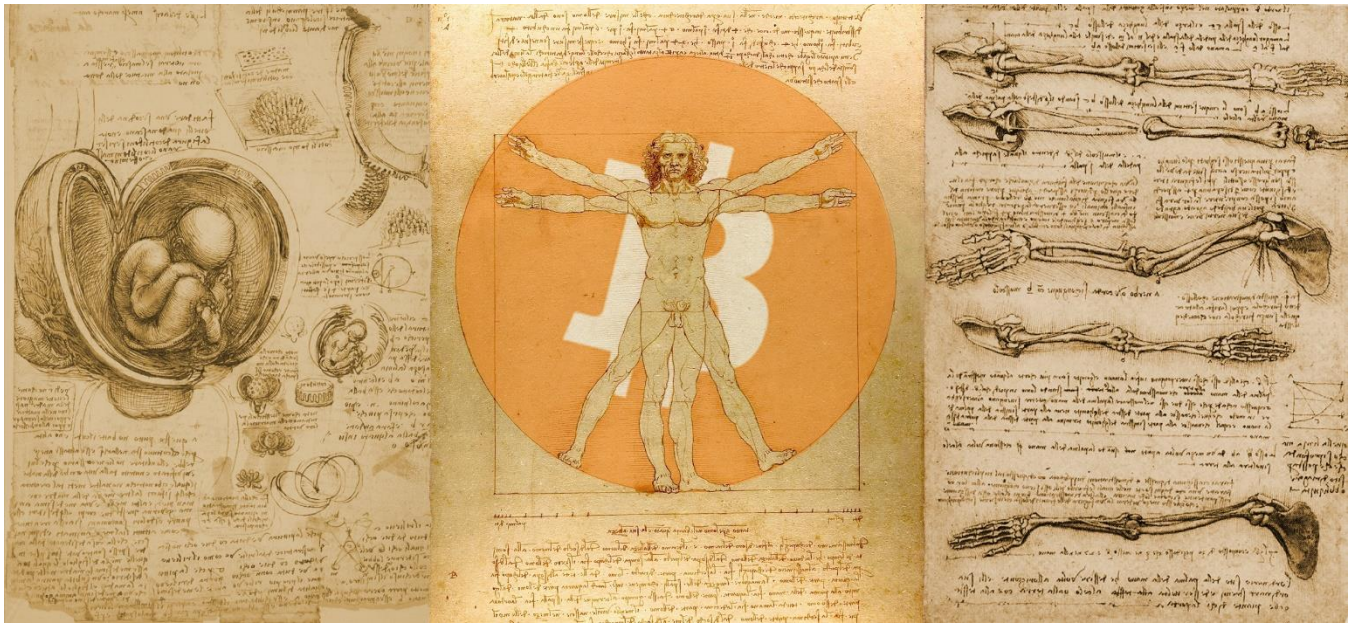
What I've Learned From Bitcoin: Part III

By Gigi

Posted April 2, 2019

This is part 3 of a 3 part series

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



What is Bitcoin? The many answers to this question are as interesting as they are varied. Bitcoin is both a social and a monetary phenomenon, but it is also a technological one. The intersection of many disciplines is what makes Bitcoin endlessly fascinating. Like many others, I began to stumble down this strange rabbit hole a while ago. Even though this article is the last of this series, I am still stumbling down with no end in sight, and I invite you to stumble along with me.

This is the third chapter of a personal journey. Again, I am indebted to Arjun Balaji who asked the following on Twitter: "What have you learned from Bitcoin?" It is this question which has led me to write this series to outline some of the things I've learned.

- I: Philosophical Teachings of Bitcoin
- II: Economic Teachings of Bitcoin
- **III: Technological Teachings of Bitcoin**

Part one explored what I've learned from Bitcoin when seen through a philosophical lens: the interplay of immutability and change, copying and scarcity, Bitcoin's origin story and identity, locality in a world of replication, money as free speech, and the limits of knowledge.

Part two discussed some of the economic teachings of Bitcoin: the concept of value, (sound) money and its history, inflation, and some aspects of "modern" banking like fractional reserve banking.

Part three will explore seven things I have learned from examining Bitcoin through the lens of technology. As in the previous parts, I will only be able to scratch the surface. Bitcoin is an expanding universe, evolving and improving every day. Whole books can be and have been written on small, specific parts of this cosmos. And just like in our own universe, the expansion seems to be accelerating.

Find lessons 1–7 here and lessons 8–14 here.

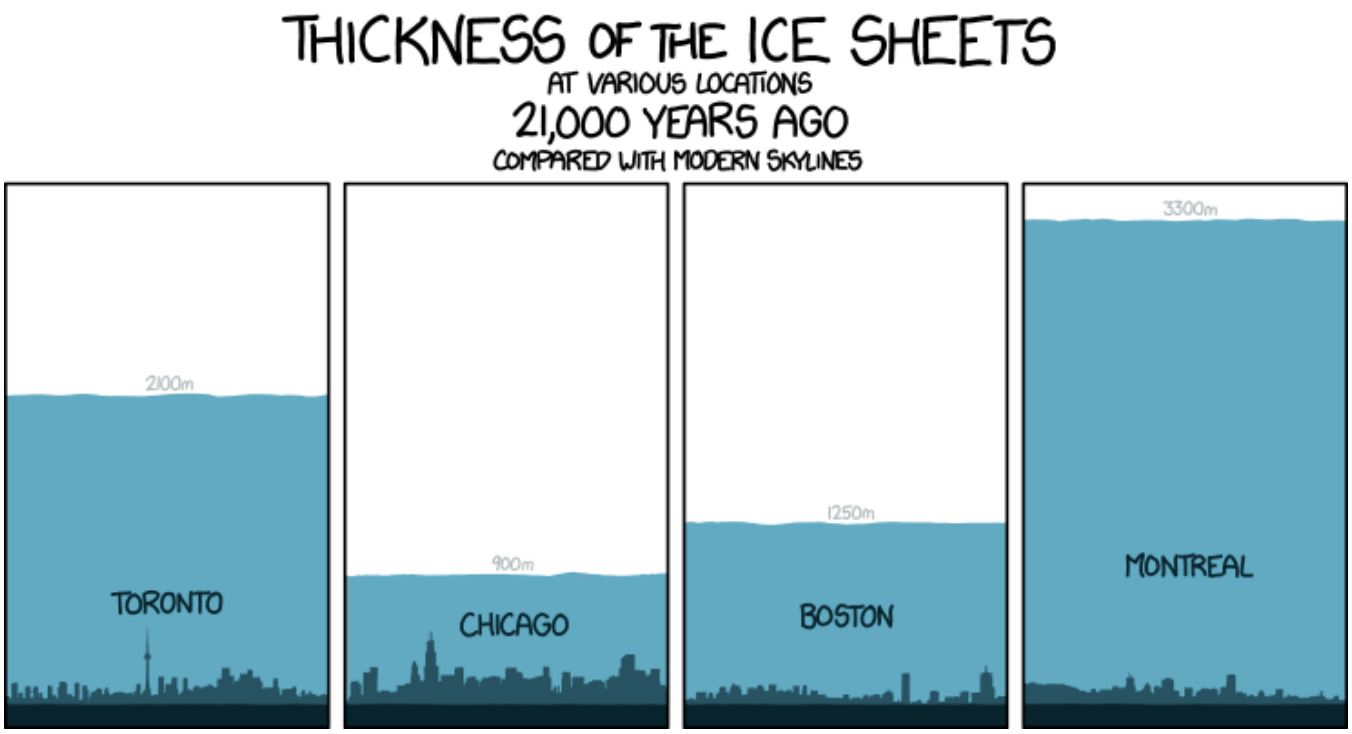
Lesson 15: Strength in numbers

Numbers are an essential part of our everyday life. Large numbers, however, aren't something most of us are too familiar with. The largest numbers we might encounter in everyday life are in the range of millions, billions, or trillions. We might read about millions of people in poverty, billions of dollars spent on bank bailouts, and trillions of national debt. Even though it's hard to make sense of these headlines, we are somewhat comfortable with the size of those numbers.

Although we might seem comfortable with billions and trillions, our intuition already starts to fail with numbers of this magnitude. Do you have an intuition how long you would have to wait for a million/billion/trillion seconds to pass? If you are anything like me, you are lost without actually crunching the numbers.

Let's take a closer look at this example: the difference between each is an increase by three orders of magnitude: 10^6, 10^9, 10^{12}. Thinking about seconds is not very useful, so let's translate this into something we can wrap our head around:

- 10^6: One million seconds was 1½ weeks ago.
- 10^9: One billion seconds was almost 32 years ago.
- 10^{12}: One trillion seconds ago Manhattan was covered under a thick layer of ice.



About 1 trillion seconds ago. Source: [xkcd #1125]

As soon as we enter the beyond-astronomical realm of modern cryptography, our intuition fails catastrophically. Bitcoin is built around large numbers and the virtual impossibility of guessing them. These numbers are way, way larger than anything we might encounter in day-to-day life. Many orders of magnitude larger. Understanding how large these numbers truly are is essential to understanding Bitcoin as a whole.

Let's take SHA-256, one of the hash functions used in Bitcoin, as a concrete example. It is only natural to think about 256 bits as "two hundred fifty-six," which isn't a large number at all. However, the number in SHA-256 is talking about orders of magnitude—something our brains are not well-equipped to deal with.

While bit length is a convenient metric, the true meaning of 256-bit security is lost in translation. Similar to the millions (10^6) and billions (10^9) above, the number in SHA-256 is about orders of magnitude (2^{256}).

So, how strong is SHA-256, exactly?

"SHA-256 is very strong. It's not like the incremental step from MD5 to SHA1. It can last several decades unless there's some massive breakthrough attack."

—Satoshi Nakamoto

Let's spell things out. 2^{256} equals the following number:

115 quattuorvigintillion 792 trevigintillion 89 duovigintillion 237 unvigintillion 316 vigintillion 195 novemdecillion 423 octodecillion 570 septendecillion 985 sexdecillion 8 quindecillion 687 quattuordecillion 907 tredecillion 853 duodecillion 269 undecillion 984 decillion 665 nonillion 640 octillion 564 septillion 39 sextillion 457 quintillion 584 quadrillion 7 trillion 913 billion 129 million 639 thousand 936.

That's a lot of nonillions! Wrapping your head around this number is pretty much impossible. There is nothing in the physical universe to compare it to. It is far larger than the number of atoms in the observable universe. The human brain simply isn't made to make sense of it.

One of the best visualizations of the true strength of SHA-256 is the following video by Grant Sanderson. Aptly named "How secure is 256 bit security?" it beautifully shows how large a 256-bit space is. Do yourself a favor and take the five minutes to watch it. As all other 3Blue1Brown videos it is not only fascinating but also exceptionally well made. Warning: You might fall down a math rabbit hole.

Answer: Pretty secure.

Bruce Schneier used the physical limits of computation to put this number into perspective: even if we could build an optimal computer, which would use any provided energy to flip bits perfectly, build a Dyson sphere around our sun, and let it run for 100 billion billion years, we would still only have a 25% chance to find a needle in a 256-bit haystack.

"These numbers have nothing to do with the technology of the devices; they are the maximums that thermodynamics will allow. And they strongly imply that brute-force attacks against 256-bit keys will be infeasible until computers are built from something other than matter and occupy something other than space."

—Bruce Schneier

It is hard to overstate the profoundness of this. Strong cryptography inverts the power-balance of the physical world we are so used to. Unbreakable things do not exist in the real world. Apply enough force, and you will be able to open any door, box, or treasure chest.

Bitcoin's treasure chest is very different. It is secured by strong cryptography, which does not give way to brute force. And as long as the underlying mathematical assumptions hold, brute force is all we have. Granted, there is also the option of a global $5 wrench attack. But torture won't work for all bitcoin addresses, and the cryptographic walls of bitcoin will defeat brute force attacks. Even if you come at it with the force of a thousand suns. Literally.

This fact and its implications were poignantly summarized in the call to cryptographic arms: " *No amount of coercive force will ever solve a math problem.*"

"It isn't obvious that the world had to work this way. But somehow the universe smiles on encryption."

—Julian Assange

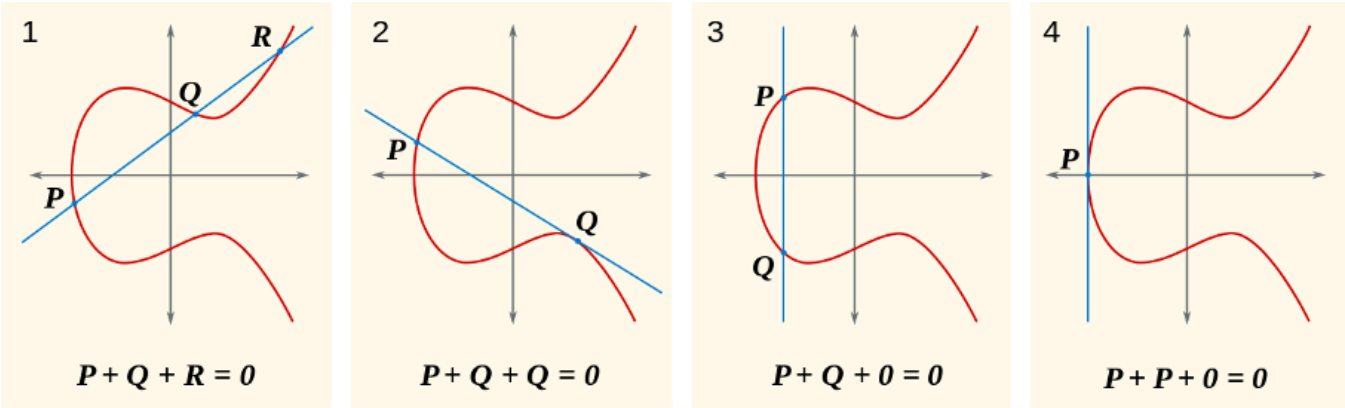
Nobody yet knows for sure if the universe's smile is genuine or not. It is possible that our assumption of mathematical asymmetries is wrong and we find that P actually equals NP, or we find surprisingly quick solutions to specific problems which we currently assume to be hard. If that should be the case, cryptography as we know it will cease to exist, and the implications would most likely change the world beyond recognition.

"Vires in Numeris" = "Strength in Numbers"

—epii

Vires in numeris is not only a catchy motto used by bitcoiners. The realization that there is an unfathomable strength to be found in numbers is a profound one. Understanding this, and the inversion of existing power balances which it enables changed my view of the world and the future which lies ahead of us.

One direct result of this is the fact that you don't have to ask anyone for permission to participate in Bitcoin. There is no page to sign up, no company in charge, no government agency to send application forms to. Simply generate a large number and you are pretty much good to go. The central authority of account creation is mathematics. And God only knows who is in charge of that.



Elliptic curve examples (cc-by-sa Emmanuel Boutet)

Bitcoin is built upon our best understanding of reality. While there are still many open problems in physics, computer science, and mathematics, we are pretty sure about some things. That there is an asymmetry between finding solutions and

validating the correctness of these solutions is one such thing. That computation needs energy is another one. In other words: finding a needle in a haystack is harder than checking if the pointy thing in your hand is indeed a needle or not. And finding the needle takes work.

The vastness of Bitcoin's address space is truly mind-boggling. The number of private keys even more so. It is fascinating how much of our modern world boils down to the improbability of finding a needle in an unfathomably large haystack. I am now more aware of this fact than ever.

Bitcoin taught me that there is strength in numbers.

Lesson 16: Reflections on "Don't Trust, Verify"

Bitcoin aims to replace, or at least provide an alternative to, conventional currency. Conventional currency is bound to a centralized authority, no matter if we are talking about legal tender like the US dollar or modern monopoly money like Fortnite's V-Bucks. In both examples, you are bound to trust the central authority to issue, manage and circulate your money. Bitcoin unties this bound, and the main issue Bitcoin solves is the issue of *trust*.

"The root problem with conventional currency is all the trust that's required to make it work. [...] What is needed is an electronic payment system based on cryptographic proof instead of trust" —Satoshi Nakamoto

Bitcoin solves the problem of trust by being completely decentralized, with no central server or trusted parties. Not even trusted *third* parties, but trusted parties, period. When there is no central authority, there simply *is* no-one to trust. Complete decentralization is the innovation. It is the root of Bitcoin's resilience, the reason why it is still alive. Decentralization is also why we have mining, nodes, hardware wallets, and yes, the blockchain. The only thing you have to "trust" is that our understanding of mathematics and physics isn't totally off and that the majority of miners act honestly (which they are incentivized to do).

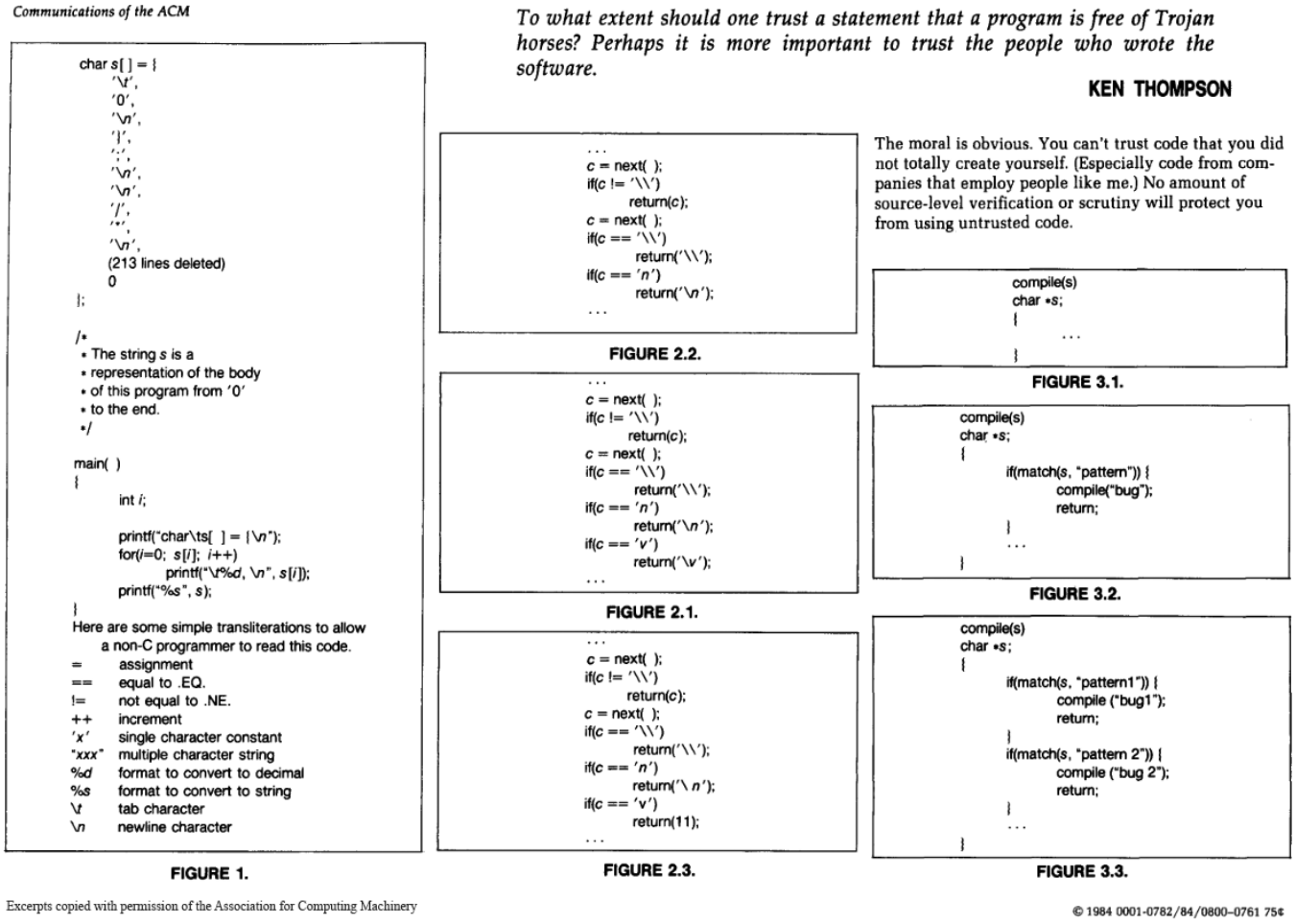
While the regular world operates under the assumption of *"trust, but verify,"* Bitcoin operates under the assumption of *"don't trust, verify."*_*Satoshi made the importance of removing trust very clear in both the introduction as well as the conclusion of the Bitcoin whitepaper*.

"Conclusion: We have proposed a system for electronic transactions without relying on trust." —Satoshi Nakamoto

Note that "without relying on trust" is used in a very specific context here. We are talking about trusted third parties, i.e. other entities which you trust to produce, hold,

and process your money. It is assumed, for example, that you can trust your computer.

As Ken Thompson showed in his Turing Award lecture, trust is an extremely tricky thing in the computational world. When running a program, you have to trust all kinds of software (and hardware) which, in theory, could alter the program you are trying to run in a malicious way. As Thompson summarized in his *Reflections on Trusting Trust*: "The moral is obvious. You can't trust code that you did not totally create yourself."



Communications of the ACM

```
char s[ ] = {
        '\t',
        '0',
        '\n',
        '}',
        ';',
        '\n',
        '\n',
        '/',
        '*',
        '\n',
        (213 lines deleted)
        0
};

/*
 * The string s is a
 * representation of the body
 * of this program from '0'
 * to the end.
 */

main( )
{
        int i;

        printf("char\ts[ ] = {\n");
        for(i=0; s[i]; i++)
                printf("\t%d, \n", s[i]);
        printf("%s", s);
}
```

Here are some simple transliterations to allow a non-C programmer to read this code.

=	assignment
==	equal to .EQ.
!=	not equal to .NE.
++	increment
'x'	single character constant
"xxx"	multiple character string
%d	format to convert to decimal
%s	format to convert to string
\t	tab character
\n	newline character

FIGURE 1.

To what extent should one trust a statement that a program is free of Trojan horses? Perhaps it is more important to trust the people who wrote the software.

KEN THOMPSON

```
...
c = next( );
if(c != '\\')
        return(c);
c = next( );
if(c == '\\')
        return('\\');
if(c == 'n')
        return('\n');
...
```

FIGURE 2.2.

```
...
c = next( );
if(c != '\\')
        return(c);
c = next( );
if(c == '\\')
        return('\\');
if(c == 'n')
        return('\n');
if(c == 'v')
        return('\v');
...
```

FIGURE 2.1.

```
...
c = next( );
if(c != '\\')
        return(c);
c = next( );
if(c == '\\')
        return('\\');
if(c == 'n')
        return('\ n');
if(c == 'v')
        return(11);
...
```

FIGURE 2.3.

The moral is obvious. You can't trust code that you did not totally create yourself. (Especially code from companies that employ people like me.) No amount of source-level verification or scrutiny will protect you from using untrusted code.

```
compile(s)
char *s;
{
        ...
}
```

FIGURE 3.1.

```
compile(s)
char *s;
{
        if(match(s, "pattern")) {
                compile("bug");
                return;
        }
        ...
}
```

FIGURE 3.2.

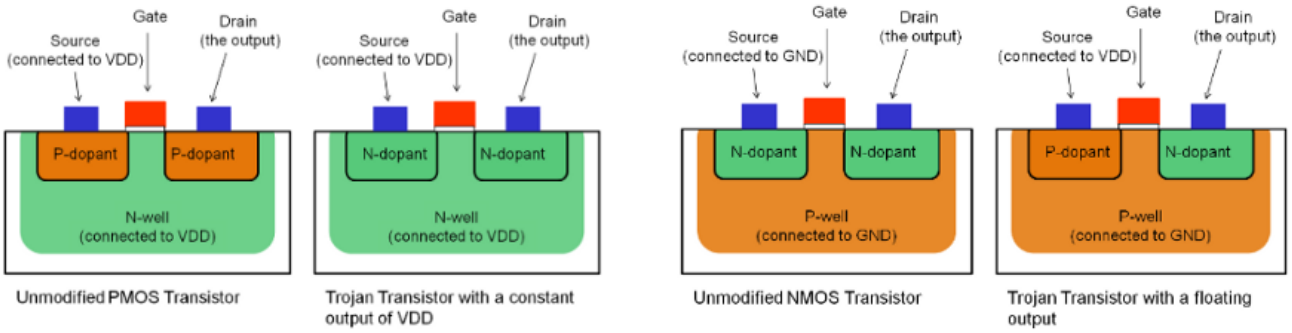
```
compile(s)
char *s;
{
        if(match(s, "pattern1")) {
                compile ("bug1");
                return;
        }
        if(match(s, "pattern 2")) {
                compile ("bug 2");
                return;
        }
        ...
}
```

FIGURE 3.3.

Thompson demonstrated that even if you have access to the source code, your compiler—or any other program-handling program or hardware—could be compromised and detecting this backdoor would be very difficult. Thus, in practice, a truly *trustless* system does not exist. You would have to create all your software *and* all your hardware (assemblers, compilers, linkers, etc.) from scratch, without the aid of any external software or software-aided machinery.

"If you wish to make an apple pie from scratch, you must first invent the universe." — Carl Sagan

The Ken Thompson Hack is a particularly ingenious and hard-to-detect backdoor, so let's take a quick look at a hard-to-detect backdoor which works without modifying any software. Researchers found a way to compromise security-critical hardware by altering the polarity of silicon impurities. Just by changing the physical properties of the stuff that computer chips are made of they were able to compromise a cryptographically secure random number generator. Since this change can't be seen, the backdoor can't be detected by optical inspection, which is one of the most important tamper-detection mechanism for chips like these.



(a) p-MOS Transistor (b) n-MOS Transistor

Stealthy Dopant-Level Hardware Trojans by Becker, Regazzoni, Paar, Burleson

Sounds scary? Well, even if you would be able to build everything from scratch, you would still have to trust the underlying mathematics. You would have to trust that secp256k1 is an elliptic curve without backdoors. Yes, malicious backdoors can be inserted in the mathematical foundations of cryptographic functions and arguably this has already happened at least once. There are good reasons to be paranoid, and the fact that everything from your hardware, to your software, to the elliptic curves used can have backdoors are some of them.

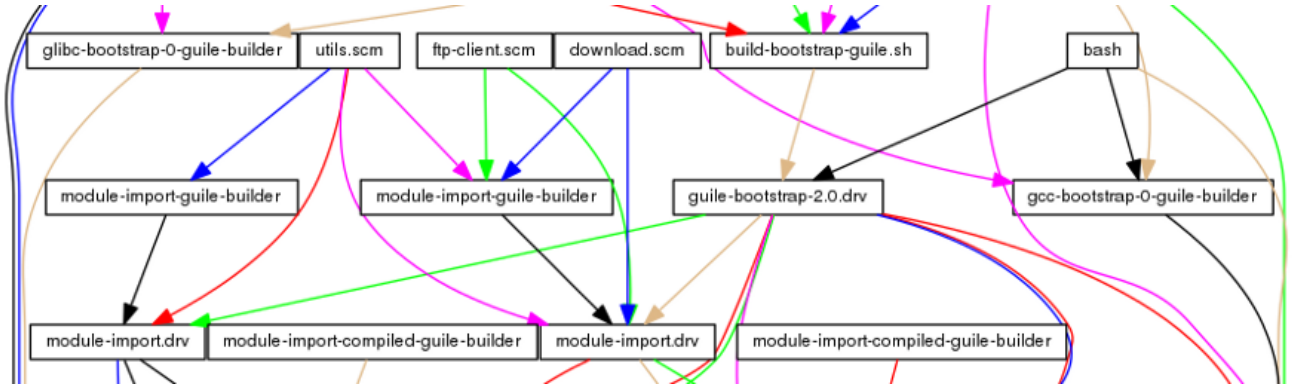
"Don't trust. Verify."

The above examples should illustrate that *trustless* computing is utopic. Bitcoin is probably the one system which comes closest to this utopia, but still, it is *trust-minimized*—aiming to remove trust wherever possible. Arguably, the chain-of-trust is neverending, since you will also have to trust that computation requires energy, that P does not equal NP, and that you are actually in base reality and not emprisoned in a simulation by malicious actors.

Developers are working on tools and procedures to minimize any remaining trust even further. For example, Bitcoin developers created Gitian, which is a software distribution method to create deterministic builds. The idea is that if multiple developers are able to reproduce identical binaries, the chance of malicious tampering is reduced. Fancy backdoors aren't the only attack vector. Simple

blackmail or extortion are real threats as well. As in the main protocol, decentralization is used to minimize trust.

Various efforts are being made to improve upon the chicken-and-egg problem of bootstrapping which Ken Thompson's hack so brilliantly pointed out. One such effort is Guix (pronounced *geeks*), which uses functionally declared package management leading to bit-for-bit reproducible builds by design. The result is that you don't have to trust any software-providing servers anymore since you can verify that the served binary was not tampered with by rebuilding it from scratch. As of this writing, a pull-request is in progress to integrate Guix into the Bitcoin build process.



Which came first, the chicken or the egg?

Luckily, Bitcoin doesn't rely on a single algorithm or piece of hardware. One effect of Bitcoin's radical decentralization is a distributed security model. Although the backdoors described above are not to be taken lightly, it is unlikely that every software wallet, every hardware wallet, every cryptographic library, every node implementation, and every compiler of every language is compromised. Possible, but highly unlikely.

Note that you can generate a private key without relying on any computational hardware or software. You can flip a coin a couple of times, although depending on your coin and tossing style this source of randomness might not be sufficiently random. There is a reason why storage protocols like Glacier advise to use casino-grade dice as one of two sources of entropy.

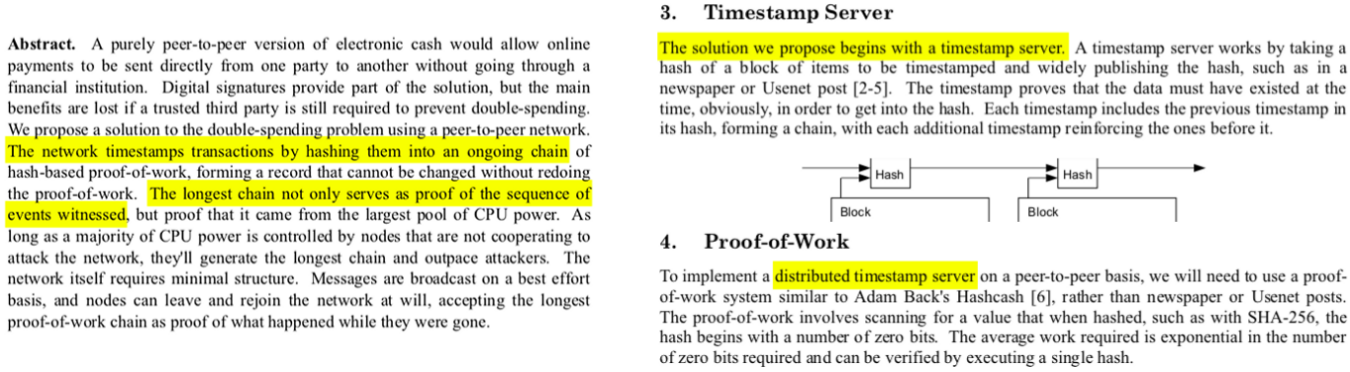
Bitcoin forced me to reflect on what trusting nobody actually entails. It raised my awareness of the bootstrapping problem, and the implicit chain-of-trust in developing and running software. It also raised my awareness of the many ways in which software and hardware can be compromised.

Bitcoin taught me not to trust, but to verify.

Lesson 17: Telling time takes work

It is often said that bitcoins are mined because thousands of computers work on solving *very complex* mathematical problems. Certain problems are to be solved, and if you compute the right answer, you "produce" a bitcoin. While this simplified view of bitcoin mining might be easier to convey, it does miss the point somewhat. Bitcoins aren't produced or created, and the whole ordeal is not really about solving particular math problems. Also, the math isn't particularly complex. What is complex is *telling the time* in a decentralized system.

As outlined in the whitepaper, the proof-of-work system (aka mining) is a way to implement a distributed timestamp server.



Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

3. Timestamp Server

The solution we propose begins with a timestamp server. A timestamp server works by taking a hash of a block of items to be timestamped and widely publishing the hash, such as in a newspaper or Usenet post [2-5]. The timestamp proves that the data must have existed at the time, obviously, in order to get into the hash. Each timestamp includes the previous timestamp in its hash, forming a chain, with each additional timestamp reinforcing the ones before it.

4. Proof-of-Work

To implement a distributed timestamp server on a peer-to-peer basis, we will need to use a proof-of-work system similar to Adam Back's Hashcash [6], rather than newspaper or Usenet posts. The proof-of-work involves scanning for a value that when hashed, such as with SHA-256, the hash begins with a number of zero bits. The average work required is exponential in the number of zero bits required and can be verified by executing a single hash.

Excerpts from the whitepaper. Did someone say timechain?

When I first learned how Bitcoin works I also thought that proof-of-work is inefficient and wasteful. After a while, I started to shift my perspective on Bitcoin's energy consumption. It seems that proof-of-work is still widely misunderstood today, in the year 10 AB (after Bitcoin).

> ***Bitcoin's Energy Consumption*** *A shift in perspective*

Since the problems to be solved in proof-of-work are made up, many people seem to believe that it is *useless* work. If the focus is purely on the computation, this is an understandable conclusion. But Bitcoin isn't about computation. It is about *independently agreeing on the order of things.*

Proof-of-work is a system in which everyone can validate what happened and in what order it happened. This independent validation is what leads to consensus, an individual agreement by multiple parties about who owns what.

In a radically decentralized environment, we don't have the luxury of absolute time. Any clock would introduce a trusted third party, a central point in the system which had to be relied upon and could be attacked. "Timing is the root problem," as Grisha Trubetskoy points out. And Satoshi brilliantly solved this problem by implementing a decentralized clock via a proof-of-work blockchain. Everyone agrees beforehand that the chain with the most cumulative work is the source of truth. It is per definition

what actually happened. This agreement is what is now known as Nakamoto consensus.

“The network timestamps transactions by hashing them into an ongoing chain [which] serves as proof of the sequence of events witnessed” —Satoshi Nakamoto

Without a consistent way to tell the time, there is no consistent way to tell before from after. Reliable ordering is impossible. As mentioned above, Nakamoto consensus is Bitcoin’s way to consistently tell the time. The system’s incentive structure produces a probabilistic, decentralized clock, by utilizing both greed and self-interest of competing participants. The fact that this clock is imprecise is irrelevant because the order of events is eventually unambiguous and can be verified by anyone.

Thanks to proof-of-work, both the work *and* the validation of the work are radically decentralized. Everyone can join and leave at will, and everyone can validate everything at all times. Not only that, but everyone can validate the state of the system *individually*, without having to rely on anyone else for validation.

Understanding proof-of-work takes time. It is often counter-intuitive, and while the rules are simple, they lead to quite complex phenomena. For me, shifting my perspective on mining helped. Useful, not useless. Validation, not computation. Time, not blocks.

Bitcoin taught me that telling the time is tricky, especially if you are decentralized.

Lesson 18: Move slowly and don’t break things

It might be a dead mantra, but “move fast and break things” is still how much of the tech world operates. The idea that it doesn’t matter if you get things right the first time is a basic pillar of the *fail early, fail often* mentality. Success is measured in growth, so as long as you are growing everything is fine. If something doesn’t work at first you simply pivot and iterate. In other words: throw enough shit against the wall and see what sticks.

Bitcoin is very different. It is different by design. It is different out of necessity. As Satoshi pointed out, e-currency has been tried many times before, and all previous attempts have failed because there was a head which could be cut off. The novelty of Bitcoin is that it is a beast without heads.

“A lot of people automatically dismiss e-currency as a lost cause because of all the companies that failed since the 1990’s. I hope it’s obvious it was only the centrally controlled nature of those systems that doomed them.” —Satoshi Nakamoto

One consequence of this radical decentralization is an inherent resistance to change. “Move fast and break things” does not and will never work on the Bitcoin base layer. Even if it would be desirable, it wouldn’t be possible without convincing *everyone* to change their ways. That’s distributed consensus. That’s the nature of Bitcoin.

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

This is one of the many paradoxical properties of Bitcoin. We all came to believe that anything which is software can be changed easily. But the nature of the beast makes changing it bloody hard.

As Hasu beautifully shows in Unpacking Bitcoin’s Social Contract, changing the rules of Bitcoin is only possible by *proposing* a change, and consequently *convincing* all users of Bitcoin to adopt this change. This makes Bitcoin very resilient to change, even though it is software.

This resilience is one of the most important properties of Bitcoin. Critical software systems have to be antifragile, which is what the interplay of Bitcoin’s social layer and its technical layer guarantees. Monetary systems are adversarial by nature, and as we have known for thousands of years solid foundations are essential in an adversarial environment.

“The rain came down, the floods came, and the winds blew, and beat on that house; and it didn’t fall, for it was founded on the rock.” —Matthew 7:24–27

Arguably, in this parable of the wise and the foolish builders Bitcoin isn’t the house. It is the rock. Unchangeable, unmoving, providing the foundation for a new financial system.

Just like geologists, who know that rock formations are always moving and evolving, one can see that Bitcoin is always moving and evolving as well. You just have to know where to look and how to look at it.

The introduction of pay to script hash and segregated witness are proof that Bitcoin’s rules can be changed if enough users are convinced that adopting said change is to the benefit of the network. The latter enabled the development of the lightning network, which is one of the houses being built on Bitcoin’s solid foundation. Future upgrades like Schnorr signatures will enhance efficiency and privacy, as well as scripts (read: smart contracts) which will be indistinguishable from regular transactions thanks to Taproot. Wise builders do indeed build on solid foundations.

Satoshi wasn’t only a wise builder technologically. He also understood that it would be necessary to make wise decisions ideologically.

"Being open source means anyone can independently review the code. If it was closed source, nobody could verify the security. I think it's essential for a program of this nature to be open source." —Satoshi Nakamoto

Openness is paramount to security and inherent in open source and the free software movement. As Satoshi pointed out, secure protocols and the code which implements them have to be open—there is no security through obscurity. Another benefit is again related to decentralization: code which can be run, studied, modified, copied, and distributed freely ensures that it is spread far and wide.

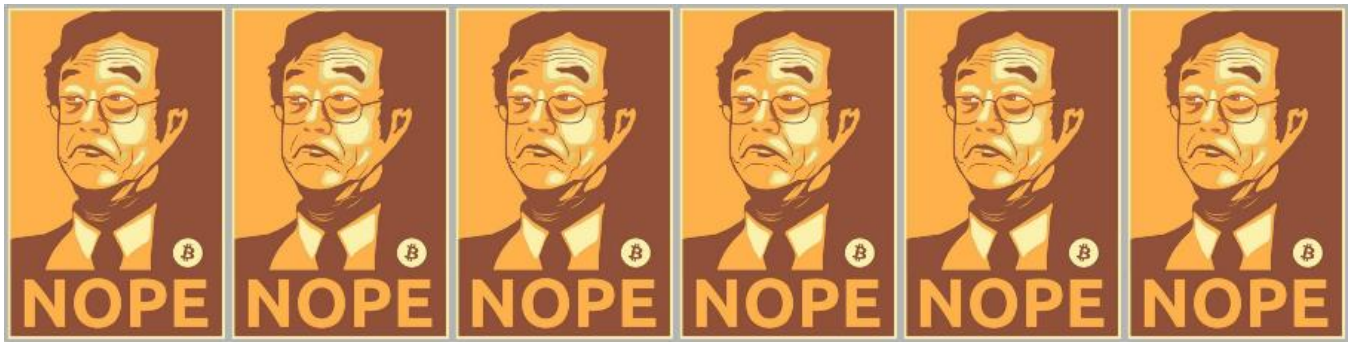
The radically decentralized nature of Bitcoin is what makes it move slowly and deliberately. A network of nodes, each run by a sovereign individual, is inherently resistant to change—malicious or not. With no way to force updates upon users the only way to introduce changes is by slowly convincing each and every one of those individuals to adopt a change. This non-central process of introducing and deploying changes is what makes the network incredibly resilient to malicious changes. It is also what makes fixing broken things more difficult than in a centralized environment, which is why everyone tries not to break things in the first place.

Bitcoin taught me that moving slowly is one of its features, not a bug.

Lesson 19: Privacy is not dead

If pundits are to believed, privacy has been dead since the 80ies. The pseudonymous invention of Bitcoin and other events in recent history show that this is not the case. Privacy is alive, even though it is by no means easy to escape the surveillance state.

Satoshi went through great lengths to cover up his tracks and conceal his identity. Ten years later, it is still unknown if Satoshi Nakamoto was a single person, a group of people, male, female, or a time-traveling AI which bootstrapped itself to take over the world. Conspiracy theories aside, Satoshi chose to identify himself to be a Japanese male, which is why I don't assume but respect his chosen gender and refer to him as *he*.



"I am not Dorian Nakamoto."

Whatever his real identity might be, Satoshi was successful in hiding it. He set an encouraging example for everyone who wishes to remain anonymous: it is possible to have privacy online.

“Encryption works. Properly implemented strong crypto systems are one of the few things that you can rely on.”

—Edward Snowden

Satoshi wasn’t the first pseudonymous or anonymous inventor, and he won’t be the last. Some have directly imitated this pseudonymous publication style, like Tom Elvis Yedusor of MimbleWimble fame, while others have published advanced mathematical proofs while remaining completely anonymous.

It is a strange new world we are living in. A world where identity is optional, contributions are accepted based on merit, and people can collaborate and transact freely. It will take some adjustment to get comfortable with these new paradigms, but I strongly believe that all of this has the potential to change the world for the better.

We should all remember that privacy is a fundamental human right. And as long as people exercise and defend these rights the battle for privacy is far from over. Bitcoin taught me that privacy is not dead.

Lesson 20: Cypherpunks write code

Like many great ideas, Bitcoin didn’t come out of nowhere. It was made possible by utilizing and combining many innovations and discoveries in mathematics, physics, computer science, and other fields. While undoubtedly a genius, Satoshi wouldn’t have been able to invent Bitcoin without the giants on whose shoulders he was standing on.

“He who only wishes and hopes does not interfere actively with the course of events and with the shaping of his own destiny.”

—Ludwig Von Mises

One of these giants is Eric Hughes, one of the founders of the cypherpunk movement and author of the cypherpunk manifesto. It’s hard to imagine that Satoshi wasn’t influenced by this manifesto. It speaks of many things which Bitcoin enables and utilizes, such as direct and private transactions, electronic money and cash, anonymous systems, and defending privacy with cryptography and digital signatures.

“Privacy is necessary for an open society in the electronic age. [...] Since we desire privacy, we must ensure that each party to a transaction have knowledge only of that which is directly necessary for that transaction. [...]

Therefore, privacy in an open society requires anonymous transaction systems. Until now, cash has been the primary such system. An anonymous transaction system is not a secret transaction system. [...]

We the Cypherpunks are dedicated to building anonymous systems. We are defending our privacy with cryptography, with anonymous mail forwarding systems, with digital signatures, and with electronic money.

Cypherpunks write code.”

Cypherpunks do not find comfort in hopes and wishes. They actively interfere with the course of events and shape their own destiny. Cypherpunks write code.

Thus, in true cypherpunk fashion, Satoshi sat down and started to write code. Code which took an abstract idea and proved to the world that it actually worked. Code which planted the seed of a new economic reality. Thanks to this code, everyone can verify that this novel system actually works, and every 10 minutes or so Bitcoin proofs to the world that it is still living.

```
23  map<uint256, CBlockIndex*> mapBlockIndex;
24  const uint256 hashGenesisBlock("0x000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f");
25  CBlockIndex* pindexGenesisBlock = NULL;
26  int nBestHeight = -1;
27  uint256 hashBestChain = 0;
28  CBlockIndex* pindexBest = NULL;
 :
675 int64 CBlock::GetBlockValue(int64 nFees) const
676 {
677     int64 nSubsidy = 50 * COIN;
678
679     // Subsidy is cut in half every 4 years
680     nSubsidy >>= (nBestHeight / 210000);
681
682     return nSubsidy + nFees;
683 }
684
685 unsigned int GetNextWorkRequired(const CBlockIndex* pindexLast)
686 {
687     const unsigned int nTargetTimespan = 14 * 24 * 60 * 60; // two weeks
688     const unsigned int nTargetSpacing = 10 * 60;
689     const unsigned int nInterval = nTargetTimespan / nTargetSpacing;
690
691     // Genesis block
692     if (pindexLast == NULL)
693         return bnProofOfWorkLimit.GetCompact();
```

Code excerpts from Bitcoin [version 0.1.0]

To make sure that his innovation transcends fantasy and becomes reality, Satoshi wrote code to implement his idea before he wrote the whitepaper. He also made sure not to delay any release forever. After all, "there's always going to be one more thing to do."

"I had to write all the code before I could convince myself that I could solve every problem, then I wrote the paper."

—Satoshi Nakamoto

In today's world of endless promises and doubtful execution, an exercise in dedicated building was desperately needed. Be deliberate, convince yourself that you can actually solve the problems, and implement the solutions. We should all aim to be a bit more cypherpunk.

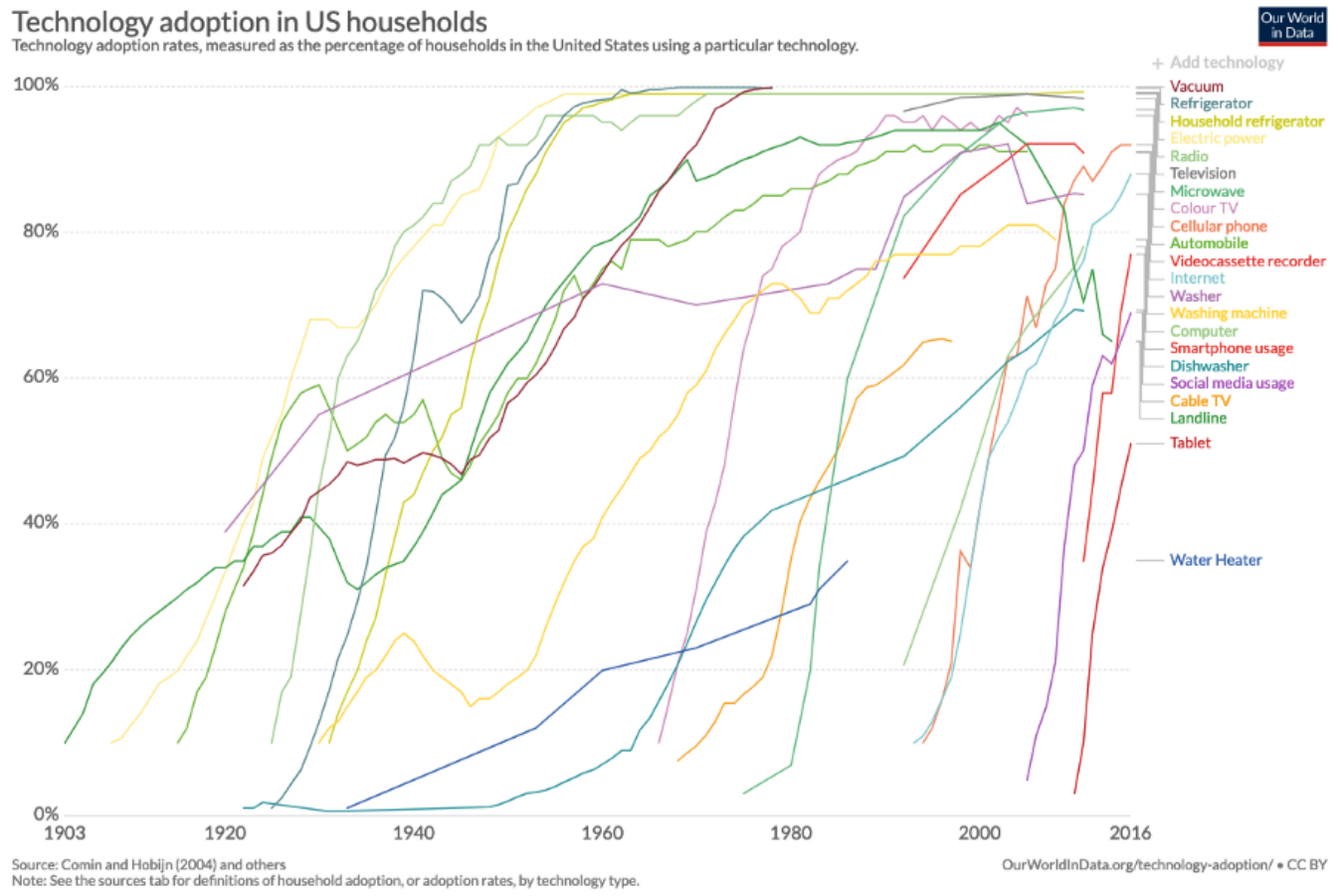
Bitcoin taught me that cypherpunks write code.

Lesson 21: Metaphors for Bitcoin's future

In the last couple of decades, it became apparent that technological innovation does not follow a linear trend. Whether you believe in the technological singularity or not,

it is undeniable that progress is exponential in many fields. Not only that, but the rate at which technologies are being adopted is accelerating, and before you know it the bush in the local schoolyard is gone and your kids are using Snapchat instead. Exponential curves have the tendency to slap you in the face way before you see them coming.

Bitcoin is an exponential technology built upon exponential technologies. Our World in Data beautifully shows the rising speed of technological adoption, starting in 1903 with the introduction of landlines. Landlines, electricity, computers, the internet, smartphones; all follow exponential trends in price-performance and adoption. Bitcoin does too.



Bitcoin is literally off the charts.

Bitcoin has not one but multiple network effects, all of which resulting in exponential growth patterns in their respective area: price, users, security, developers, market share, and adoption as global money.

Having survived its infancy, Bitcoin is continuing to grow every day in more aspects than one. Granted, the technology has not reached maturity yet. It might be in its

adolescence. But if the technology is exponential, the path from obscurity to ubiquity is short.

Mobile phone, ca 1965 vs 2019.

In his 2003 TED talk, Jeff Bezos chose to use electricity as a metaphor for the web's future. All three phenomena—electricity, the internet, Bitcoin—are *enabling* technologies, networks which enable other things. They are infrastructure to be built upon, foundational in nature.

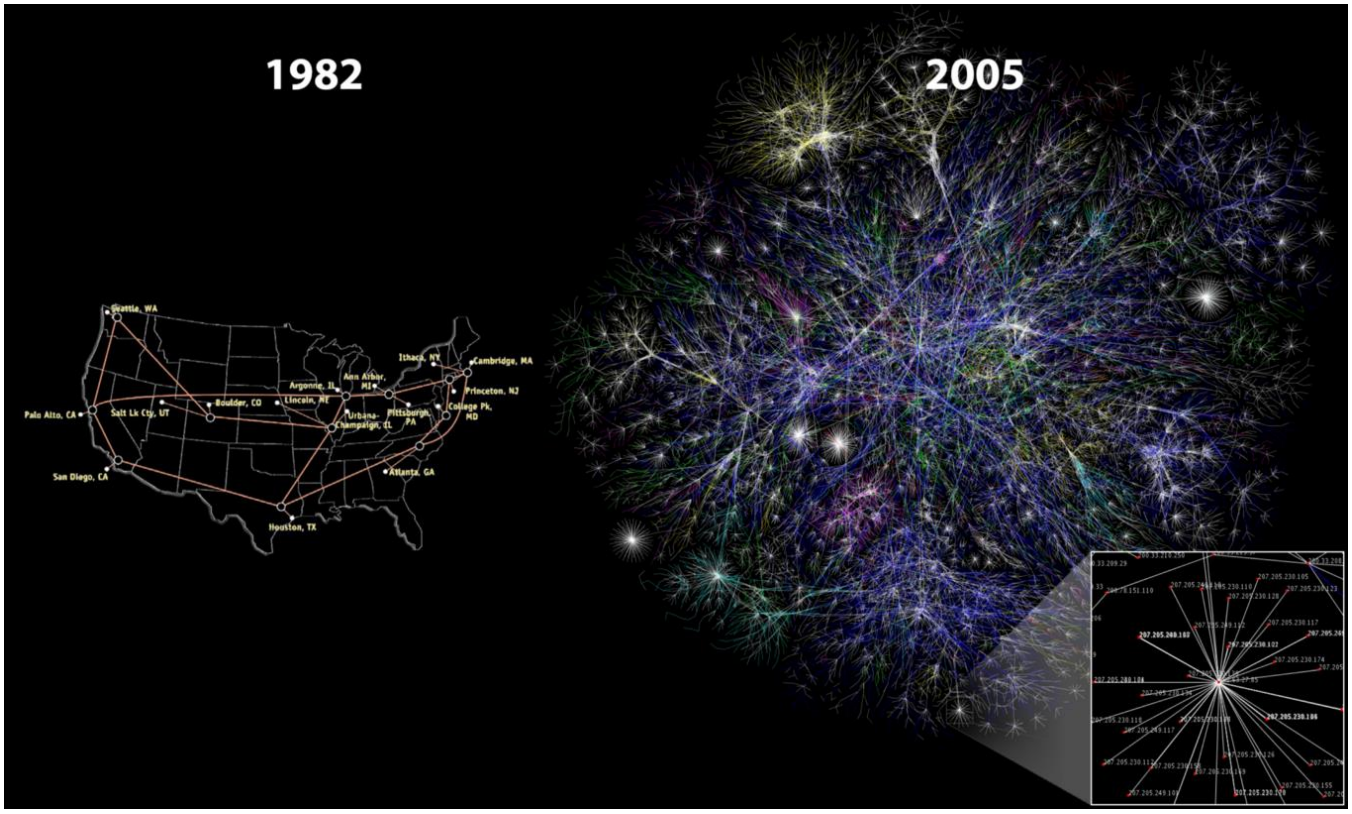
Electricity has been around for a while now. We take it for granted. The internet is quite a bit younger, but most people already take it for granted as well. Bitcoin is ten years old and has entered public consciousness during the last hype cycle. Only the earliest of adopters take it for granted. As more time passes, more and more people will recognize Bitcoin as something which simply is.

In 1994, the internet was still confusing and unintuitive. Watching this old recording of the Today Show makes it obvious that what feels natural and intuitive now actually wasn't back then. Bitcoin is still confusing and alien to most, but just like the internet is second nature for digital natives, spending and stacking sats will be second nature to the bitcoin natives of the future.

"The future is already here—it's just not very evenly distributed." —William Gibson

In 1995, about 15% of American adults used the internet. Historical data from the Pew Research Center shows how the internet has woven itself into all our lives. According to a consumer survey by Kaspersky Lab, 13% of respondents have used Bitcoin and its clones to pay for goods in 2018. While payments aren't the only use-case of bitcoin, it is some indication of where we are in Internet time: in the early- to mid-90s.

In 1997, Jeff Bezos stated in a letter to shareholders that "this is Day 1 for the Internet," recognizing the great untapped potential for the internet and, by extension, his company. Whatever day this is for Bitcoin, the vast amounts of untapped potential are clear to all but the most casual observer.

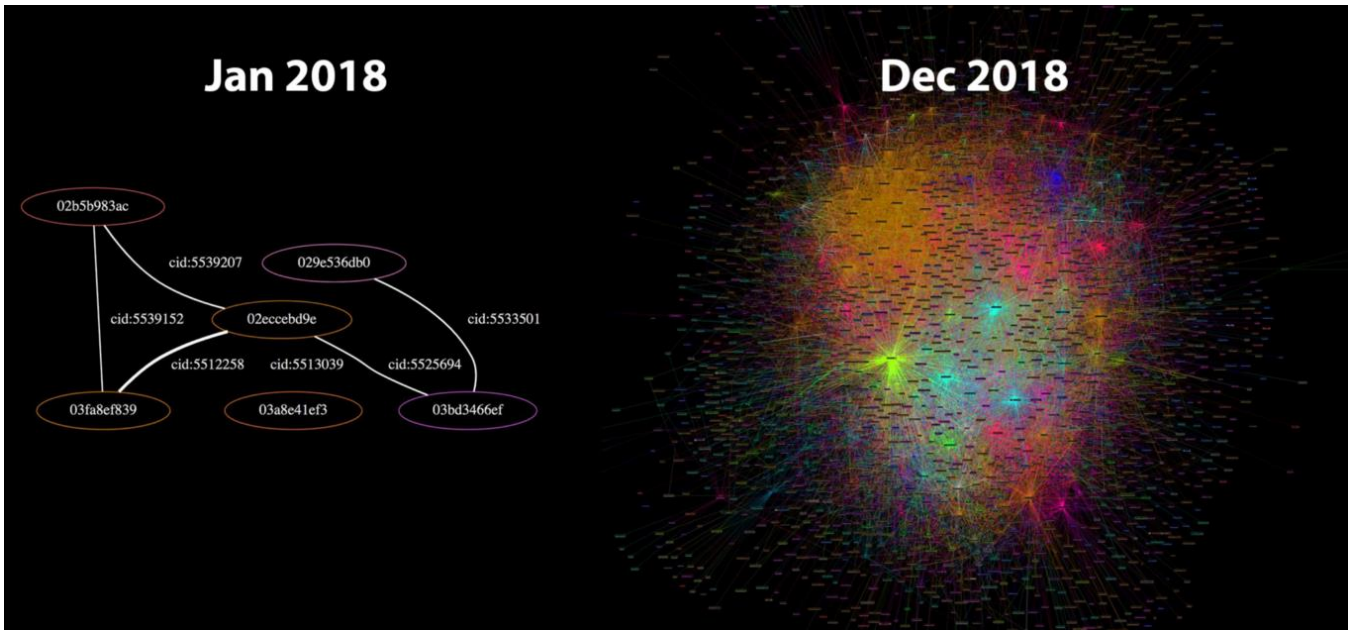


The internet, 1982 vs 2005. Source: cc-by Merit Network, Inc. and Barrett Lyon, Opte Project

Bitcoin's first node went online in 2009 after Satoshi mined the genesis block and released the software into the wild. His node wasn't alone for long. Hal Finney was one of the first people to pick up on the idea and join the network. Ten years later, as of this writing, more than 10.000 nodes are running bitcoin.

The protocol's base layer isn't the only thing growing exponentially. The lightning network, a second layer technology, is growing at an even faster rate.

In January 2018, the lightning network had 40 nodes and 60 channels. In April 2019, the network grew to more than 4000 nodes and around 40.000 channels. Keep in mind that this is still experimental technology where loss of funds can and does occur. Yet the trend is clear: thousands of people are reckless and eager to use it.



Lightning Network, January 2018 vs December 2018. Source: Jameson Lopp

To me, having lived through the meteoric rise of the web, the parallels between the internet and Bitcoin are obvious. Both are networks, both are exponential technologies, and both enable new possibilities, new industries, new ways of life. Just like electricity was the best metaphor to understand where the internet is heading, the internet might be the best metaphor to understand where bitcoin is heading. Or, in the words of Andreas Antonopoulos, Bitcoin is *The Internet of Money*. These metaphors are a great reminder that while history doesn't repeat itself, it often rhymes.

Exponential technologies are hard to grasp and often underestimated. Even though I have a great interest in such technologies, I am constantly surprised by the pace of progress and innovation. Watching the Bitcoin ecosystem grow is like watching the rise of the internet in fast-forward. It is exhilarating.

My quest of trying to make sense of Bitcoin has led me down the pathways of history in more ways than one. Understanding ancient societal structures, past monies, and how communication networks evolved were all part of the journey. From the handaxe to the smartphone, technology has undoubtedly changed our world many times over. Networked technologies are especially transformational: writing, roads, electricity, the internet. All of them changed the world. Bitcoin has changed mine and will continue to change the minds and hearts of those who dare to use it.

Bitcoin taught me that understanding the past is essential to understanding its future. A future which is just beginning.

Conclusion

Technology is all about the application of scientific knowledge to solve problems in the real world. Every technology has to make tradeoffs in terms of efficiency, cost, security, and many other properties. Just like there is no perfect solution to deriving a square from a circle, any solution to the problems which Bitcoin tries to solve will always be imperfect as well.

Da Vinci tried to solve the intractable problem of squaring a circle with the *Vitruvian Man*, which places a human right at the center of it. Bitcoin tries to solve the double spending problem with sovereign individuals, which places humans behind each node, effectively removing any concept of a center.

Bitcoin's headless nature shows us that seemingly simple concepts like creating accounts and agreeing on time require creative solutions in decentralized systems. It also shows that such systems can be astonishingly antifragile. How do you best kill something if the best point of attack is everywhere?

Even with all its quirks and seeming shortcomings, Bitcoin undoubtedly works. It keeps producing blocks roughly every ten minutes and does so beautifully. The longer Bitcoin continues to work, the more people will opt-in to use it.

"It's true that things are beautiful when they work. Art is function." —Giannina Braschi

Bitcoin is growing exponentially, blurring the line between disciplines. It isn't clear where the realm of pure technology ends and where another realm begins. I tried to differentiate the economic teachings of Bitcoin from the philosophical and the technological ones, which turned out more difficult than expected.

Just like in biological systems, removing one part seems to affect the whole. Maybe the most important lesson is that Bitcoin should be examined holistically, from multiple angles, if one would like to have a complete picture. Just like removing one part from Bitcoin destroys the whole (*cough* blockchain *cough*), examining parts of Bitcoin in isolation seems to taint the understanding of the whole system.

My journey continues, and as mentioned in part one, I think that any answer to the question *"What have you learned from Bitcoin?"* will always be incomplete. In any case, I've learned that the philosophy, economics, and technology of Bitcoin interact in a complex feedback loop, and I hope that these 21 lessons are just the beginning of what I've learned from Bitcoin.

Acknowledgments

- Once more, thanks to Arjun Balaji for the tweet which gave birth to this series.
- Thanks to Andreas M. Antonopoulos for all the educational material he has put out over the years.

- Thanks to Marty and Matt for guiding me through the rabbit hole and reminding us all to stay humble and stack sats.
- Thanks to Francis Pouliot for sharing his excitement about finding out about the timechain.
- Thanks to Brandon,Camilo,Daniel,Jannik, Michael, and Raphael for providing feedback to early drafts of this article
- Thanks to the countless authors and content producers who influenced my thinking on Bitcoin and the topics it touches. There are simply too many to name.
- And finally, thank *you* for reading this series. I hope you enjoyed it as much as I did enjoy writing it. Feel free to reach out to me on twitter. My DMs are open.

Further Reading

- *Bitcoin: A Peer-to-Peer Electronic Cash System* by Satoshi Nakamoto
- *Mastering Bitcoin* by Andreas Antonopoulos
- *The Internet of Money* by Andreas Antonopoulos
- *Inventing Bitcoin* by Yan Pritzker
- *Applied Cryptography* by Bruce Schneier
- *Reflections on Trusting Trust* by Ken Thompson
- *Cypherpunks* by Julian Assange with Jacob Appelbaum
- *The Anatomy of Proof-of-Work* by Hugo Nguyen
- *Blockchain Proof-of-Work Is a Decentralized Clock* by Gregory Trubetskoy
- *Unpacking Bitcoin's Social Contract* by Hasu
- *Why Bitcoin Matters* by Aleksandar Svetski
- *Guess My Bitcoin Private Key* by Michael Kerbleski

The Puell Multiple

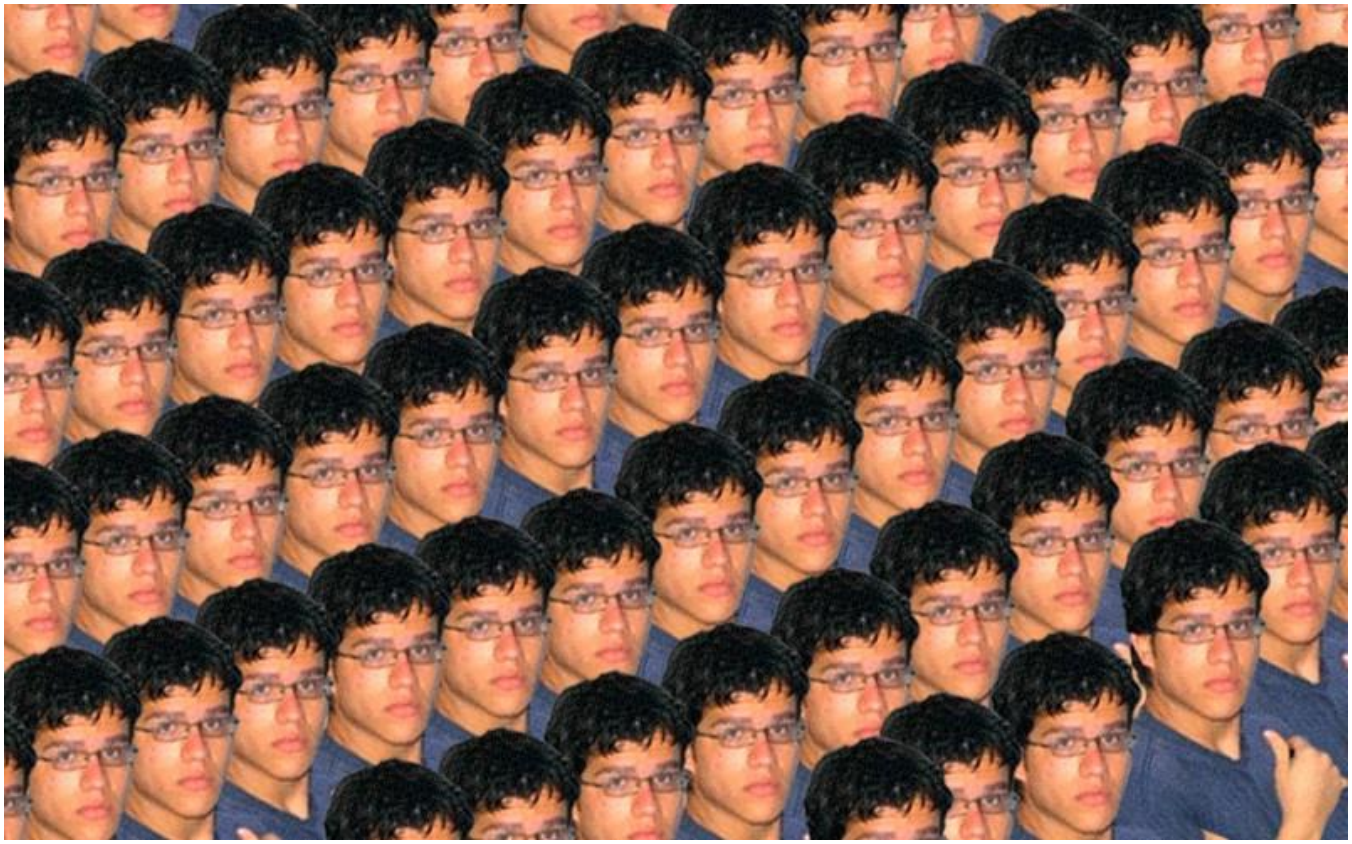
A New Barometer of Bitcoin's Market Cycles

By cryptopoiesis

Posted April 4, 2019

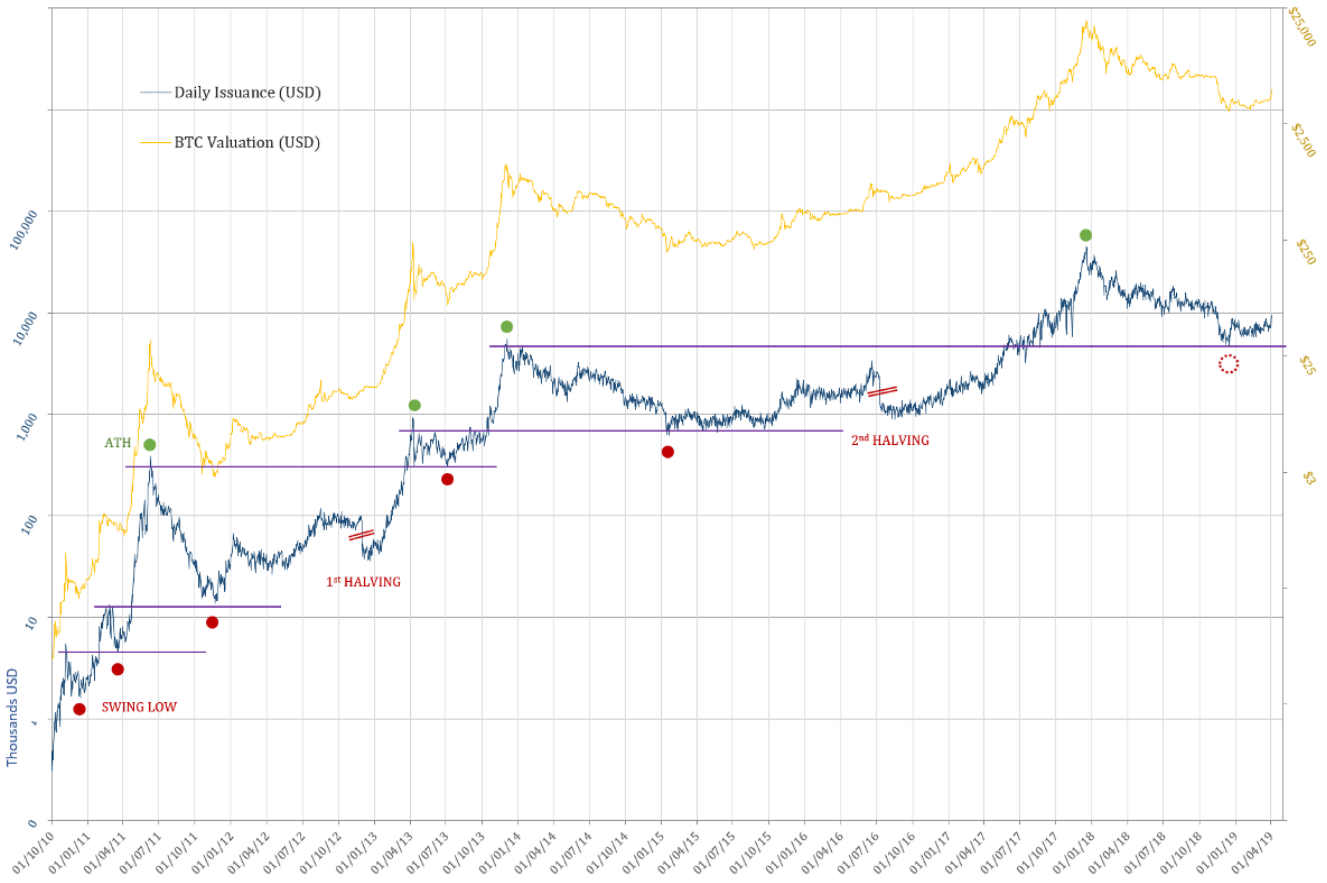
Most metrics aimed at timing or quantifying Bitcoin's market cycles, from a fundamental perspective, have by and large focused on the velocity of value settled on chain, or lack there of, thus analysing the cycles from a buyer/investor's

perspective. Realised Cap, NVT Ratio, Market-Value-to- Realised-Cap (MVRV) and HODL Waves are just a few powerful metrics and visuals that have provided valuable insight.



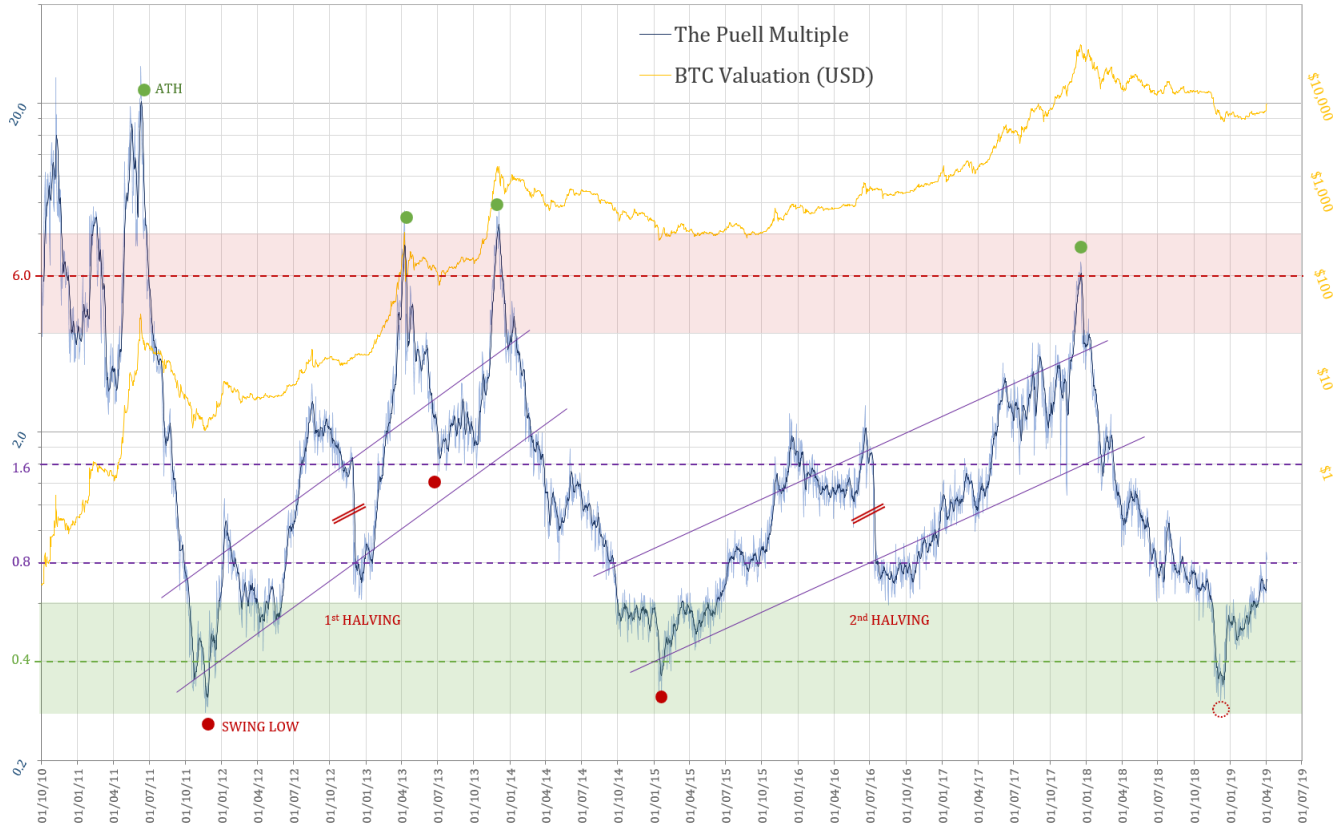
Being David Puell

Another type of metric, which has recently gained some attention in the Crypto community, is the the **Dollar Value of Mined Coins** on daily basis or **Bitcoin's Daily Issuance**. This metric proved to have consistently identify all the **swing lows** based on previous **All Time Highs** like clockwork. This relationship held for the two major, halving associated, bull-bear market cycles as well as the several shorter ones during the early years.



This metric shines a light onto the other side of the coin from the proverbial ***Hodlers of Last Resort***, namely the ***Compulsory Sellers*** and the ***fundamentals of mining profitability*** that are at play in shaping Bitcoin's market cycles. **David Puell**'s simple yet ingenious idea of adjusting this metric by its yearly simple moving average has produce a new, powerful and elegant tool to gauge the market cycles from a ***Mining Profitability/ Compulsory Sellers***' perspective.

$$Puell\ Multiple = \frac{Daily\ Coin\ Issuance_{USD}}{MA_{365}(Daily\ Coin\ Issuance_{USD})}$$



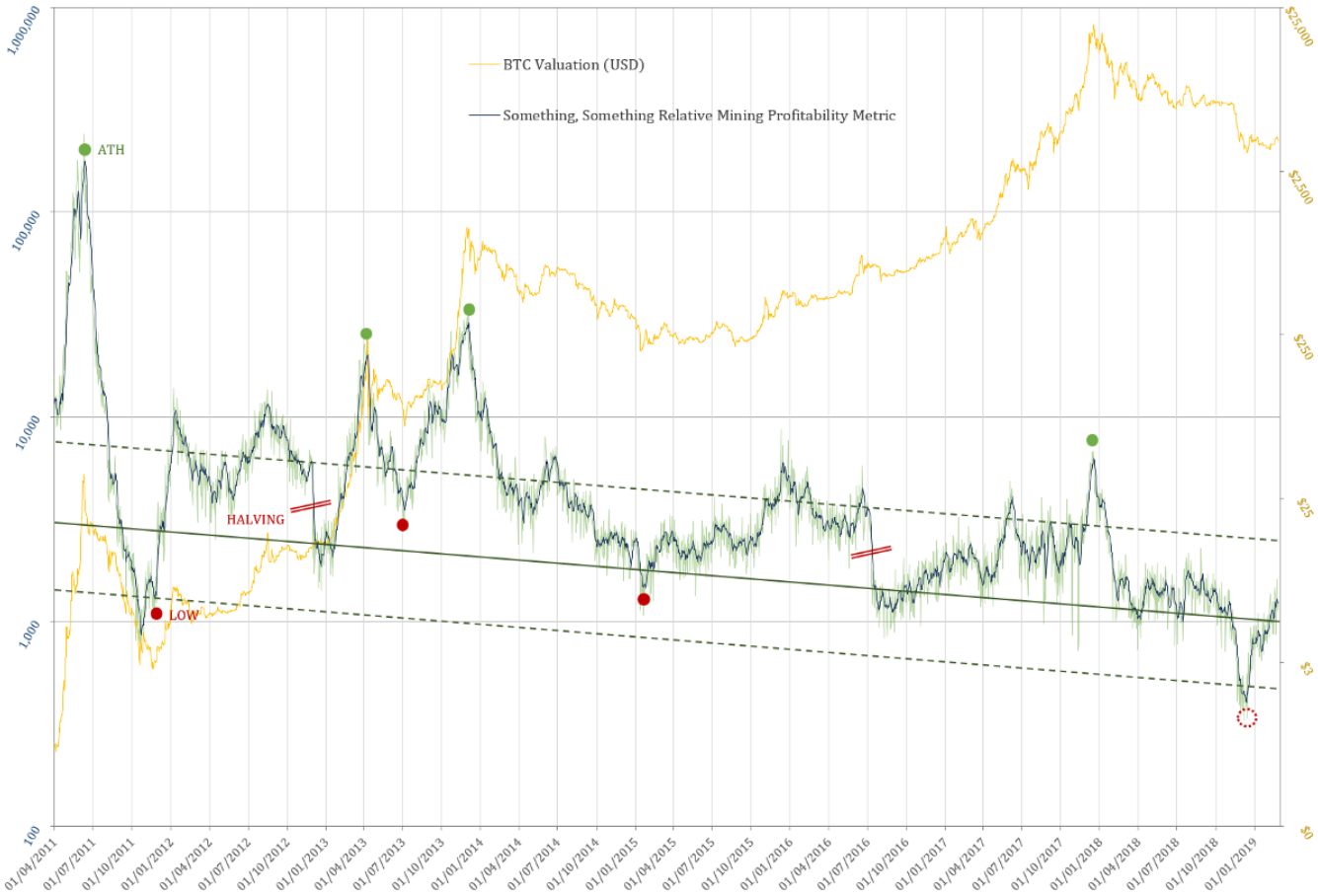
The Puell Multiple

As the mechanism which underpin the correlations are dictated by the dynamics of Mining Profitability, the daily bitcoin issuance coming from block rewards has so far sufficed—daily coin issuance having currently a theoretical average of 1,800 bitcoin daily. However, after the next (third) halving which is due in mid 2020, the **transaction fees** collected by miners will no longer be trivial by comparison to block rewards. The relationship of this metric therefor, would most likely have to include the entire **Daily Mining Revenue,** which incorporates the transaction fees in addition to the block-reward e.g.:

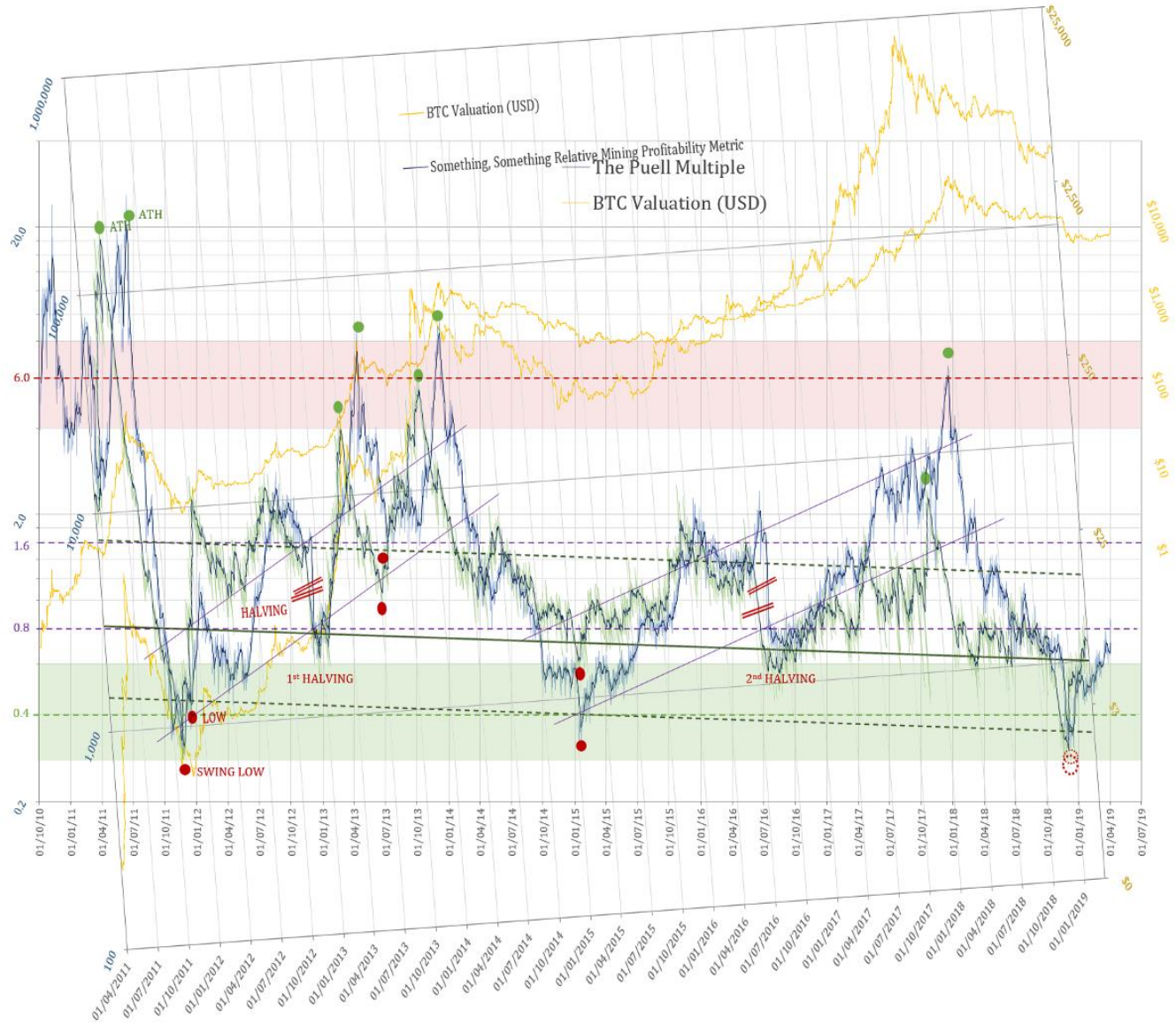
$$Puell\ Multiple = \frac{Mining\ Revenue_{USD}}{MA_{365}(Mining\ Revenue_{USD})}$$

Previous attempts at quantifying the fundamentals from the miner's perspective, used as a starting point the ***PetaHashDollar*** metric (Daily Mining Revenue divided

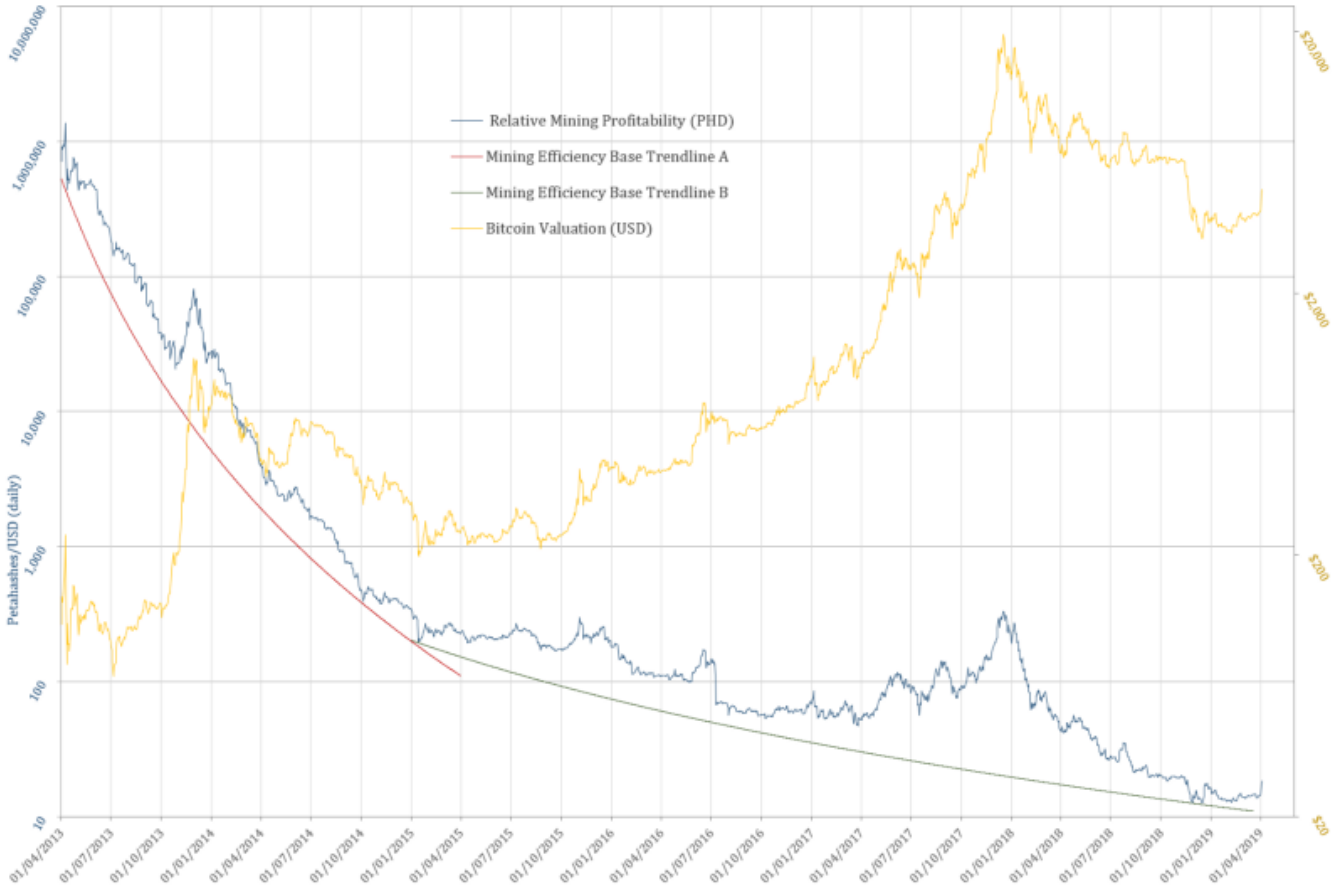
by Daily PetaHashes). The attempts at normalising, either by a trend, or more organically by using the **Difficulty Adjustment,** have all fallen short of producing a simple and accurate metric. Furthermore, all the different averages which have been tried out so far to calculate the Puell Multiple, have proven to skew the metric in one way or another. They failed at achieving a virtually perfect alignment of the tops, bottoms and, interestingly enough, the levels at which both previous halvings took place.



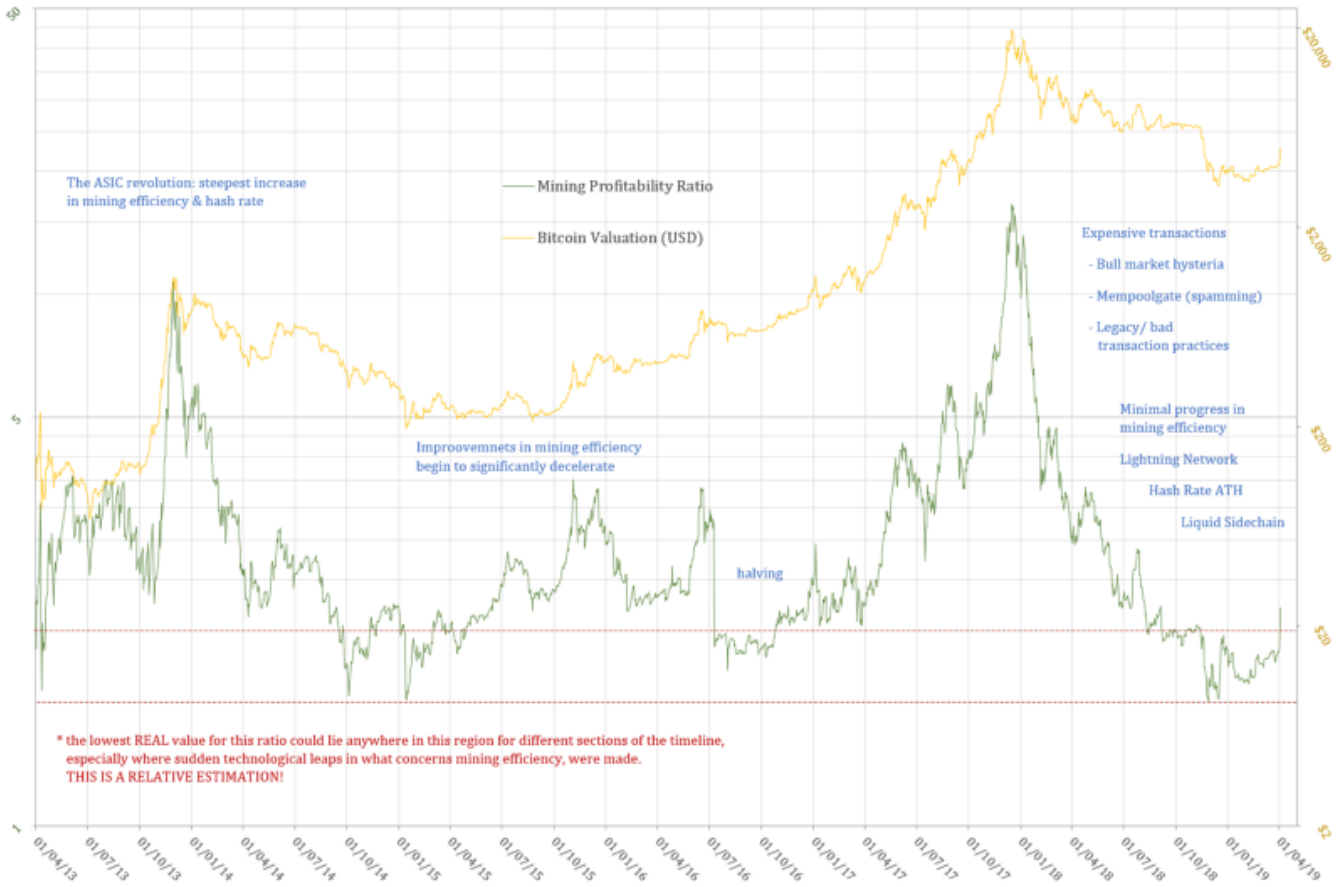
Example of a work in progress **Mining Profitability Metric** that took into account and adjusted for: **Hash Rate**, **Mining Revenue** and **Difficulty Adjustment**



The same **Mining Profitability Metric** superimposed onto the **Puell Multiple**



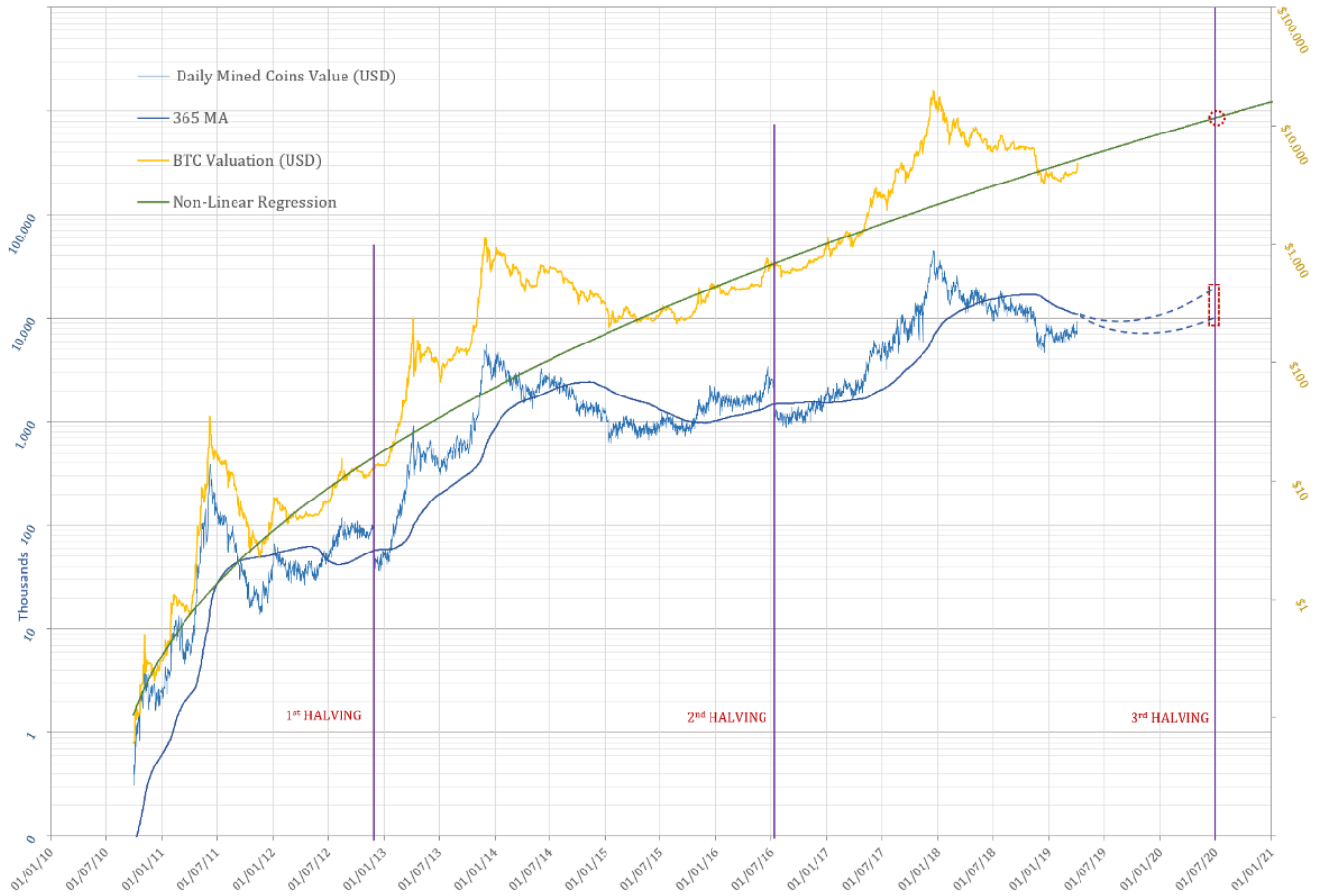
Another example: **PetaHashDollar = Mining Revenue / Hash Rate**



Mining Profitability Ratio derived from **PetaHashDollar** normalised by the baseline equations

Where To?

If one is to expect the next halving to occur at levels of the Puell Multiple in line with the two previous ones (1.6), it would be an interesting exercise to use it in approximating the price of Bitcoin around the next halving. As no data that would go into making the Daily Coin Issuance 365 days SMA is in at this time, only an eyeballing approach can be employed for this purpose. This would allow comparing this hypothetical range to the one which can be calculated by the forward projection of the non-linear regression of the price.



A variation on **Renato Shirakashi's Non-Linear Regression Curve for Bitcoin**has been developed with new parameters as to minimise the total of daily percentage divergence from the original Shirakashi's Regression, and which can be said to "better hug" the base of the price-line. As the volatility and magnitude of future bull-markets/ bubbles are expected to decrease with the maturity and growth of this financial asset, this version had been chosen for the purpose of this projection.

Eyeballing the 365day SMA of the Puell Multiple between the values shown in the the graph above would imply a price in the range from **$8,889** to **$17,778,**that of course if the halving would occur, once more, at Puell Multiple level of ~ 1.6.

The non-linear regression would be at this point in time at a level of **$11,667**. The first halving occurred below this regression model, while the second occurred at the level... will this trend continue... and see us above the non-linear regression model at the time of the halvening in mid 2020? Yes, with a large dose of hopeium :)

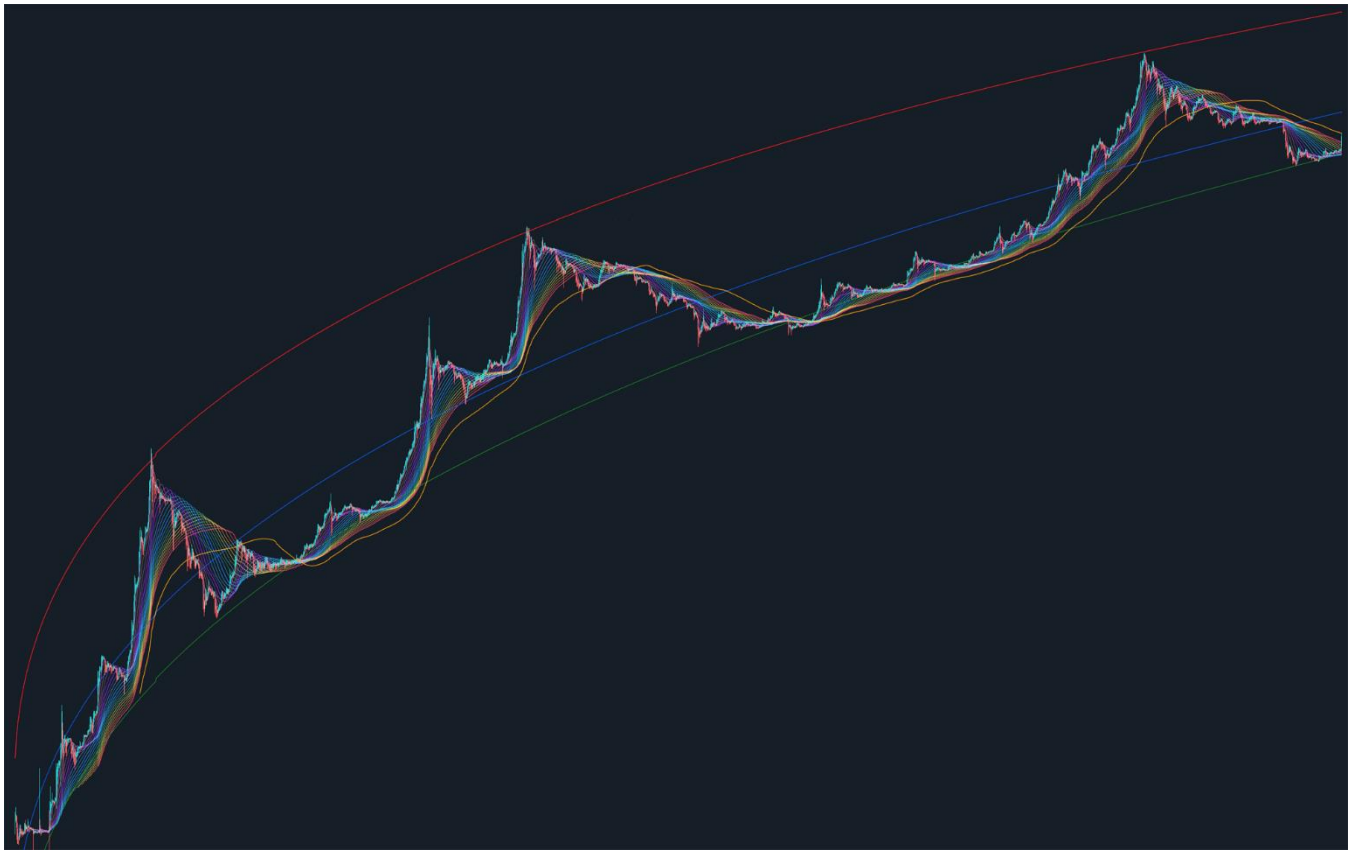
Acknowledgements

- **David Puell**
- **Renato Shirakashi**

- **TusenPi** All reference data used throughout this article has been sourced from:
- **BitcoinVisuals.com** (Hash Rate, Coin Supply)
- **Blockchain.info** (Daily Market Price, Daily Transaction Fees/BTC)
- **CoinMarketCap.com** (Closing Daily Price)

Postscriptum

Bitcoin is Beautiful!



Bitcoin's Non-Linear Regression Curve by Renato Shirakashi & Multiple SMA by TusenPi

---

Experiments on Cumulative Destruction

Two Approaches to Bring Bitcoindays Destroyed Into the Price Domain

By David Puell and Willy Woo

Posted April 9, 2019

Disclaimer: Nothing here should be considered investment or trading advice.

Okay, so this article is now well overdue given the recent price action. BTC never rests! The last few months have been very productive in terms of discovering new valuation metrics based on on-chain analytics. The recent proposals using coindays destroyed by Tamas Blummer and the team at Adamant Capital have put this essential metric once again on the map. We thought we'd give it a go at coming up with a way to best translate the concept of destruction into a precise price level for market analysis.

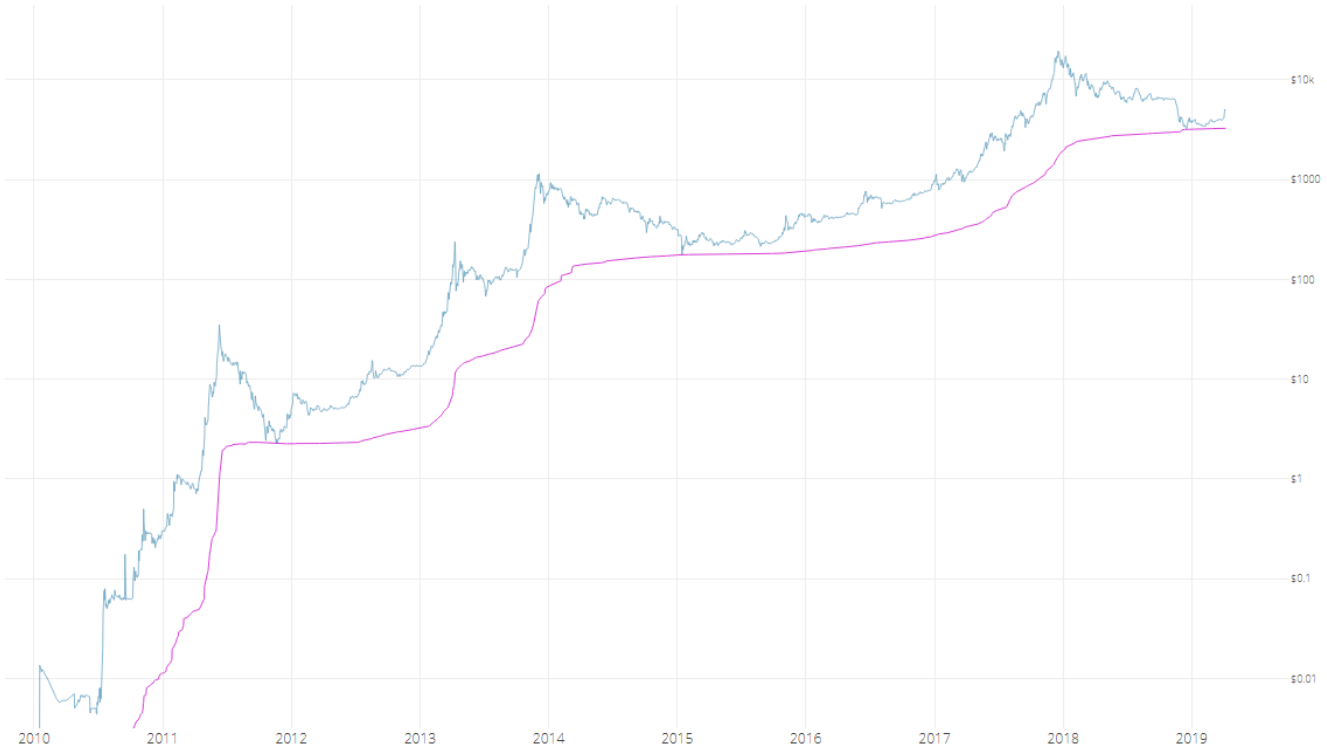
Experiment A: Cumulative Value-Days Destroyed (CVDD) by Willy Woo

When coins move from one investor to another, the transaction carries both a USD value and also destroys a time value relating to how long the original investor held their coins. CVDD tracks the cumulative sum of this value-time destruction as coins move from old hands into new hands as a ratio to the market age. It is calculated with the following formula:

$$CVDD_{USD} = \frac{\sum(CoindaysDestroyed \cdot Price_{USD})}{Days \cdot 6{,}000{,}000}$$

Note that 6 million is used for calibrating the chart. This number is arbitrary and would be different had we used hours or blocks as unit for the age of the market.

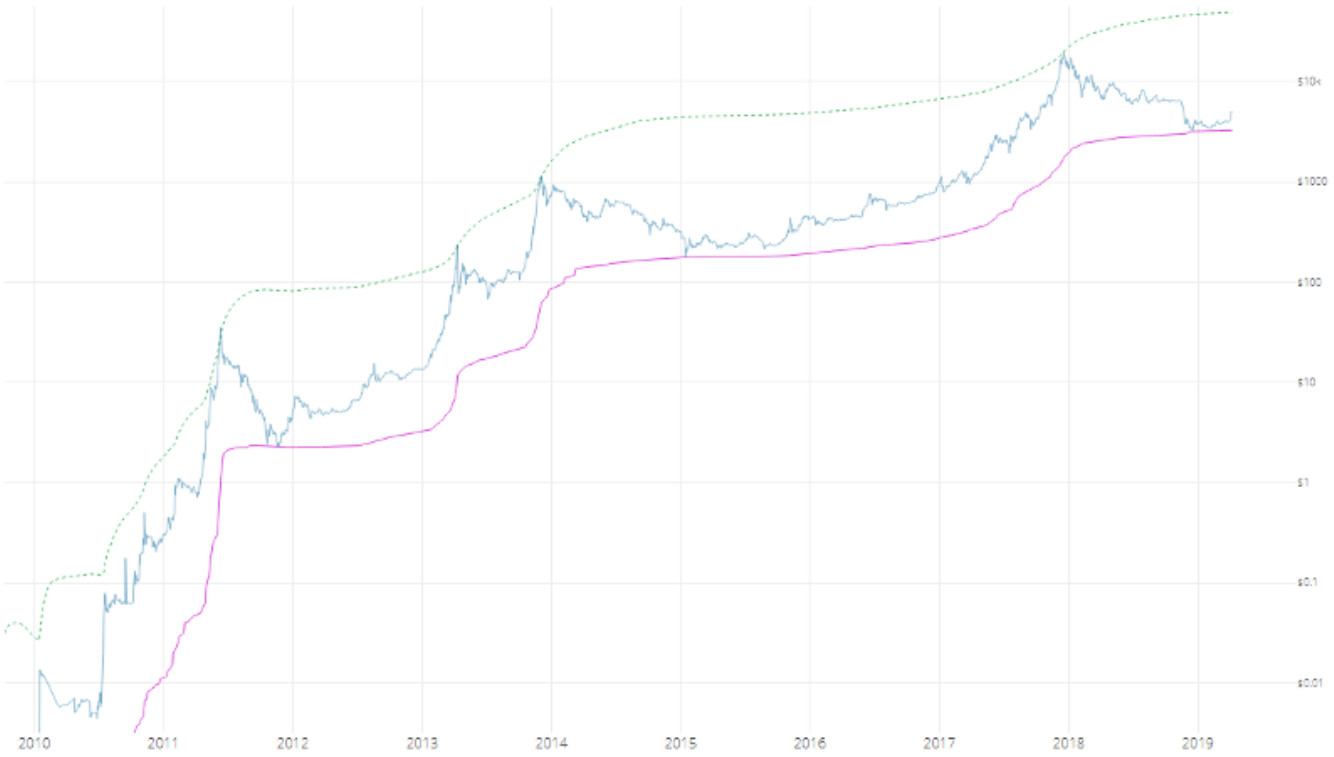
CVDD has hit the historical Bitcoin price bottoms with remarkable accuracy.



CVDD

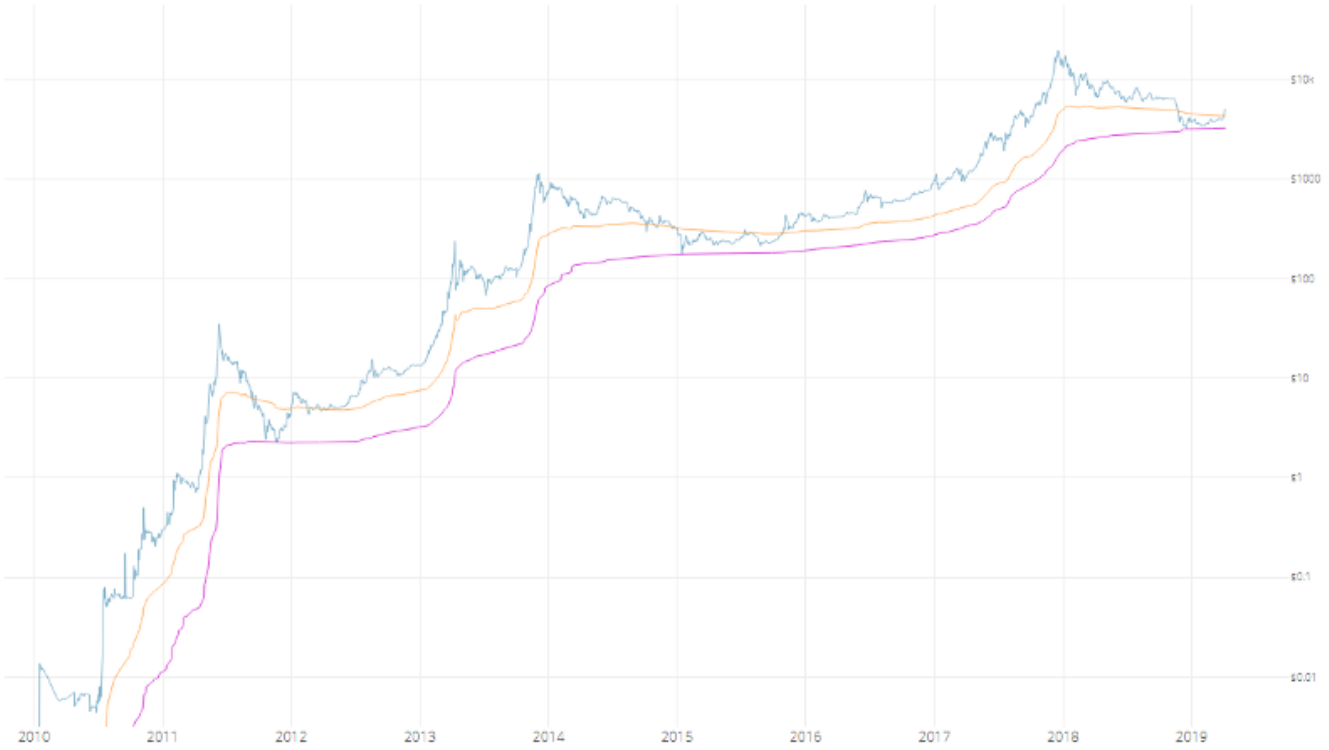
Unlike delta cap, CVDD tends to consistently climb in value—this becomes useful to frame an increasing lower bound for a market bottom during bear seasons when the market price is falling.

When used in conjunction with the top price model, CVDD and top price provide upper and lower bands for price action.



CVDD and top price

When used in conjunction with Coinmetric's realized price, CVDD can help the visualization of Bitcoin's accumulation bottoms.



CVDD and realized price

Both CVDD and realized price have remarkable resemblances in shape, so it is no coincidence that they both use HODL time by the investor in their calculation. It is important to note that both CVDD and top price are interesting curiosities, and are not guaranteed to work in future cycles.

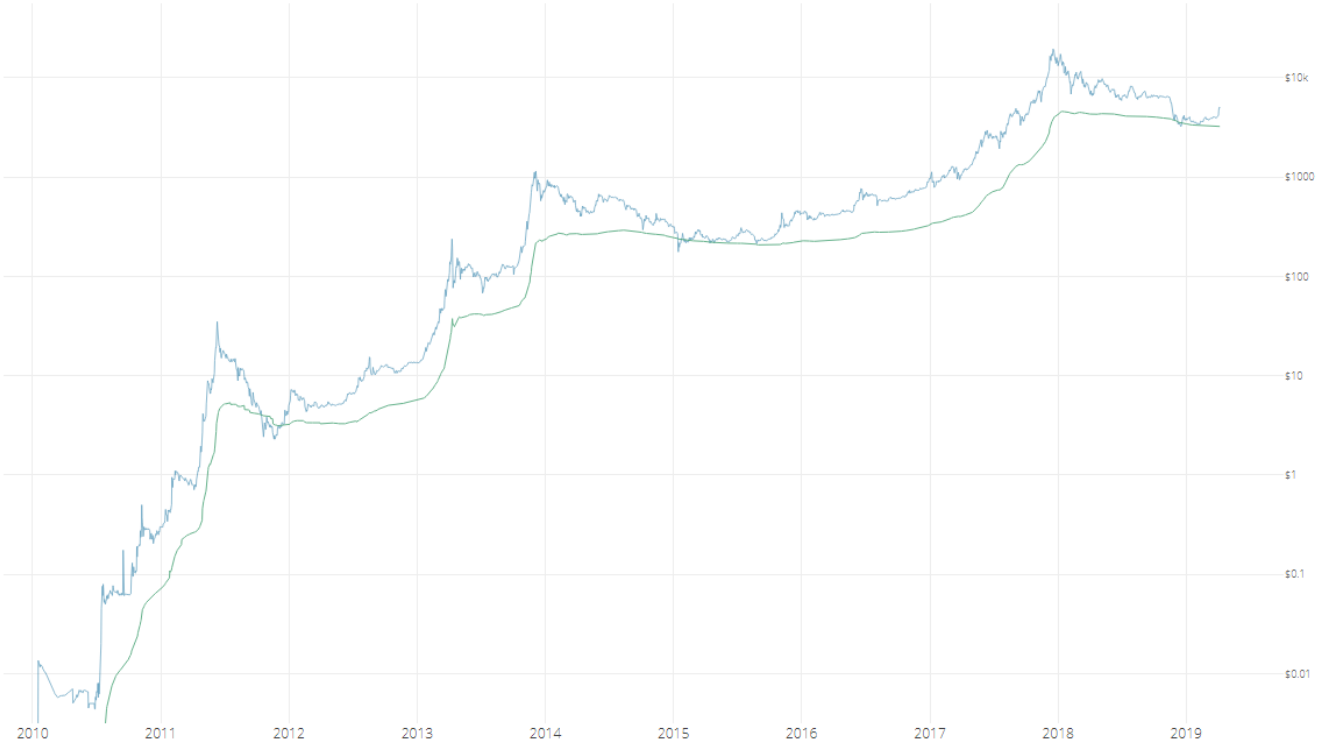
Experiment B: Transferred Price and Balanced Price by David Puell

Instead of using a 6-million figure, transferred price uses supply to bring destruction into the price domain:

$$\boldsymbol{TransferredPrice_{USD}} = \frac{\sum(CoindaysDestroyed \cdot Price_{USD})}{Days \cdot Supply}$$

Looking at this as a life-to-date moving average of spending behavior (again, old hands selling into new hands), it can be assumed that when subtracted from realized price (the average paid for all coins in the market), a "fair" valuation measure emerges. Balanced price denotes the level at which, during bear markets, a full detox has been achieved—market price matching what was paid minus what was spent.

$$\boldsymbol{BalancedPrice_{USD}} = RealizedPrice_{USD} - TransferredPrice_{USD}$$



Balanced price

It goes without saying that this evokes delta price in both calculation and visualization. We believe that delta serves as a technical analysis proxy of balanced price. The former seems to be agile enough to catch exact bottoms—the "wicks"—while the latter catches the full accumulation level prior to the bull run, also defining the brief moment when price remains below it as "capitulation."

More iterations on coindays destroyed to follow. Stay tuned…

Sources

1. *Woobull.com* : Charts and early price data archeology.
2. *Coinmetrics.io* : Realized price data.
3. *Blochchair.com*: Coindays destroyed data. **Authors**
4. Willy Woo, on-chain analytics pioneer @Woobull.com.
5. David Puell, Head of Research @ Adaptive Capital.

Bitcoin is a Weapon

By Hector Rosenkrans

Posted April 11, 2019

One of my most vivid memories from active duty is standing in the middle of the command center on my billion dollar warship, watching a Somali pirate take a piss in grainy infrared. It was around 4AM, I was sipping coffee in dark room lit by a few dozen radar screens, and counting his sleeping colleagues that my team would need to detain at first light.

Through its command of high tech violence, the U.S. Navy can influence anything on, under, above, or near the sea. As a Surface Warfare Officer, my job was the day-to-day maintenance of American hegemony, that power that has ensured free trade and capitalism dominates the global economy. Our closest competitor, China, is at best decades behind.

At the same time, in Iraq and Afghanistan my brothers and sisters were struggling against an enemy who could leverage the power of low tech distributed violence, enabled by the AK-47 and the improvised explosive device. America had forgotten the lessons of Vietnam and was re-learning them in the streets of Fallujah, the Somali pirates were just the latest group to tap into this trend.

The Navy was a practical education in global economics, distributed systems, and high stakes game theory. It taught me that civilization is shaped by the powers that master commerce. Today, that power is the carrier strike group. Tomorrow it will be a Bitcoin node.

The Fleet

Everything you hear about the Navy is true. Sailors like to drink when they hit a port and we aren't overly picky. Yet about halfway through my first deployment I had developed a taste for Newcastle, thanks to the English-style pubs my fellow officers managed to find in every port from Bahrain to Hong Kong. I was literally following in the staggering footsteps of Royal Navy officers who carried the British Empire around the world centuries before. The Brits were never known for their cuisine however, and fortunately most nights ended with a late night stop at McDonalds. In 10,000 years, archeologists will probably use the Super Value Menu as their Rosetta Stone to unlock the mysteries of 21st century language.

Brits do pubs, Americans do burgers, and it's no accident that you can find both in every major port around the world. For a few centuries, the ships flying the Union

Jack let that tiny island mold the entire world in its image. And they weren't the first. Spanish galleons ensured that Catholic missionaries sailed to the Americas, and Aztec gold sailed them back. The lesson is simple – control of the commons means control of the commerce, and there is no greater commons than the high seas.

Naval power lies in its connection to trade. An army can take and hold important resources, but its reach is limited by the constraints of geography. A fleet on the other hand can establish blockades, occupy choke points, and interdict smugglers around the world. It can rapidly project power across time and space, linger indefinitely, and retreat without cost. The British used these tools to build their empire. McDonalds, Apple, Hollywood, and the rest of American-style capitalism ride in the wake of carrier strike groups today.

Vacuums and Violence

On the opposite end of the economic spectrum, the pirates got started as disgruntled fishermen. Somalia's government collapsed in 1991 and the coast guard packed up and went home, leaving the rich local fisheries open for foreign factory trawlers. The stocks were decimated, and the local economies that relied on them collapsed.

In response to this, a few enterprising fishermen realized that while they didn't have fish, there were plenty of guns around. They built a naval militia and would board trawlers to demand payment for the stolen fish. Their plan worked far better than expected, ransom money began pouring in, and the pirates expanded their operations to the narrow commercial shipping packed with ships heading to Europe, Asia, and the Middle East.

Best of all, no one really cared.

The Gulf of Aden runs from the southern tip of the Red Sea to the western Indian Ocean. It connects oil from the Persian Gulf and electronics from Asia to ports on the Black Sea, the Mediterranean, and Europe's Atlantic seaboard. A few million dollar insurance payouts is a drop in the ocean against a quarter of all global trade. Voyage insurance premiums didn't even move until the media picked up the story, and Lloyd's of London realized they could make a quick buck on the attention.

On top of this, the U.S. Navy isn't built for small scale operations. Pirates might get press coverage, but the Pentagon cares a lot more about Chinese submarines and Russian bombers.

Kalashnikovonomics

The real problems started when other groups began to capitalize on Somalia's collapse. Al Qaeda's East African offshoot Al Shabbab was building a foothold in anarchy, and started pressuring the pirates for tribute to boost their own revenue. Ten million dollars of ransom money might not mean much to the global economy, but it will buy a lot of guns for the holy war.

Forget nukes. The AK-47 was the most important weapon of the 20th century and shows no signs of giving up that crown in the 21st. It is rugged, user-friendly, and will kill you just as dead as a stealth bomber.

The reason is straightforward – death is a fixed cost for the individual. Complex weapon systems are expensive to build and difficult to operate. A single bomb might cost $25,000, but that doesn't include the plane that carries it, the larger plane that refuels that plane, the pilots that fly them, the maintenance crews that repair them, the HR department that manages training, payroll, and career advancement. The list keeps going. The U.S. military is extremely capable but not very flexible, and everything costs an arm and a leg.

Rifles on the other hand are cheap, effective, and highly distributed. Anyone with standard issue human equipment can learn to operate one in an afternoon, and basic infantry tactics aren't rocket science. The AK-47 is to warfare what the iPhone is to computers – user friendly power in the hands of the people. This kind of scalability allowed rice farmers and goat herders to defeat the world's two most powerful militaries in the 1970s and 1980s. Vietnam and Russia's war in Afghanistan are classic studies of low-end disruption.

AK = RSA

Cheap and scalable can defeat large and centralized when the conditions are right. Diffe and Hellman took Kalashnikov's ideas to information warfare.

Prior to asymmetric cryptography, the business of secure communications was a massive headache. Key management for large organizations was so complex that it was only practical for massive bureaucracies with an existential need for secrecy. This excluded everyone outside of the military and intelligence services. Even when you have those kinds of resources, security is never guaranteed, just ask Admiral Yamamoto.

RSA changed everything. The simple idea that certain math problems are hard to solve but easy to check (think a jigsaw puzzle) meant that anyone with a computer could communicate securely at a trivial cost.

Of course, a motivated adversary can still hack your laptop if they really want to, most likely by applying a wrench to your skull until you provide your private keys. That

wrench-wielder however needs to be motivated, compensated, and willing and able to keep a secret. They are certainly a threat to any one individual, but at scale the dynamics change. One whistle-blower or viral video and the political benefit of this type of coercion can be swamped by blowback.

Asymmetric Money

Cypherpunks have been building tools for individual liberty, freedom to communicate, and the right to privacy for decades, but the rest of the world moved faster. Netscape and Oracle built the new digital commons, Google and Facebook mastered it. They poured in capital until their product could dominate network choke points, and now any would-be competitor is better off joining their regime than competing. As long as commercial power was in the hands of centralized entities, the digital commons would function much like the maritime commons – dominated by monopolists who had the up-front capital to win early.

The problem for incumbents is that the terrain isn't fixed. Digital scarcity is a tectonic shift for the architecture of the internet, and a potential threat to business models that make their money curating infinite reams data.

Digital commons are like the sea. They move ideas across borders seamlessly, and expose us to the best (and the worst) that the world has to offer. With the rise of Bitcoin, real economic value is beginning to run through these pipes as well. No one can occupy any one position for long. Choke points spring up, flourish briefly, and die out as traffic finds a better route.

Unlike at sea however, the balance of power in the digital realm is shifting to individuals. The power of asymmetric cryptography is similar to asymmetric warfare. State cyber security organizations are incredibly capable and well funded, but like the militaries of the 20th century they cannot match the scale of new technologies with their inherent centralization.

Alfred Thayer Mahan was the naval equivalent of Sun Tzu, and he developed the core idea that the goal of any navy should be to control of the commons. Control of the commons means controlling commerce, and the gears of commerce move the world.

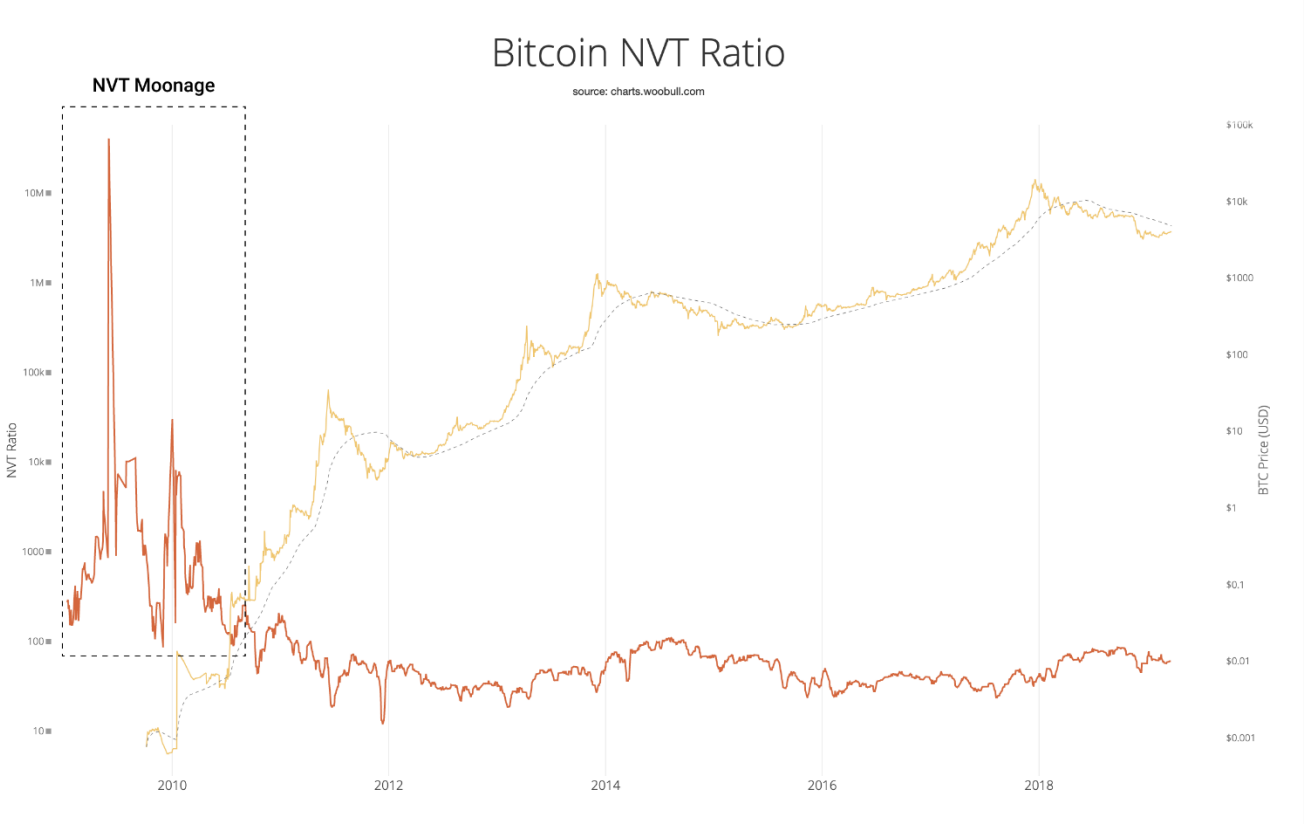
Satoshi built all of humanity a weapon to take that power for ourselves.

When did Bitcoin's investment era begin? A study using NVT

By Willy Woo

Posted April 13, 2019

For those familiar with NVT Ratio, the data from the early years comes off very skewed, sometimes written off as noisy rubbish data.

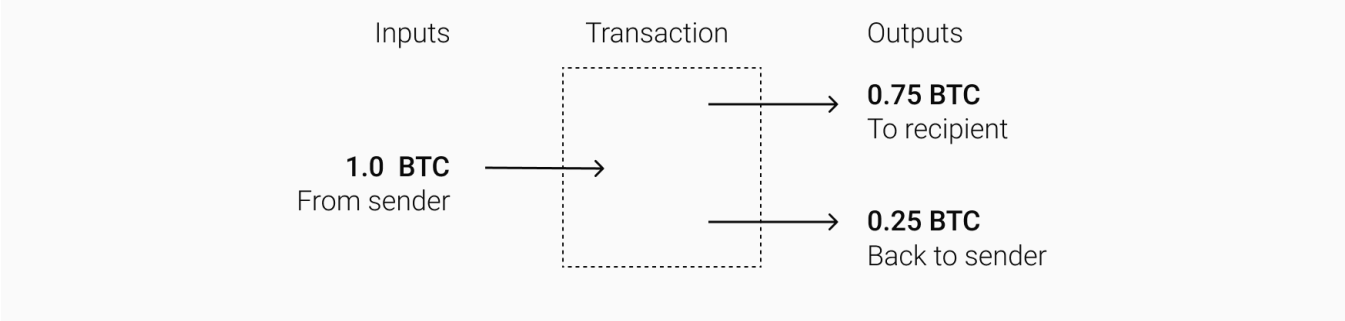


To answer the mystery of early NVT moonage, come with me on a trip down memory lane and visit the transactional data of Bitcoin's early years.

How Bitcoin transactions work

First on our journey we must understand how a Bitcoin transactions work...

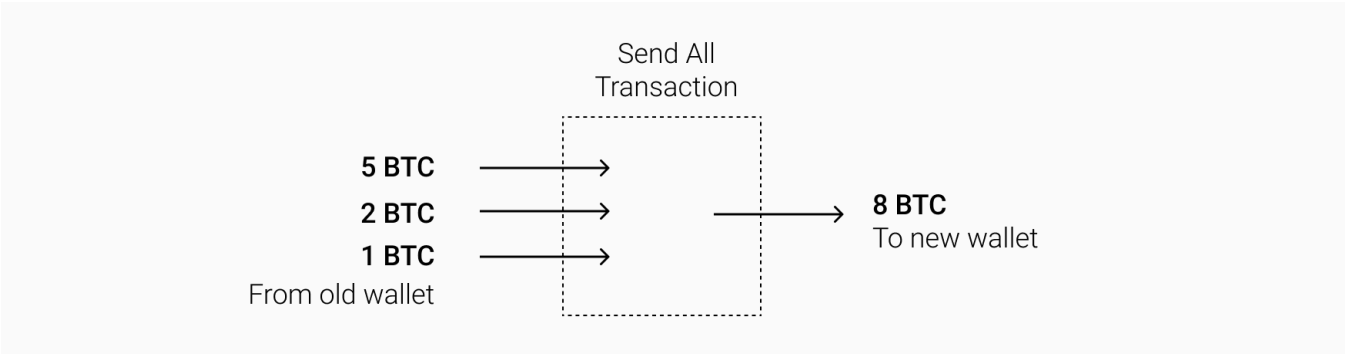
All transactions on the network consists of shards of BTC value (called UXTOs) moving between wallets. This is what a typical transaction might look like...



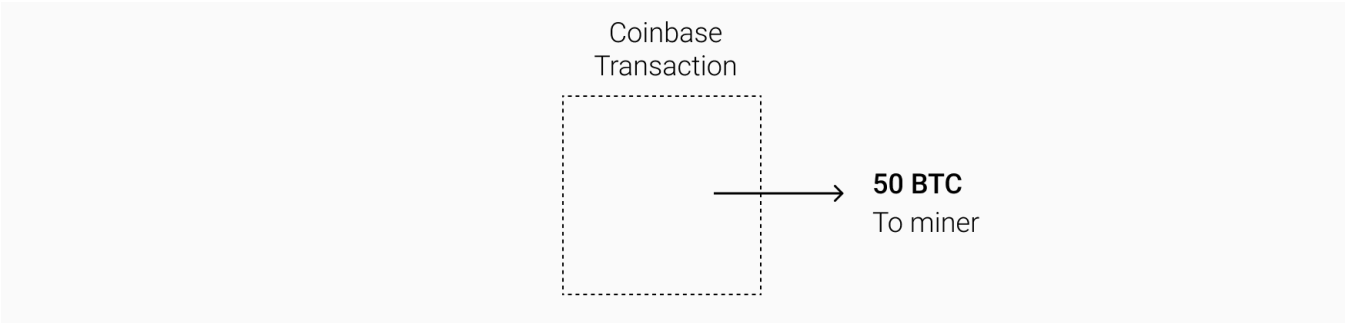
In this example, a 0.75BTC shard was sent to a recipient, and importantly there was a new 0.25BTC shard returning to the sender as the change from the transaction. In this common example the transaction had two output shards.

When sending to others we usually see 2 or more outputs due to the change output returning. (Sometimes there are a multitude of outputs, especially if payments are made to many recipients in the same transaction, Bitcoin exchanges like to do this for efficiency.)

Another common thing we do is cleaning out a wallet, sending all coins to a new wallet. This is a common example of a single output transaction.



Now here's a special case...

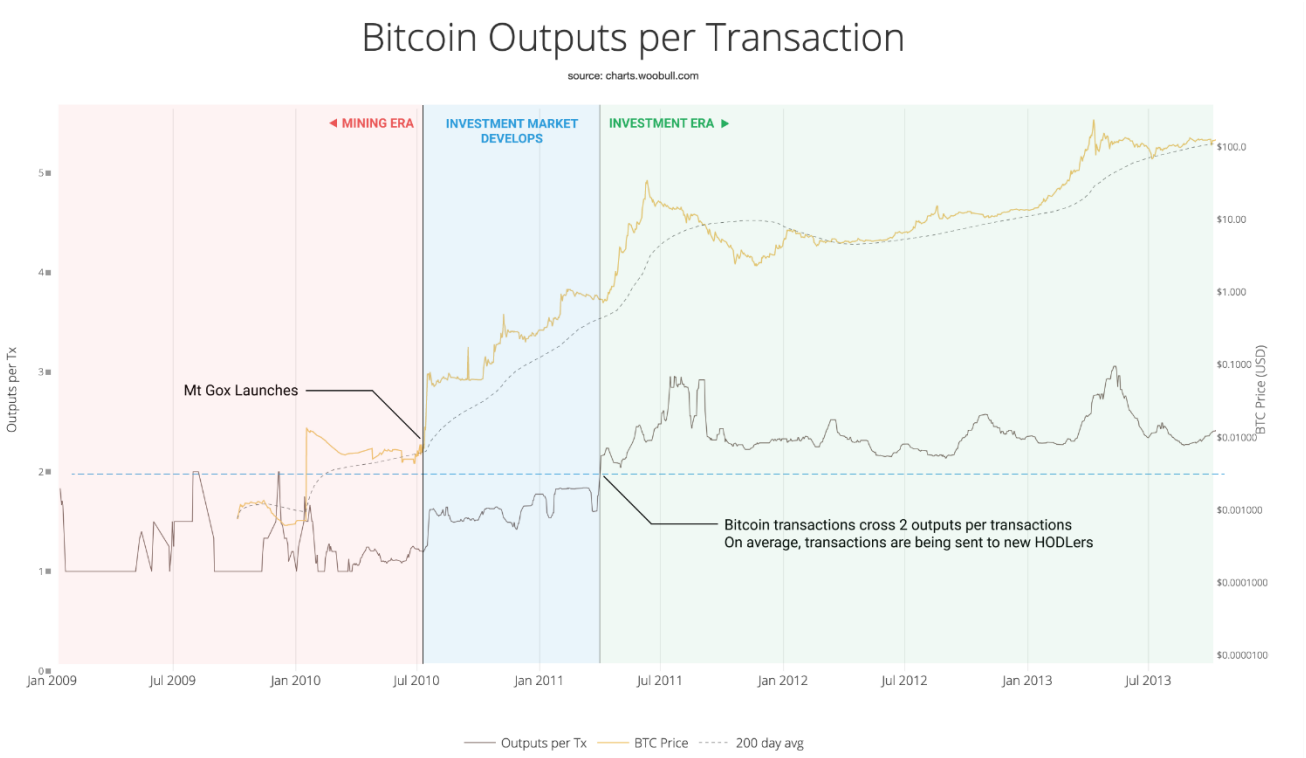


This transaction has no inputs, and one output. This happens when a new coin is mined into existence, we call this a **coinbase transaction** .

Great, after that primer we we can revisit Bitcoin, the early years...

The early investment market

In the early era, the network was dominated by mining. Coins were either mined straight into wallets and held, or moved from one wallet to another. We can see this because the average outputs hovered around 1.



On 5th October 2009, a website called New Liberty Standard started pricing bitcoins using the price of electricity it took to mine them. This was the first time Bitcoin had a daily price.

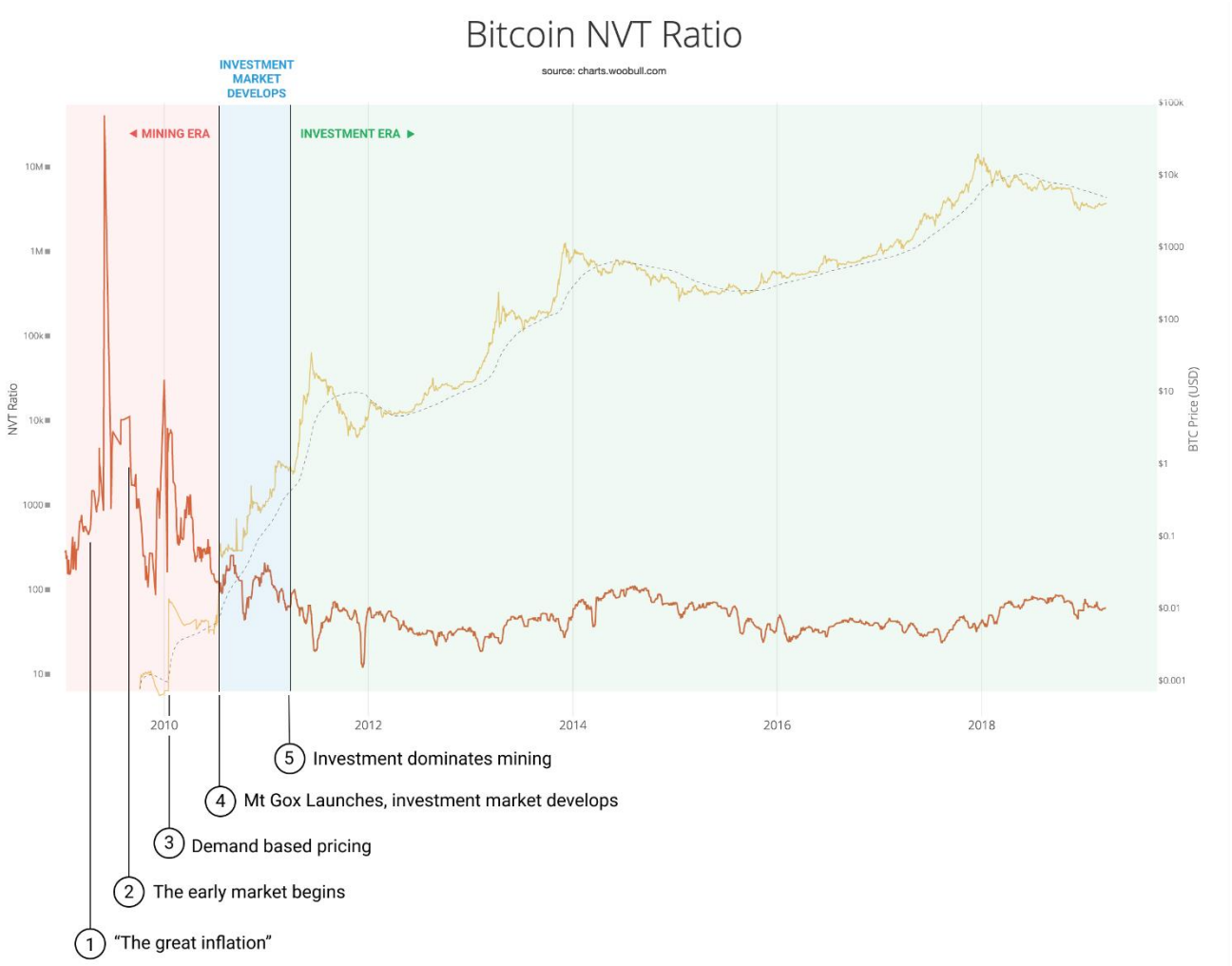
By 16th January 2010, New Liberty Standard started pricing according to buy and sell demand, and the price jumped 19x from 0.07 cents to 1.3 cents.

On 25th May 2010, a second market opened called Bitcoin Market. It also traded according to buy and sell demand. (Its first day of trade had a close price of 0.3 cents with a volume of 1000 BTC, that's $3 of trade volume.)

The third exchange to open was the infamous MtGox, launching one month later in July 2010. It's here we see the price leap again, and the average outputs per transactions start to climb towards 2, this is where the early investment market starts to develop. Average outputs climbing to 2 was the telltale sign that transactions between investors were outnumbering those from mining.

Breaking down the early market under the lens of NVT

Now we can move onto the NVT domain and look at the actions the market took in its early history. Here's the NVT Ratio chart using the latest volume estimates from [Coin Metrics](#) Pro.



Breaking this down:

1. **The Great Inflation**. This is the period where the sheer volume of new coins arriving via coinbase transactions meant the value flowing on the blockchain was high in comparison to the money supply. (NVT Ratio by definition is the ratio of the money supply to the coins flowing on-chain). As the money supply increased the impact of the coinbase transactions got diluted and you can see the NVT Ratio climbing steeply as the ratio of money supply outstrips the new coins moving into existence.
2. **The early market begins**. In June 2009 interestingly before even the first prices of BTC was published by New Liberty Standard, we see activity between

different HODLers, likely OTC trades. Enough coins move on-chain to bring NVT Ratio downwards over time, we can also confirm this as a blip on the outputs per transaction chart further above. (One could suggest this was also testing by early supporters of the network, but the volumes and time period of sustained activity look too consistent and high for this to be a viable reason in my opinion).

3. **Demand based pricing**. When New Liberty Standard introduces their demand based pricing we see an immediate increase in NVT, the flows of coins between HODLers dry up as price jumps 19x. We also see the market adapt to the new prices and on-chain flows between investors start to increase again, we see NVT dropping.
4. **MtGox launches**. With the advent of MtGox which immediately became popular, we see further drives of on-chain volume (as a percentage to the supply) to the normal zone we typically see in the Bitcoin investment era.
5. **Investment dominates mining**. As early as April 2011, investment flows mature into the same kind of ratios we see today. NVT comes into the normal band which we've seen for the last 8 years.

How to scale Bitcoin (without changing a thing)

Why Bitcoin banks need to prove their solvency

By Nic Carter

Posted April 14, 2019

Almost from inception, the "scaling debate" in Bitcoin, and cryptocurrency more generally, has been framed in what could be called Hegelian terms.

- **Thesis**: peer-to-peer cryptocurrencies are useful for online commerce
- **Antithesis**: online commerce requires millions of transactions a day
- **Synthesis**: to succeed, cryptocurrencies must scale

This has been the default backdrop for discourse in the industry and the onlooker press for the better part of the last decade. In this piece I'll posit that this obsession, which has driven discourse in Bitcoin land for the better part of a decade, misses the point, and I'll suggest an alternative framing. I believe that *institutional scaling* presents an under-appreciated scaling vector, and it is quite possible to employ it without significantly compromising Bitcoin's assurances.

By this I mean the Finneyan view of Bitcoin in which Bitcoin banks emerge and issue notes against deposited Bitcoin. If you look carefully, a proto version of this system is in place today. However, for cherished assurances like scarcity to be upheld, exchanges and custodians need to start making routine attestations that their reserves match their liabilities.

Before we start, a tiny literature review (optional):

- Spencer Bogart on Bitcoin's strong assurances
- Hasu on how Bitcoin supports non-state property rights
- Yours truly on the quality of Bitcoin's touted assurances
- Jameson Lopp on the exact technical guarantees and near-guarantees that PoW gives you
- Davidson, De Filippi, and Potts on how public blockchains are a new type of institutional technology
- Saifedean Ammous on how Bitcoin could function solely as a settlement network

Prescience on the mailing list

The very first public comment on Satoshi's white paper, coming as a response on the cryptography mailing list five hours after publication, was this astute observation from James A. Donald:

If hundreds of millions of people are doing transactions, that is a lot of bandwidth—each must know all, or a substantial part thereof.

What James understood is something that has escaped many who scampered down terabyte-block rabbit holes: Bitcoin only works because anyone can retain a copy of the ledger and stay in sync. If you make syncing with the current state of the ledger

too expensive, only a privileged few can stay up to date, effectively adding a hierarchy to a system which must be flat to function.

Satoshi's answer to this question, interestingly, involved SPV proofs, which, bathed in a present-day epistemic light, appears somewhat naive. SPV proofs ostensibly allow a non-full node to know that a transaction has been included in Bitcoin without downloading the whole chain. Casually invoking SPV proofs as the solution to scaling is a bit like the scientists behind the Apollo program remarking: "Oh, a trip to Alpha Centauri? Just the simple matter of faster than light travel."

Suffice to say, SPV proofs have been virtually abandoned as a viable scaling method today. Under a variety of scenarios, they tend to collapse into users having to validate the entire chain anyway.

James was spot on. He immediately understood that Bitcoin was a single ledger which all of the nodes in the network had to continuously reaffirm at 10 minute intervals. Since everyone had to see everything, hundreds of millions of transactors would simply overwhelm the system.

But what if this teleological premise—*Bitcoin is for global, online, peer-to-peer commerce at the individual level*—was flawed? Enter Hal Finney.

Stairway atop Diana's Peak, St Helena

Hal's vision

In 2010, digital cash pioneer Hal Finney famously made the case for what could be called the institutional approach to scaling Bitcoin.

Actually there is a very good reason for Bitcoin-backed banks to exist, issuing their own digital cash currency, redeemable for bitcoins. Bitcoin itself cannot scale to have every single financial transaction in the world be broadcast to everyone and included in the block chain. There needs to be a secondary level of payment systems which is lighter weight and more efficient. Likewise, the time needed for Bitcoin transactions to finalize will be impractical for medium to large value purchases. Bitcoin backed banks will solve these problems. They can work like banks did before nationalization of currency. Different banks can have different policies, some more aggressive, some more conservative. Some would be fractional reserve while others may be 100% Bitcoin backed. Interest rates may vary. Cash from some banks may trade at a discount to that from others.

In a brilliant stroke of foresight, Hal understood that base layer Bitcoin would never scale to the desired level in its current format. (Unfortunately, many Bitcoin evangelists failed to understand this, and their misapprehensions led to the bitter blocksize wars of 2015–17.) In Hal's view, Bitcoin would be a high-powered money mediating large settlements between financial institutions, rather than a payment token used for the online equivalent of petty cash payments. He realized that Bitcoin's rather slow settlement times (compared to physical cash or credit cards) combined with the inefficiency of the chain itself meant that directing Bitcoin to the brick-and-mortar payments use case was a square peg in a round hole.

What Hal envisioned was a system where banks could be auditable, transparent in their capital ratios, and accountable. A free market for reserve/capital ratios could even develop, as depositors would be able to select banks with varying levels of reserves to suit their risk preference.

Undercapitalized banks might fail—but this would be a healthy market signal, a culling of weaker entities to render the herd stronger overall. Compare this to the system that became unraveled in 2008/09: financial institutions heaping on leverage, knowing that they would be bailed out if something went wrong. Since the government made it clear that it would not allow banks to fail, the market was robbed of that valuable feedback mechanism and risk became increasingly abstracted, obscure, and hidden.

In the words of Elaine Ou:

Financial institutions make people feel safe by hiding risk behind layers of complexity. Crypto brings risk front and center and brags about it on the internet.

In finance, risk never truly disappears, even if hidden—and suppressing it often has the nasty effect of unleashing it in a more dramatic fashion later on.

Just as risk crept up on us, unheralded, and financial institutions failed one after the next in a cascade of toxic balance sheets in 2009, so too will the long-suppressed forces of systemic risk unleash themselves when our present monetary experiment finally unwinds.

Can Bitcoin mollify this? Perhaps not. But its very structure facilitates the creation of an alternative financial system which is far more transparent and open about risk than the present one. This is the Finneyan view of Bitcoin: Bitcoin as a virtual commodity sitting in provable reserves in financial institutions. No one's liability, a provable virtual commodity which a bank can rely on to attest to its viability.

Winding road through Glencoe, Scotland.

Scaling assurances

Let's briefly revisit what we mean by scaling, anyway. It's clear by now that simply opening up the block space throttle doesn't work. This is because Bitcoin is designed to be auditable, and auditing the blockchain requires the full, unabridged ledger.

Fundamentally, Bitcoin relies on everyone being aware of every transaction. Can this be scaled without compromising this core feature? Let's see how the major classes of scaling innovation fare under this lens:

1. **Deferred settlement/reconciliation**(chiefly lightning). What lightning and other defer-reconcile models of transacting do is grant users the ability to create relationships which are then settled at a later date. The chain's assurances are still present and available, they just aren't employed for each transfer. These models do however trade off by (temporarily) weakening assurances—final settlement is no longer instant and you have to be online to receive a payment, for instance.
2. **Database model** (massive base layer scaling). As mentioned, simply increasing the ledger size compromises the assurances of the blockchain—not everyone is able to maintain the ledger. There may be a way to do this in a trust-minimized way with SPV and fraud proofs, but we haven't found it yet.
3. **Extending assurances to other chains** (sidechain, security inheritance, merged mining). This model blesses other block space with Bitcoin's security or extends Bitcoin's own block space. Merged mined coins like Namecoin, proof-of-proof approaches like Veriblock, and sidechains like Rootstock are all roughly in the same family of approaches to the problem. These represent a compelling potential avenue to scaling, as they extend Bitcoin's settlement guarantees to a potentially unbounded block space, but it is still under explored. However, assurance impairment is possible—risks remain that miners might censor sidechain closures or otherwise interfere with the sidechain. The productized implementations that we've seen like Liquid have used consortia rather than relying on PoW.
4. **Trust-minimized institutions**. This approach takes the assurances of Bitcoin—natively auditable, scarce digital cash—and applies them in the context of a depository institution. In short, rather than individual users being the clients of Bitcoin, institutions like exchanges, banks, and custodians adopt the end user role, with their own users indirectly benefiting from Bitcoin's assurances. Trade offs remain, and some features of Bitcoin don't apply in a custodial context, but if protocols like Proof of Solvency are implemented, some of Bitcoin's guarantees can shine through, even if filtered through an intermediary.

What should Bitcoin banks look like?

Is Hal's vision of a world of banks backed by Bitcoin plausible? In one sense, it's the world we have today, as many users only touch Bitcoin indirectly, through custodians and intermediaries. While most exchanges are presumed to be full-reserve, and indeed generally claim to be, in practice this isn't universally the case. It's becoming clear, for instance, that QuadrigaCX was running a fractional reserve for most of its existence. I don't need to recap the sordid history of malfeasance and negligence at cryptocurrency exchanges.

Something as simple as a Proof of Solvency protocol would have made the Quadriga situation evident long before it folded. Rather, what would have happened in practice (imagine a world where solvency attestations were universal among

exchanges) is that Quadriga would have refused to prove their reserves, and would have rightly come under suspicion, pre-emptively saving users a lot of heartache and lost coins.

Scaling the base layer. Rockport MA.

An ideal Bitcoin bank would employ schemas like Proofs of Solvency to *pass through Bitcoin's assurances to depositors*. Of course, these aren't faultless, and can be cheated, but it's a high bar to clear. You *can* lie to your auditors if you're a publicly traded company, but you'll likely be found out at some point, and now you've broken the law. Any serious Bitcoin bank engaging in an audit would likely only do so if they felt that they were going to pass it. As mentioned above, if this became popular, it would segment the Bitcoin depository industry into reputable, trusted banks which

routinely proved reserves, and untrusted banks held in suspicion due to their unwillingness to provide these audits.

To be clear: I am not denying that IOUs circulating within and among banks generally fail to instantiate the properties of Bitcoin. What I am suggesting is a way to make those IOUs more Bitcoin-like, by providing depositors with certain assurances.

Selected Bitcoin properties by usage method

Property	Bearer asset nature	Permissionlessness	Scarcity	Programmability	Verifiability
Definition	*The holder is presumed to be the owner; ownership is not beholden to a third party*	*Users can transact without asking permission of any third party*	*Only 21 million units will exist; no third party can alter the rate of production*	*Basic conditional contracts can be created*	*Users can verify that the core protocol rules are not being violated*
Strength					
Base layer Bitcoin	Strong; the Bitcoin protocol treats anyone with a key to unlock a UTXOs as the owner	Strong; base-layer Bitcoin does not require permission to send or receive	Strong; PoW ensures that the creation schedule is adhered to	Limited programmability with script: multisig, HTLC's	Strong; full validation allows a user to verify the correctness of the entire chain
Lightning-held Bitcoin	Strong w/ caveats; Bitcoin in channels is encumbered but ultimately available	Non-custodial LN users can transact permissionlessly	Strong; LN cannot be used to create new Bitcoin	Vastly enhanced programmability, still featuring bitcoin assurances	Strong albeit requiring more active monitoring
Exchange-held Bitcoin	Weak. Redemption required to obtain genuine Bitcoin	Virtually absent. Permission is required to operate	Can be impaired; fractional reserves can temporarily inflate BTC supply	Limited programmability, lacks the assurances of Bitcoin	No verifiability
Exchange held-Bitcoin + Proof of Solvency	Weak, although depositors can trust that liabilities can be met	Still absent as above	Strong; given a credible solvency protocol, users can be assured that deposits are as claimed	Limited programmability	Some verifiability regarding no inflation possible; albeit less than running a full node

This table demonstrates that, while Lightning and other on- or near-chain layered approaches expand Bitcoin's assurances to other domains, exchanges with proofs of solvency can chip in as well. Sidechains (if they ever get figured out) and Lightning are not mutually exclusive with the proposed institutional model: I envision them as parallel and complimentary approaches to scaling Bitcoin. The important thing to note is how little an IOU at a non-proof-of-reserve exchange means. It is very remote from base-layer Bitcoin.

Something else which is worth calling out: Lightning and other L2 approaches may well become mainstream approaches to scaling, but they do so *under a different set of assurances*. The assumptions that hold in Bitcoin are different in Lightning! There is nothing inherently wrong with this—and Lightning enthusiasts and developers will admit this—but they aren't *quite* as ironclad as the settlement assurances that vanilla Bitcoin gives you. So the precedent that Bitcoin scales under various alternate tradeoffs is well-established, and should be generalized to institutions as well.

Credit creation on Bitcoin

Many Bitcoiners will recoil in horror at the words “fractional reserve,” even though they were uttered by Satoshi’s first disciple himself, Hal Finney. However, I believe that the risk of fractional reserves can be managed, **if they are accountable to the free market**and **if the banks are transparent about their actual reserves.**

The problem with exchanges running fractional reserves is not, I’d argue, that they fail to operate at full reserve, but that they *misrepresent their risk to depositors*. While this is a heated debate among Austrian economists, I personally support a free market for user deposits, with exchanges running at various reserve or capital ratios.

The important thing is that they are transparent about it, so that users can adequately assess the risk of insolvency. As we well know, full reserves are not required for a bank to operate in practice, as users do not typically redeem all of their deposits at once. In the US, for instance, larger depository institutions must maintain a reserve equal to at least 10% of reservable liabilities. For a history of reserve requirements in the US, see this article by the Fed. I don’t know what the right number is in Bitcoinland, but I believe in the market’s ability to find that number. It’s evident by the popularity of lending facilities like BlockFi that some users will prefer interest-bearing accounts, and as such will tolerate some more risk at their bank.

Robust to external shocks: Bova's bakery. Boston, MA.

What do proofs of solvency actually prove?

So far I've been treating proofs of solvency/reserve as largely homogenous, which does them a disservice. In fact, I should be more precise about the nomenclature. A proof of reserve involves proving **what you actually own,**and it is generally meaningless without a corresponding proof of liability, which is a proof of **what you claim you owe**. Together, if executed correctly, they can serve as a conditional proof of solvency.

Proof of Reserve	+	Proof of Liability	=	Proof of Solvency
You own what you say you own		*You owe what you say you owe*		*Your reserves match your liabilities*

The first method to prove solvency was formalized Greg Maxwell and Peter Todd, which we'll call the **Merkle approach.**Presented at length here by Zak Wilcox, the

Merkle approach allows users of the exchange to verify that their balance is included in the list of all customer balances that the exchange publishes in their attestation. There are two parts to the process, proving what you owe, and demonstrating what you own. As described by Greg Maxwell:

```
<@gmaxwell> First you show how much funds you have via signmessage for actual coins
on the chain. Thats easy enough.

Then you need to prove how much you should have. This is a little tricker. You
could just publish EVERYONE's balances e.g.  by          account ID but thats
undesirable for privacy and commercial reasons.
```

Proving reserves is actually the easy part—the exchange signs a transaction with all of their UTXOs. Everyone can now see that the exchange owns x BTC. Of course, the exchange can borrow Bitcoins for this. This is why the attestation only works on an ongoing basis, and should be paired with an analysis of cash flows (imagine an exchange that habitually borrowed 10,000 BTC every quarter, the week before their solvency attestation, and paid it back the next day!)

The challenging part is proving what you owe—that is, what your liabilities are to depositors. This is where the Merkle tree comes in—it allows users to verify that their accounts and balances are included in the final hash without leaking the details of everyone's balances and account information. Like herd immunity, users can have relatively strong assurances that the exchange is not lying if a sufficient number of them verify their balance.

A malicious exchange can of course cheat by publishing 0 balances for dormant accounts that they expect not to perform the check; but they run a big risk in doing this—if even one of the zeroed accounts makes the check, the exchange is exposed.

As Zak says, the Merkle approach

[...] gives you the means to check your own belief of the exchange's liability/obligation to you is included in their publicly declared one, and to let you make an informed decision about whether to continue doing business with them if those numbers differ.

Steven Roose of Blockstream has formalized the proof of reserve portion of the process with a BIP and a Github implementation. This should be paired either with the proof of liabilities (as described above) or a credible auditor.

The problem with the Merkle approach is that it makes public the exchange's liability, which many exchanges may not want to do. Thus in 2015 Dagher, Bunz, Bonneau, Clark and Boneh published *Provisions: Privacy-preserving proofs of solvency for Bitcoin exchanges* . Addressing the shortcomings in the Merkle approach, Dagher et al set out in *Provisions* to:

[E]nable an exchange E to publicly prove that it owns enough bitcoin to cover all its customers' balances such that (1) all customer accounts remain fully confidential, (2) no account contains a negative balance, (3) the exchange does not reveal its total liabilities or total assets, and (4) the exchange does not reveal its Bitcoin addresses.

Provisions consists of three protocols:

- Proof of assets (/reserves): the exchange uses some ZKP trickery to prove that it owns a certain number of BTC, without revealing that number (read the paper for more detail)
- Proof of liability: the exchange commits to the total sum of user balances, also allowing depositors to privately verify that the exchange is committing to the right balance
- Proof of solvency: the exchange proves in zero knowledge that the proof of assets and liability sum to 0

This is an improvement over the Merkle + signmessage approach, as it doesn't leak the exchange's balance, instead outputting a simple 1 or 0—the exchange is solvent or not.

Other work on the topic that I wont summarize includes:

- Decker, Guthrie, Seidel, Wattenhofer (2015),*Making Bitcoin Exchanges Transparent*
- Mohan and Devi (2017),*Privacy Preserving Non-interactive Proof of Assets for Bitcoin Exchanges*
- Narula, Vasquez, Virza (2018),*zkLedger: Privacy-Preserving Auditing for Distributed Ledgers*

In short, between the Merkle approach, and the various ZKP approaches that have been proposed, copious tools exist to enable Bitcoin banks to prove their solvency. Today, they have little reason not to.

Where are the Bitcoin banks?

So if Finney's Bitcoin banks can help scale Bitcoin, where are they? The large exchanges and custodians (I'm using exchanges, custodians, and other depository institutions that take Bitcoins interchangeably with 'banks' here) are just another set of trusted third parties. As the gatekeepers to Bitcoin, they often do more harm than good, impairing open access and free exit.

Ok, so the title was a slight exaggeration. Coinbase-BTC-IOUs and Bitfinex-BTC-IOUs and Xapo-BTC-IOUs don't grant users the same transactional assurances as raw, commodity Bitcoin, but they still represent an under-appreciated scaling vector.

Those who have professed their belief in institutional scaling include Xapo CEO, Wences Casares:

We have a lot of transactions that happen within Xapo. Because the Xapo to Xapo transactions don't need to go through the blockchain so they don't. They can happen in real time and for free. So today we see about 20 Xapo to Xapo transactions for every transaction that we run through the blockchain.

It's easy to see how a bitcoin bank could issue actual notes against deposits, serving as the pegs in a sidechain. For it to be credible though, you need redeemability. This is the same issue that Tether faced—for a time, no one believed that they could actually redeem USDT. Ongoing attestations to reserves would help with this.

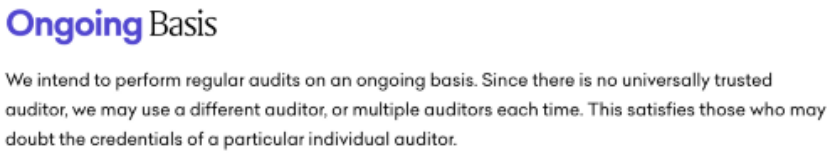
As stated, a proof of reserve audit allows a depository institution to prove that they hold a certain amount in reserve, which would then—with the help of a trusted auditor—be used to demonstrate that their liabilities matched their reserves.

Alternatively, you can let users determine that internal balances exist to match their own deposits; if enough users do this, you can have reasonably strong assurances that the exchange is solvent. It should be noted that proofs of reserves are by no means a silver bullet. Coindesk's Danny Bradbury notes that both Bitcoin reserves and fiat operations should be proven, and that snapshots are far inferior to an ongoing reserve proof.

Historically, many exchanges have conducted proofs of reserves. These appear to have mostly been catalyzed by the Mt Gox insolvency. Interestingly, the history of proofs of reserves is mostly one of broken promises. Several exchanges have deleted any trace of their previous proof of reserves attestations and others have backtracked on promises to perform proofs of reserves on an ongoing basis.

- June 2011: Mark Karpeles constructs a crude proof of solvency with the famous 424,242 BTC transaction
- February 2014: Coinkite posts a now-deleted proof of reserve audit
- February 2014: in the wake of the Gox insolvency, executives at Coinbase, Kraken, Bitstamp, BTC China, Blockchain.info, and Circle publish a joint statement promising audits and more transparency. Only Kraken and Bitstamp prove reserves, and none on an ongoing basis
- February 2014: Coinbase summons Andreas Antonopoulos to review their storage practices, although he does not conduct a formal review. He subsequently deletes his blog about it
- March 2014: Bitstamp publishes an outside attestation as to their solvency, in the process creating the largest transaction in history (at the time)

- March 2014: Kraken proves reserves using the merkle approach,claiming that they "intend to perform regular audits on an ongoing basis." They do not.



Ongoing Basis

We intend to perform regular audits on an ongoing basis. Since there is no universally trusted auditor, we may use a different auditor, or multiple auditors each time. This satisfies those who may doubt the credentials of a particular individual auditor.

- April 2014: British exchange Coinfloor issues their first provable solvency report. Unlike every other Bitcoin exchange in existence, they follow it up with another report the following next month. And again. And again. Last month, they published their 60th report, far more than every other exchange combined.
- August 2014: Stefan Thomas announces that he has completed a successful proof of reserve audit for OKCoin. However, in a now-deleted reddit post, the outgoing OKCoin CTO subsequently claims that OKCoin misled Thomas and partially faked the audit. A CCN article entitled "OKCoin passes proof of reserve audit" is also later deleted

I can confirm OKCoin removed a number of accounts (used by OKCoin bots) to pass the Proof-of-Reserve audit in Aug 2014. In essence, these bots trade on fractional (or fictional) reserves. Stephan Thomas was lied to during the audit. This is an unfortunate limitation of the proof-of-reserves method.

- August 2014: Huobi releases a proof of reserve audit administered by Stefan Thomas
- June 2015: Bitfinex issues a press release stating that, using Bitgo's multisig software, they will rid themselves of their omnibus model and store user coins in segregated accounts, so that depositors could verify their holdings on-chain in real time. In August 2016, Bitfinex is hacked to the tune of of 119k BTC and they abandon the segregated multisig method. Bitfinex subsequently publishes BTC, EOS, and ETH coldwallet addresses for public scrutiny
- November 2018: Tether issues a quasi-proof of reserves; their banking partner Deltec Bank and Trust Limited attests to their cash balance. This matches the amount of Tethers in circulation, although skeptics aren't quite satisfied

 *Waiting for exchanges to follow up on initial proofs of reserves*

One commonality emerges: exchanges and depository institutions tend only to issue attestations or proofs of reserve under extreme duress. The flurry of activity in 2014 was precipitated by the Gox insolvency. Despite claims that proofs of reserves would become enduring and routine processes at these exchanges, not one has honored that promise aside from Coinfloor.

Perhaps things are changing. New depository institutions like Fidelity Digital Assets, Square Crypto, Bakkt, and ErisX are entering the market, several of which have announced their intention to be more accountable to Bitcoin users. As regulators become more sophisticated, it doesn't seem inconceivable that they might one day expect cryptographic audits from Bitcoin banks. Now that QuadrigaCX is being exposed as not an accidental key loss but an actual insolvency and potential fraud, 2019 might be an opportune time for some of these exchanges to revisit their proof of reserve protocols. If they don't, the new breed may well eat their lunch.

Conclusion

Bitcoin is an institutional technology, a nation state without an army. Perhaps instead of trying to force it into a mold that ill-suits it, we should instead try to reckon with its present reality. Yes, a messy patchwork of custodians and banks has

emerged, many of them taking a devil-may-care attitude to user deposits. Over a billion dollars have been stolen or misappropriated from these honeypots.

How, realistically, can this state of affairs be amended to suit Bitcoin's nature? Despite a refrain of "not your keys, not your coins," the Bitcoin banks are here to stay: the convenience tradeoff is simply too compelling. What if we acknowledge that they will persist as long as they perform a useful service, and focus instead of bringing Bitcoin's assurances to them?

Ten years on, Bitcoin has entered its adolescence. Perhaps by seeing it for what it is—a peculiar beast, suitable for a narrow set of things—it can become more comfortable in its own skin. By adding institutions to the set of entities accountable to Bitcoin's innate transparency, we can radically improve the state of affairs in Bitcoin's depository industry today.

Objections

Bitcoin Banks are inherently incompatible with Bitcoin

There is a somewhat nihilistic view present in Bitcoinland which starkly denies the importance of exchanges and custodians, as if they didn't exist. This is often born, in my opinion, of a nostalgia for the 2010–12 era when the network was genuinely quite flat and non-hierarchical. Of course, you can't inhibit free enterprise and commerce, and smart entrepreneurs decided to create useful services of exchange, custody, and banking for bitcoiners.

Far from being a dark irony, as most pundits maintain, I think this is a perfectly natural evolution. Banks are now a meaningful portion of our network, and we have to live with that. Yes, running a node to verify incoming payments matters, but factually, some nodes matter more than others. In particular, exchange nodes, the nodes powering block explorers, blockchain API companies, merchant services, and one day, big lightning hubs. There's nothing wrong with this, and it doesn't compromise Bitcoin.

It is fashionable to declare *not your keys, not your bitcoin*, and while absolutely true, this also misses the point. What do we do about the people that have decided to surrender their keys in exchange for IOUs at a bank? Do we smugly deride them for being unwilling to self-custody (still not intuitive for most normal people)? Or do we empathize with them, and try and ameliorate their situation by holding exchanges accountable? I strongly suggest we do the latter .

Why would anyone start proving reserves now, given that it's so out of favor?

There is a perverse feature of the cryptocurrency industry that could be referred to as the paradox of transparency. Put simply, the more transparent you are, the more attack surface you open up, and the more opportunity your critics have to undermine you. As a consequence, being open and transparent is disincentivized. Since this industry has been lightly regulated so far, most successful projects are highly obscure in their operation. There is no equivalent of a 10-K for established projects or an S1 for new token launches.

The same goes for Bitcoin depository institutions: they are regulated under a vague patchwork of regimes with no domain-specific regulation in place (in the US at least). Against this backdrop, it is often advantageous to them to disclose as little as possible about their operations. Additionally, proofs of reserves are costly; and in the lasts three years exchanges have not sought to differentiate themselves on credibility but rather liquidity and number of listings.

I believe that there are several catalysts for exchanges to start proving reserves:

- The growth of SROs. Absent any new legislation or more activist regulators, self-regulatory organizations may come to play a larger role in the US and other developed nations. Japan leads the way already. SROs will need to advocate to their national governments that they are imposing standards on exchanges, and asking member organizations to prove solvency is an easy (and not overly onerous) carrot.
- The extended fallout from QuadrigaCX. The full details from the scandal have not yet been revealed, but it is increasingly likely that it was not a case of misplaced keys. Forensic evidence is pointing to a deliberate, years-long fractional reserve. This kind of deception is unprecedented in Bitcoin; in Gox, the exchange was hacked rather than deliberately stealing funds from depositors.
- A bifurcation into grey/black market and compliant exchanges. A split is coming where a set of sophisticated, regulator-friendly exchanges emerge make a clean break from the underclass of unregulated exchanges.This new cohort will seek to differentiate themselves, not on the basis of the number of tokens traded, but in terms of credibility and security. Introducing audits which include proofs of reserve will be a natural source of differentiation.

Fractional reserves at banks permanently destroy the value proposition of Bitcoin

There is a common misconception that a Bitcoin bank running a fractional reserve permanently impairs Bitcoin's assurances. For sure, a fractional reserve at a bank

inflates the supply of credit (loosely, money) for the period that it persists. QuadrigaCX did exactly this: they didn't have sufficient reserves, and they *covertly* increased the supply of Bitcoin, if you include Bitcoin IOUs in your assessment of Bitcoin's supply.

However, covert fractional reserves are unsustainable—they typically get found out, as happened with Gox, and Quadriga, etc. When this happens, the Bitcoin credit supply shrinks as the fraud is uncovered and those IOUs lose their convertability. Fractional reserves are leveraging, and their discovery is a deleveraging. So the covert inflation of the money supply only occurs while that covert fractional reserve is running. The largest banks—Coinbase, Bitfinex, etc—have a strong incentive not to misrepresent their solvency, because they have reputations to uphold, and executives face jail time if they do. And as this industry matures and more regulated banks come to account for a larger fraction of the market, most funds under custody will settle with the most responsible banks.

Fractional reserves are inherently bad/evil

This is more of a philosophical position than one that can be settled empirically. I happen to believe that non-full-reserve banking on Bitcoin is inevitable, and since it is inevitable, we might as well advocate for it to be as responsible and transparent as possible. I believe that the reason fractional reserves at Bitcoin banks are bad is not due to any inherent problem with fractional reserves themselves because they misrepresent the solvency of an exchange. Full reserve exchanges can always redeem deposits; fractional reserve exchanges occasionally default on that obligation.

If I lend my friend Bitcoin for a month, I have created credit. Genesis, BlockFi, and Unchained Capital all do this, but on a bigger scale. Institutional prime brokerage—the same concept, but on a much larger scale—is just around the corner. When a bank runs a fractional reserve, they are doing the same thing. They create credit by lending out a portion of user deposits and they make money by charging a higher rate on those loans than the interest that they pay depositors. So for fractional reserve skeptics to be consistent, they have to be against *all lending activity* relating to Bitcoin. I have actually seen this view expressed, but it seems extremely draconian—and unrealistic to boot. There is a clear demand to borrow and lend Bitcoin.

I take a similar attitude to fractional reserves as I do to the existence of custodians: they are inevitable, so we might as well make them as transparent as possible. I propose exposing Bitcoin banks to the same forces that gave rise to Bitcoin itself: the free market. Right now we have a market for custody which everyone naively believes is fair, and is periodically beset by shocks as fraud is exposed. Why not a market for custody where the varying reserve ratios on offer are made transparent?

It's impossible to effectively audit a Bitcoin bank

One of the harshest critics of the reserve currency model of Bitcoin is Eric Voskuil. In a post on his Libbitcoin wiki, Eric pushes back at the Ammousian view of Bitcoin as a sound reserve to be used by commercial or central banks, similar to the way our monetary system used to operate with gold. (Eric also gave an interesting talk on the topic at Baltic Honeybadger 2018).

Eric dismisses the notion that paper certificates against depository Bitcoin are credible, stating:

The ratio of issued [Bitcoin IOUs] to BTC in reserve cannot ever be effectively audited.

It seems that Eric's critique relies on a few beliefs:

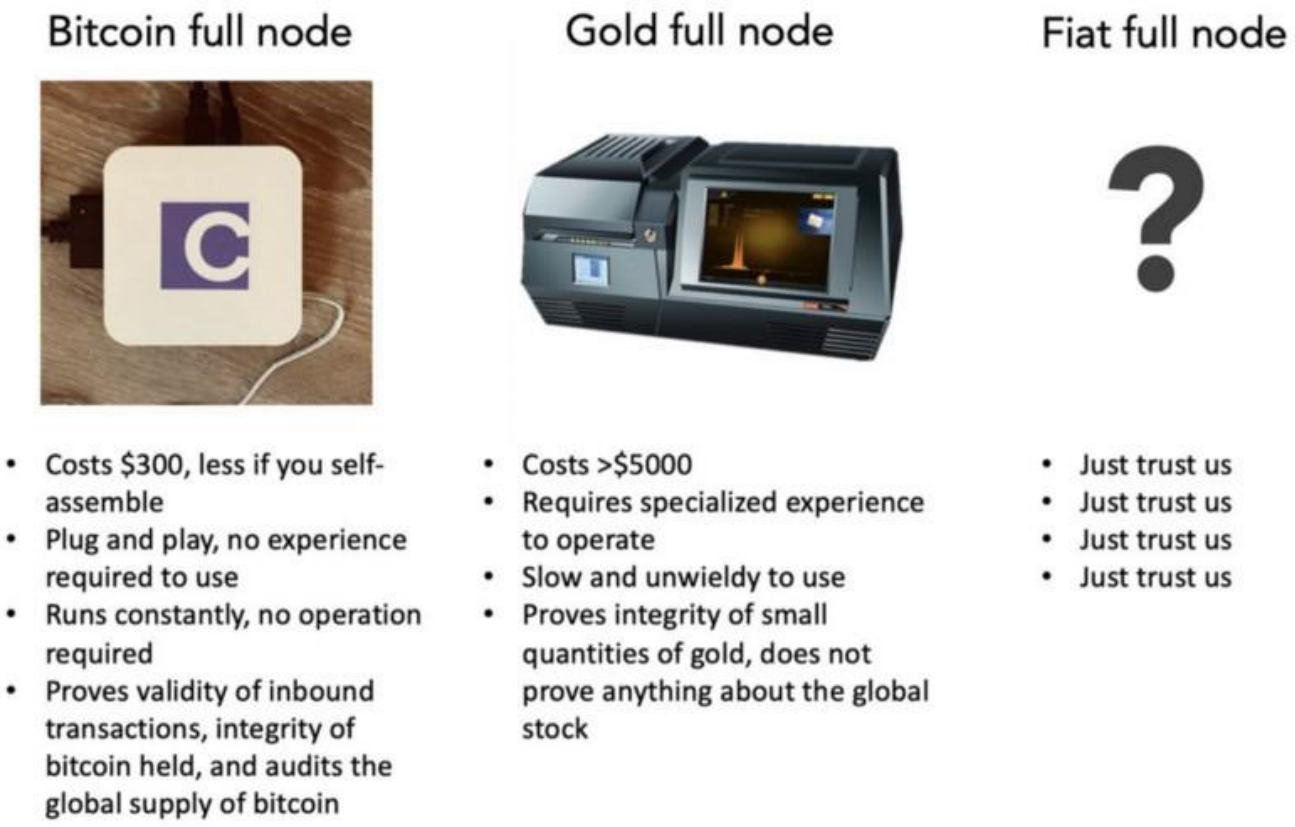
- That commercial banks would be coopted by the State—indeed, that banks are mere extensions of the State
- That proofs of reserves can *never* provide adequate guarantees to depositors
- That reserve ratios must be upheld by trust and hence would fail to be enforced
- That the entire bitcoin market would be consolidated within these depository institutions would would settle IOUs against each other

I don't have the space to give them a full treatment here; I would defer to Juice's excellent point-by-point rebuttal. To be frank, I just flat out disagree with Eric on a few key areas here. I think that proofs of reserves, if done correctly and with a reputable auditor, can provide depositors assurances of solvency *in spades*. I also don't believe that the government would immediately come to control the entire money supply in a bitcoin depository setting; commercial banks are independent, and in a non fascist state, would remain so.

Let's rewind a bit. To believe that a Bitcoin banking system can escape the problems that doomed the gold-based system, you have to believe that there are advantages that Bitcoin has relative to gold as a reserve asset. I would venture that it is the case. In particular:

- Bitcoin is auditable by design. What an individual does when they run a full node is that not only do they continuously audit the supply and make sure that the rules are being followed, but they audit the entire sequence of historical transactions to make sure every single one was legitimate and within the rules
- Auditing Bitcoin's M1 is cheap. It costs a few dollars a month to run a node. Gold nodes, by contrast, are expensive. XRF Spectrometers are pricey and tricky to operate. A fully trusted gold supply chain is so expensive that there only a handful in the world, with London being by far the biggest. In practice, in the private gold market, the cost of verifying any given lump of gold is so high that

entire trusted supply chains have been created, so that gold circulates within a walled garden and doesn't have to be reverified at every step. If you are curious, read the LBMA's good delivery rules. $300b worth of gold is currently held in London within this framework. Alternatively, central banks just custody large quantities of gold themselves and never move it.



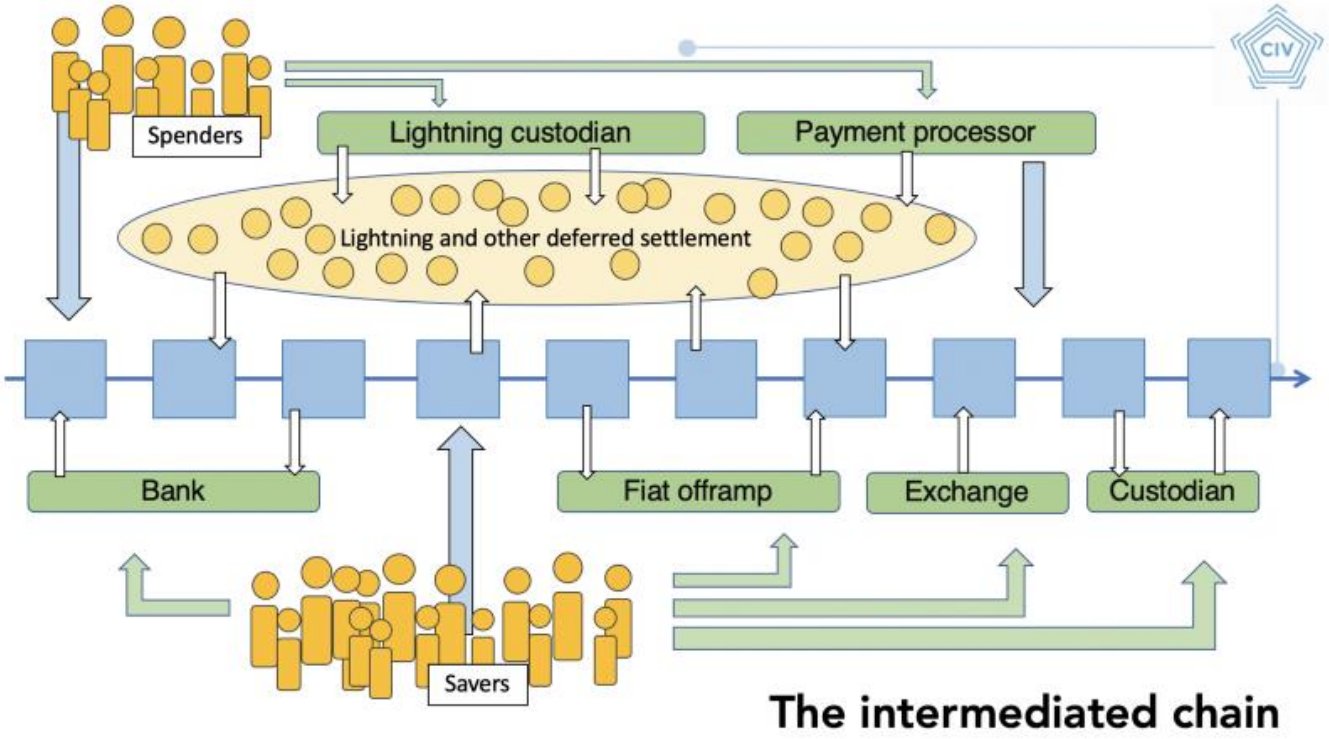
- Assessing the amount of Bitcoin credit outstanding is at least plausible, whereas for gold it's impossible. If exchanges issue IOUs redeemable for Bitcoin deposits, as they do today, we have the tools to verify that they aren't lying to us

In short, Bitcoin provides auditability guarantees that are incomparably better than those provided by gold, doing away with the need for a trusted supply chain, costly overhead for storage, or costly inbound verification. The cryptographic nature of Bitcoin, which can be extended through simple proof of reserve attestations, is exactly what makes it so amenable to trust-minimized custodianship.

Why are you settling for intermediation? Why not push for a world where Bitcoin is used directly by all?

I'm aware that my approach could be perceived as settling. However, I think the opportunity to live in a world where non-intermediated Bitcoin is the sole mode of usage has long passed us by. Normal people have a voracious demand for custodians and banks—and that makes sense. We don't self-custody our stock certificates either. These things are a challenge to custody ourselves, and the additional benefits of banks—earning interest, providing peace of mind, and so on—have made them extremely popular.

According to Coinshares, about 2.9m BTC are currently held in the custody of entities like Coinbase, Xapo, the Greyscale Bitcoin trust, Binance, and so on. Coin Metrics tells us that about 14 million Bitcoin have been active in the last 5 years (total issued supply is 17.6m, but significant portions of supply are lost or inert), so that leaves us with **20 percent of the effective bitcoin supply**in the hands of third parties!



Slide from my presentation at BH2018

I don't happen to believe that we will all collectively wake up one day and decide to self-custody. I see this industry going two directions: one where custodians continue to breach our trust and lose user deposits, or one where we hold them accountable to a high standard. For the latter to occur we need to acknowledge that they are an important part of the Bitcoin economy, for better or for worse. If the existence of

intermediation implies that Bitcoin has failed, then the dogmatists should abandon the project.

And, to be frank, even if you don't like the idea of Bitcoin banks, you have nothing to lose from demanding that they prove their reserves. Normal financial institutions deal with stringent regulations because the consequences for failure are so severe. In lieu of a regulatory regime covering institutions which take Bitcoin deposits, we might as well lobby exchanges to audit themselves.

What if [bad thing] happens to Bitcoin? Is this generalizable?

The framework I'm proposing applies to any auditable digital bearer asset. That's the distinction between gold and virtual currencies/commodities: they are natively auditable, whereas gold is extremely cumbersome to audit and verify. Privacycoins are more challenging but there are ways to audit them with viewkeys or selective disclosure.

Lending by Bitcoin banks effectively inflates the supply of BTC

Canny readers will remember their Econ 101 classes where it was demonstrated that the cascade of deposits and lending at banks with low reserve ratios leads to the effective creation of new money—far more money than existed in deposits.

This would be the case if a vibrant industry of non-full-reserve Bitcoin banks were to appear. In fact, if you squint a bit, this reality is the case today. Nominal volumes on the Bitcoin derivatives exchange Bitmex eclipse those at spot exchanges. Far more Bitcoins trade there than exist in deposits at the exchange, precisely because Bitmex extends loans to users in the form of margin. That's credit creation.

I don't think there is anything inherently wrong with the creation of credit, as it is the most basic component to finance. If credit is being created in a transparent way, on top of a reserve asset that is no one else's liability, that's a significant improvement over our current system. And I think it's something worth pursuing.

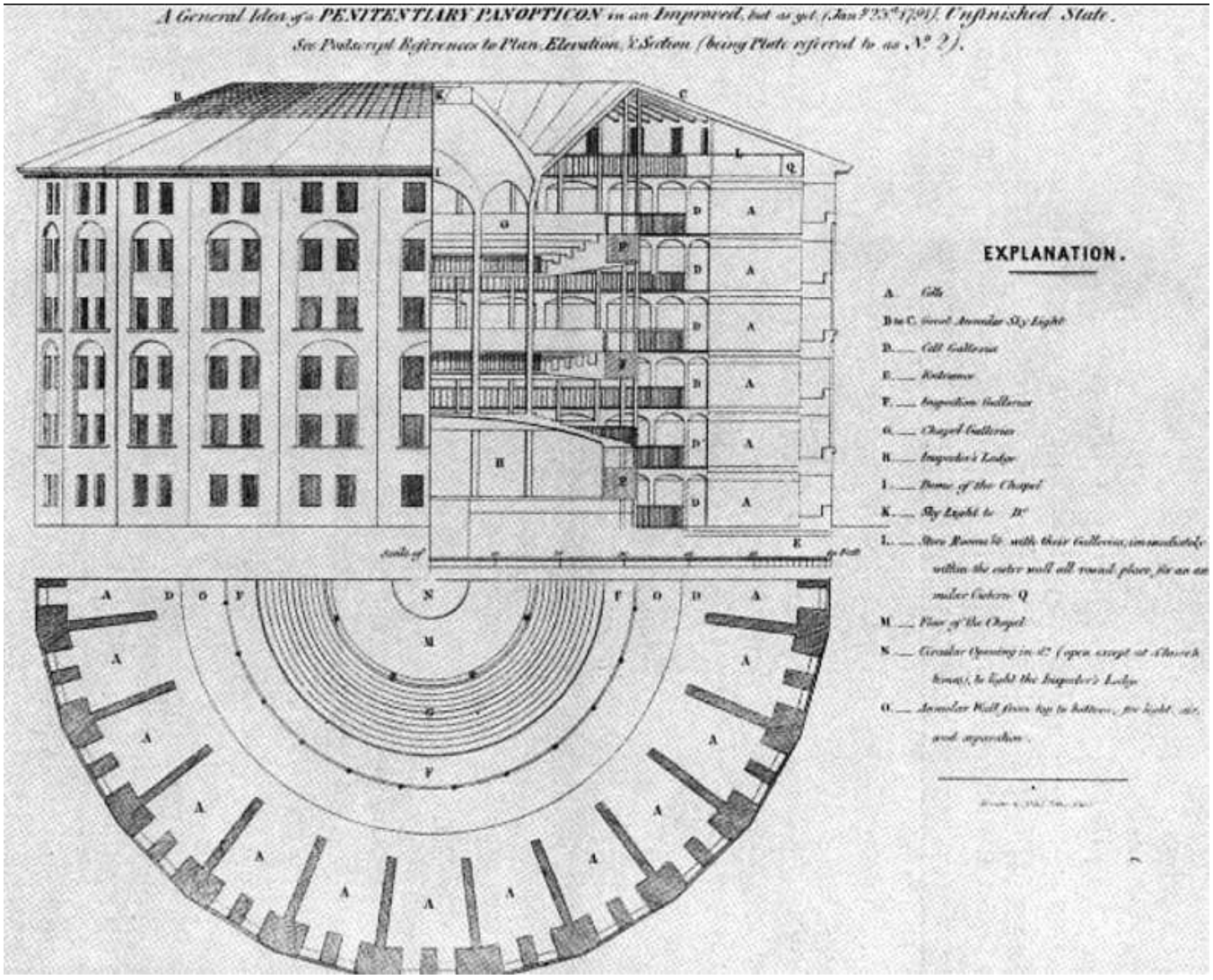
Thanks to Hasu , Matt Walsh, and Warren Togami for their feedback and assistance with this article.

I'm Not an International Drug Dealer

So Why Do I Need Privacy?

By Meltem Demirors

Posted April 15, 2019



An overview of Jeremy Bentham's concept for a panopticon — or the optimal prison design to inspire fear

'...a new mode of obtaining power of mind over mind'– Jeremy Bentham, 1798

The panopticon was a prison design conceived by the rationalist Jeremy Bentham, and detailed in his 1798 writings of the same name. As a feat of architecture, the panopticon served to create two illusions—for the prisoner, that there was no escape from surveillance at any time, and no ability to determine if one was being watched, and for the prison guard, the ability to surveil at her leisure, without detection, and disempower the individual.

For the panopticon to function, at its core, Bentham realized he needed to create a fundamental imbalance of power, and to enforce this power dynamic in every aspect of design. According to Bentham, the panopticon could be used for prison reform,

hospitals, the insane asylum, but most importantly, for schools, as they could be powerful tools of social and psychological conditioning.

The idea of power through control has guided much of human history—waxing and waning from the rise of totalitarian regimes to their ultimate defeat at the hands of revolutionaries or mass exodus.

A Brief Foray into Dystopian Fiction

Ah, doesn't attending crypto conferences make you believe our future will be a beautiful utopia, filled with tokens that only go up in value, and deFi products that make getting a loan as simple as posting your millions of ETH as collateral?

Let's explore a darker future. A dystopia, perhaps. In my view, one of the best ways to understand the present is to imagine the future and what better way to time travel through different versions of reality than by reading science fiction?

In 1933, Aldous Huxley penned Brave New World, in which the miracle of science and technology had been embraced to keep everyone happy and complacent, buzzing on *soma,* a pharmaceutical drug dispensed like Pez by the state. At the time Huxley wrote the book, much of the conversation in intellectual circles was around how humanity would solve economic and social issues, and usher in the so-called "Age of Utopia." Recall that at this time in history, Ford had just popularized industrial production (Ford is a Demi god in the book), and consumer credit was becoming popular with the rise of high value, mass produced goods. Huxley's book was in many ways a protest against this idea of utopia, and the dark places it would lead us as a society.

Ten years later, after the horrors of World War II, George Orwell published 1984, which described a dystopian future far less comforting than Huxley's, and was positively terrifying in many ways. Having witnessed the rise of Hitler's Third Reich and the brutality of the industrial war machine (fueled by new technology), Orwell no doubt drew from a different set of inspirations than Huxley. The Allied powers were busy diving the world into "spheres of influence" and setting up new political, military, and economic alliances in Africa, the Middle East, and Asia in a new form of global colonialism fueled by debt and credit.

Since then, countless novels have been written with similar themes, and you've likely read them at some point in your life. What I want to point out here is that the idea of control in these two books is very different. Both rely on mass psychological control and conditioning, but in very different ways.

Huxley's world was one of apathy. Orwell's world was one of fear.

Huxley's world was one of pleasure, derived from the sweet, sweet *soma* and the pursuit of hedonistic, basic desires. Orwell's world was one of pain, or "a boot stomping forever on the face of humanity."

Most critically, Huxley's world was one drowning in useless information, where no one cared for facts, especially not unpleasant ones. Orwell's world was one where information was limited and controlled.

Both apathy and fear are tools of oppression. And understanding how they are used is important to understanding where we might go next.

One notable theme among all of these novels is that a lack of willingness to subject to surveillance or subject to social norms somehow made a person guilty of hiding *something*. This idea is becoming more prevalent today, as the world divides into those who value privacy and those who believe it has no value other than crime or illicit activity.

The Politics of Privacy

I've been thinking more about privacy generally, and here are some of the responses I've been getting when I talk about privacy on Twitter:

Whenever there's a conversation about privacy, the inevitable ask becomes "why do you need privacy?"

Let's talk briefly about *why* we must have privacy as the *default setting* for all things in our lives.

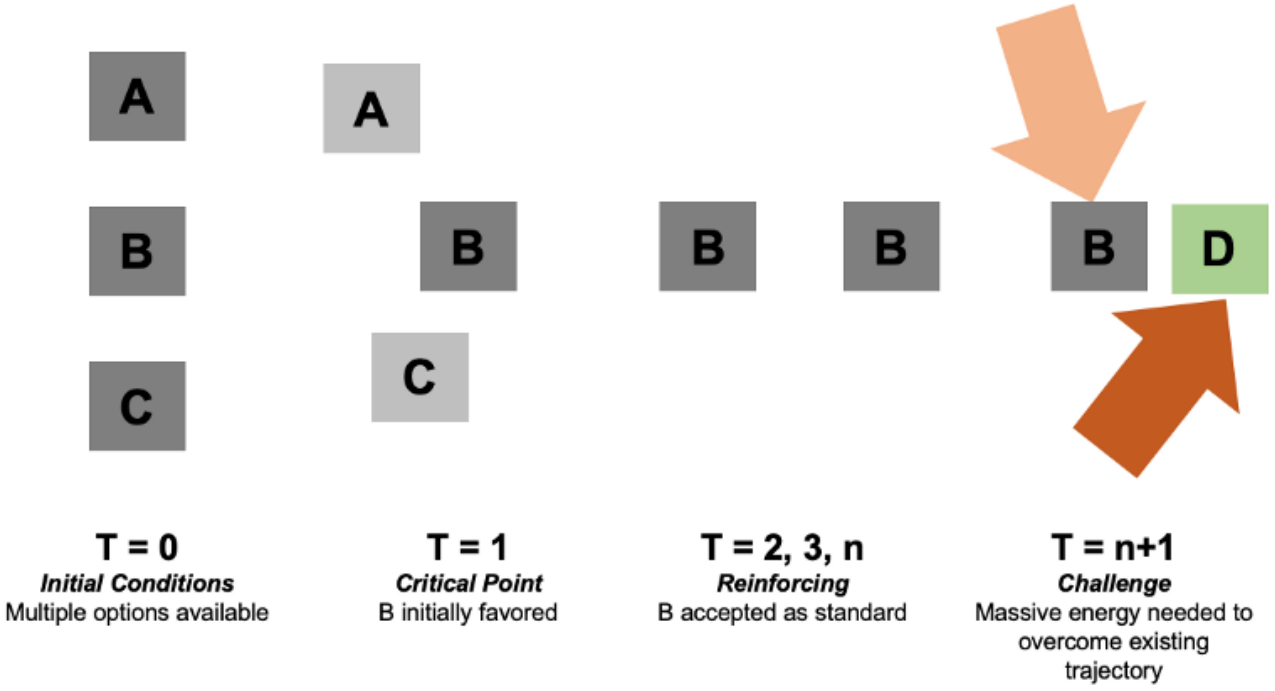
Here is a simple example. There are three options for a specific function, say, how privacy policies are served to you by an application you use. People are using different approaches, and it's very exploratory. Over time, there seems to be clustering around A, B, and C.

A—you are given a simple, click through interface which highlights the most significant points of the policy in simple language, and for each type of term requiring consent, the options to choose “I CONSENT” or “I DO NOT CONSENT”

B—you are given a hyperlink that links to the Privacy policy and one button that says “I AGREE”

C—you are given no Privacy policy information in a visible way, but it is linked that the bottom of a website page

Now over time, B seems to be used more and more, so B is what is talked about, taught, regulated, standardized, what apps are designed around, what users are accustomed to, and therefore becomes a self-reinforcing “standard.” This goes on and on, and while there may be new approaches now and again, B is for all intents and purposes “the standard.”



Yes, this is a grossly simplistic view. Yes, path dependence is still a contested area of study.

Let’s say that by time *n*, the world has changed drastically, and a growing group of people recognize the standard B is actually harmful to their interests, and devises an alternative, D, that is better for this group’s interests. There will be a tremendous amount of energy requires to (1) demonstrate B is in fact inferior in some way, and (2) prove D is superior and install it as the standard.

This “energy” may include marketing, PR, regulation, legal action and other types of economic, political, or social activity, including acceptable and less acceptable practices, like bribery, collusion, or say, outright revolution.

Social and economic systems are inevitably far more complex than what is described. The point here is that larger systems that develop over time will be built on systems and knowledge gleaned from the past. So, in some respects, the potential paths for the future are constrained and defined by the paths open today, and the logic of the initial decisions made today.

So—imagine this. Today, at t = 0, you don’t think about your privacy often, it at all, and it really has no material impact on your life. So option B feels fine. Perhaps you even justify or support option B, by tweeting things like (yes, someone said this and yes, it makes me really sad because they probably believe it):

> Why is privacy a human right? I feel like the world would be a better place with less privacy.

Tomorrow, you might find the circumstances of your reality changed, and you realize option B is in fact very much sub-optimal, and possibly even harmful to you, because of things like:

> Your right privacy is evil! Please post on twitter:
> - your bank details, including passwords & pins
> - Your address, location of any valuables in your house, & dates & times of when you will be away
> - medical data.
> - transcripts of your calls
> - naked pictures of you & your family

All of a sudden, if you attempt to protect your privacy, you have something to hide, and you must be doing something evil. You were complicit in creating the status quo, either through your *consent* or your *apathy,* so now you live with its consequences, unless there are other people with sufficient power, force, and energy to re-draw the boundaries of what is possible.

If we do not value our privacy today, and do not put into place mechanisms to protect, preserve, and enhance our privacy using technology, then we create the

conditions for a future where our privacy has no value, and cannot be protected, preserved, or enhanced.

A Quick Detour to Cypherpunks

We can't talk about privacy without talking about the cypherpunk movement. A **cypherpunk** is any activist advocating widespread use of strong cryptography and privacy-enhancing technologies as a route to social and political change. When the internet was beginning to become more commercialized, and as the world was converging on standards, a group of activists became concerned about the direction things were heading. The US government considered cryptography software to be a "weapon," and would not allow it to be commercialized or sold.

In response, this group convened more formally on a mailing list, and one of the founders of the list circulated the Cypherpunk Manifesto, a short statement describing the purpose of the list.

We must defend our own privacy if we expect to have any. We must come together and create systems which allow anonymous transactions to take place. People have been defending their own privacy for centuries with whispers, darkness, envelopes, closed doors, secret handshakes, and couriers. The technologies of the past did not allow for strong privacy, but electronic technologies do.

We the Cypherpunks are dedicated to building anonymous systems. We are defending our privacy with cryptography, with anonymous mail forwarding systems, with digital signatures, and with electronic money.

The ideas expressed by the cypherpunks were by no means new. After all, countless revolutions in history have been inspired by anonymous or pseudonymous authors, artists, philosophers, and more. Cypherpunks formalized the relationship between technology and privacy, and effectively used advocacy (see the Electronic Frontier Foundation, the Open Privacy project), education, media, literature, art, legal code (many sued the US government, and several won), subversion (hacks, leaks), political dissent, code, and a variety of other tools to further their goals.

The ethos started as "cypherpunks write code," but has evolved to mean something far greater than just writing and deploying software. Cypherpunks **take action** as individuals. They take **personal responsibility**for empowering themselves against threats to privacy, in whatever way they are capable.

We, as users of cryptocurrencies and other forms of applied cryptography in communications and computing, are doing something decidedly cypherpunk. We are participating in proving that these early prototypes have merit, and we are directly participating in their evolution to be usable at scale and en masse. These are

important and essential experiments in the future of privacy preserving technology that can reach not just the privileged few.

In the future, as it was in the past, privacy may define the line between life and death for individuals, their families, and their social groups.

Privacy Today is an Illusion

In 2013, the world got a very bitter taste of an Orwellian future, when Edward Snowden, a private government contractor who was working for the National Security Agency, or the NSA, copied and leaked thousands of highly classified documents about global surveillance programs being run by governments involving payments to private corporations for access to emails, records, logs, and other private information about citizens. The breadth and depth of the surveillance state spanning not only the US, but also Europe, was not fully appreciated by the public until it was revealed by Snowden in this act of defiance, that was decidedly very cypherpunk.

So what do we mean when we use the phrase "surveillance capitalism?" (sidebar: listen to my podcast with Jill Carlson on this topic). Effectively, we are describing a new form of capitalism focused on commodifying behavioral and experiential data, which was pioneered by Google and later Facebook, and now used by nearly every technology company.

The rise of the internet and the movement of social life, commerce, communication, and human experience from physical space into the digital space has made it challenging for nation states to monitor a new and nearly limitless frontier (that wild west of the world wide web) and for corporations to implement existing business models. As a result, many companies now make money by providing a free or low cost product or service to consumers to gather data, and then selling that data to advertisers, governments, and other buyers.

Girls Just Wanna Have Privacy

Privacy, like anything else, is a topic that must be learned. If it feels overwhelming, it's because it can be. Today, obtaining privacy is a Herculean feat that requires all sorts of trade-offs between usability and privacy. Tomorrow, I believe privacy should be easily accessible to anyone who desires it.

There are three types of privacy I believe must be preserved —

1. Privacy in Economic Interactions, meaning who we send money to, how, when, in what amount, and why is something we have a right to keep private to ourselves and the recipient
2. Privacy in Movement, meaning we should be able to move about physical, digital, and virtual space with anonymity, and we should be able to enter and

leave spaces, whether in real life or online, without giving out identifying information
3. Privacy in Communications, meaning we should be able to conduct conversations with certainty that they will remain private, and that we should be able to abstract our identity from our communications both in the physical world and online

Today, your degree of freedom in any of these is determined by a number of factors including where you live, what platforms and applications you use, your understanding of how to increase or decrease your privacy via use of additional tools like VPN, and the level of surveillance an unknown third party may want to exercise on you—just to name some. There are factors that are largely within your control, and factors that are outside of your control.

Tomorrow, freedom and privacy needs to be a default setting. We must take it upon ourselves to educate, advocate, build, and promote tools that preserve privacy.

Cryptocurrencies and Privacy

So how does this relate to the world of crypto?

By now, hopefully we all know this one fact—Bitcoin is not anonymous. It is pseudonymous. The blockchain is a public ledger—meaning anyone can download it, and since the earliest days of the bitcoin community, people have built tools to de-anonymize bitcoin users and link the blockchain pseudonyms ie wallet addressed with real people and places.

There are of course tools you can use—mixers, tumblers, and other programs to obfuscate the flow of funds, but the ability for cryptocurrency users to stay private is only secondary to the ability for companies to build business models violating this privacy so they can sell data to exchanges, regulators, and enforcement agencies.

But the future belongs to those who build it. And we have a big fight ahead.

Crypto is about freedom.

It's not about creating a new revenue stream for Wall St or delivering big IPO returns to investors. Those might be nice second order effects, but I reject the notion that this is the **primary goal**.

Crypto is about privacy.

It's not about creating a dystopian corporate digital currency on a private blockchain so you can guzzle Starbucks on piles of debt while you mainline Facebook and Instagram like a human click farm.

It's not going to be easy, but it's going to be worth it.

And as one does, I'll end with a quote, this one from a Russian dystopian sci fi novel entitled "We", published by Yevgeny Zamyatin in 1924.

"There is no final one; revolutions are infinite."

The battle for privacy won't be fought in one medium, at one time, or in some grandiose, defining way. The battle for privacy begins with the choices we make every moment—both small and large—and the manner in which we hold ourselves and others accountable.

So what will you choose?

Choose yourself.

Choose privacy.

Some Starting Resources

- How to Be Invisible (Book) by J.J. Luna
- Smart Girl's Guide to Privacy (Book) by Violet Blue
- EFF—Choosing a VPN That's Right for You
- Tripwire—Why OPSEC is for Everyone
- Kaspersky Lab—10 Tips to Improve Your Internet Privacy
- Berkeley—Top 10 Secure Computing Tips
- Jameson Lopp—A Modest Privacy Protection Proposal
- NIAIA—Individual OPSEC & Personal Security — A How To Guide

---

The Return of the Deniers and the Revenge of Patoshi

By Sergio Demian Lerner

Posted April 16, 2019

Synopsis: *In this article I will discuss what we know about the early Bitcoin blocks. Also I will present a new strong argument that a single miner mined 22k blocks. Finally I'll introduce satoshiblocks.info, new website that shows a cool visualization of early blocks.*

The last time I wrote about Satoshi I thought it would be the last. But here I am, again. Let me bring some context. It all began in a discussion in 2013, in bitcointalk

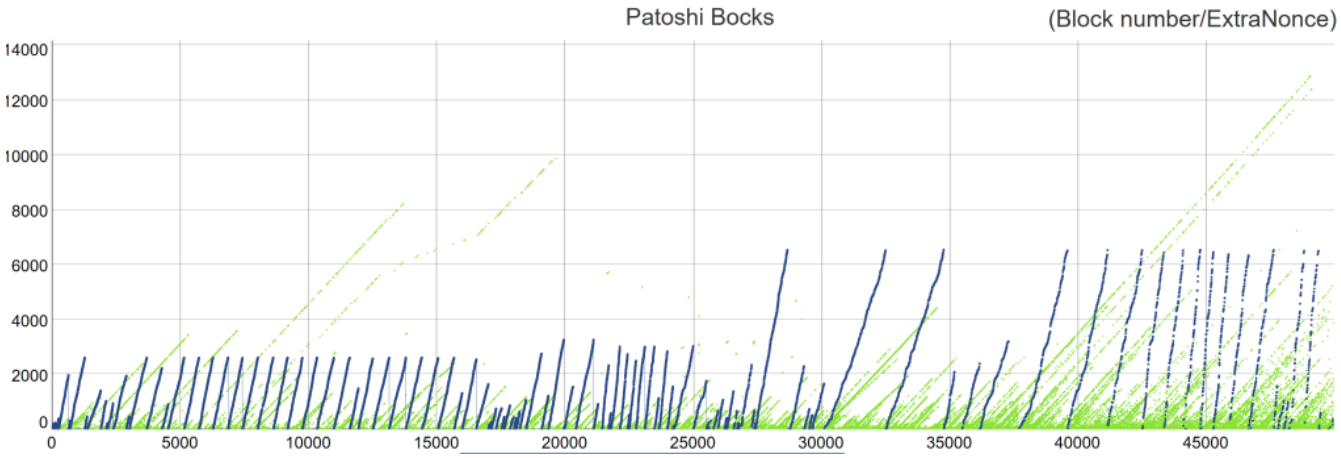
forum, where a plausible reasoning led me to believe that Satoshi would have mined one million bitcoins during 2009-2010. As you know, plausive reasoning doesn't let you prove anything mathematically, however it gives incredibly good results when applied correctly to solving real real-world problems, where information is imperfect or missing. The original argument about Satoshi coins can be simply stated like this: ***Supposition***: *Anyone who took the time and effort to create Bitcoin would not risk letting the network to halt due to lack of miners. He would run at least a miner himself.* During 2009 the mining activity was so low that it was kept active on the minimum accepted difficulty, and blocks were created at a lower rate than one every 10 minutes. It's plausible that even if Satoshi wanted to turn off his miner after a while, he may have finally decided to let it run until seeing more activity.

The Patoshi Pattern

In March 2013 I was able to turn the plausible reasoning into a probabilistically falsifiable argument, which means it it's highly improbable to be false. By reading the original Satoshi client v0.1 source code, I discovered three privacy-related flaws that, together, enable anyone to correlate the blocks mined during the first years and uncover a common origin. Also, it allows anyone to compute the approximate mining hash rate of each of the early miners. If one of these flaws had been absent, it would not have been possible to recognize a very special miner track and the tracks of the remaining miners. But first, a little technical background. The ExtraNonce field, located in the coinbase transaction, increments every time the nonce fields overflows, meaning the search space is exhausted. As the nonce field is 32 bits in length, and the Bitcoin initial difficulty was tuned to require scanning 32 bits on average, the nonce would sometimes, but not always, overflow. Now let's present the three flaws present in the original Bitcoin code:

1. The ExtraNonce works as a "free running counter", without resetting to zero between blocks mined.
2. The rate a certain miner increments the ExtraNonce is much faster than its actual hashrate would indicate, based on the original Bitcoin source code. We'll call this miner **Patoshi**.
3. Every few seconds during mining, the best block is checked. If the best block changes, the ExtraNonce is additionally incremented. Normally every external block received will increment the ExtraNonce, except for the exceptional miner Patoshi, which doesn't seem to follow this rule.

Together these flaws enable the visualization of the **Patoshi Pattern**. Blocks in the Patoshi pattern will be elements of the Patoshi set (or P set).

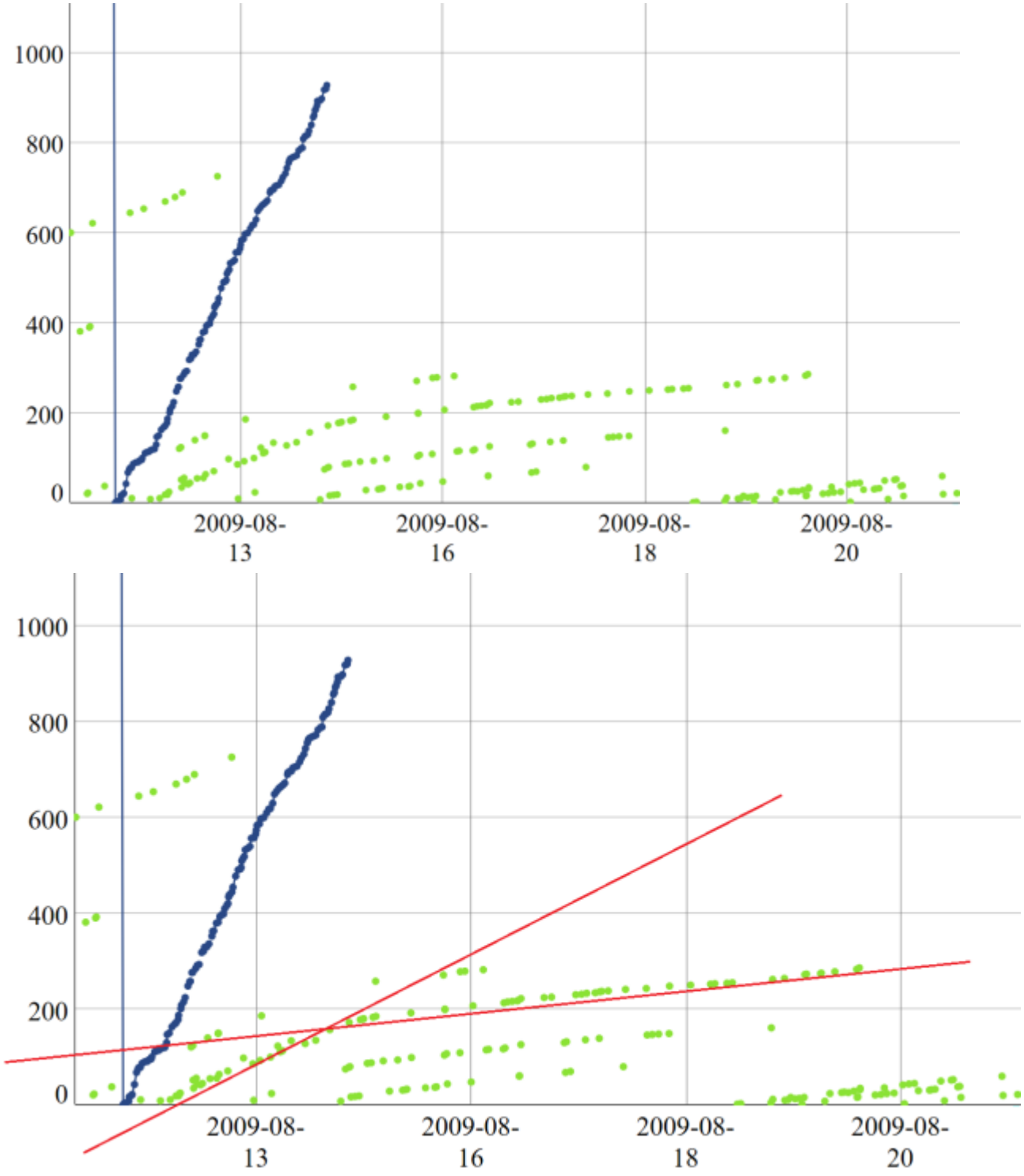


The Patoshi Pattern (blue) and the Remaining Miners Patterns (green)

The first flaw is that the ExtraNonce field was handled in a non-privacy preserving way. By not being reset each time a new block is mined, it works as a free-run counter or timestamp.

The second is that for a reason that was only uncovered a year later, the rate this timestamp is incremented by Patoshi was higher than the number of blocks solved would suggest, so even if his mining equipment was not so much faster, it looked so. This flaw alone let you very easily separate Patoshi from the rest of the miners. We lack information about how Patoshi mining software operated: for instance, it's seems that the Patoshi miner didn't followed the rule in flaw 3, but it can be the case that it checked the change in the best block less frequently and this invalidates any attempt to measure if flaw 3 was present or not in his software.

The third flaw enables anyone to follow the tracks of the remaining miners. If this flaw had not been present, most blocks of the remaining miners would be indistinguishable from "noise", having ExtraNonce values that are too close to zero, because the ExtraNonce would hardly ever increment. The nonce values of the remaining miners almost never overflow. In fact, because of this, in the blocks of the remaining miners the ExtraNonce counter behaves more like a global block counter, and therefore the ExtraNonce patterns of different miners appear with similar slope. If two blocks A and B are mined by the same miner, then the ExtraNonce delta between them would almost equal to the number of blocks mined between A and B. The moment in which the miner starts mining from a zero ExtraNonce value establishes a unique point the in the line created by every non-Patoshi miner.



When Patoshi stops mining, the remaining miners increment the ExtraNonce at a lower rate due to privacy flaw 3.

An exceptional case is when several blocks are mined in a very short time: or if the mining process is paused and resumed after a few minutes, then the ExtraNonce will be incremented only once for many blocks in a row. However, this doesn't seem to

happen often. Last, it seems that the Patoshi miner doesn't follow this rule: there are many cases where the distance between his blocks is lower than the number of blocks in-between. While the absence of this flaw is yet another way of distinguishing Patoshi blocks from the rest, we'll focus on other more interesting distinguishers.

Together, the 3 privacy flaws enable the ExtraNonce in early blocks "links to" the last block mined by the same miner, for all miners. This link is based on a coarse timestamping, it's imperfect, but it can be shown, by simple statistical analysis, that is highly precise for linking blocks. There is a perfect match between the observed behavior of non-Patoshi blocks and the Satoshi client v0.1 source code. Many people hold this historical source code. It's published in several places in the Internet. If you doubt the authenticity of such source code, you can convince yourself easily that there are some rules governing the ExtraNonce pattern: the probability that the pattern was created by chance is astonishingly low.

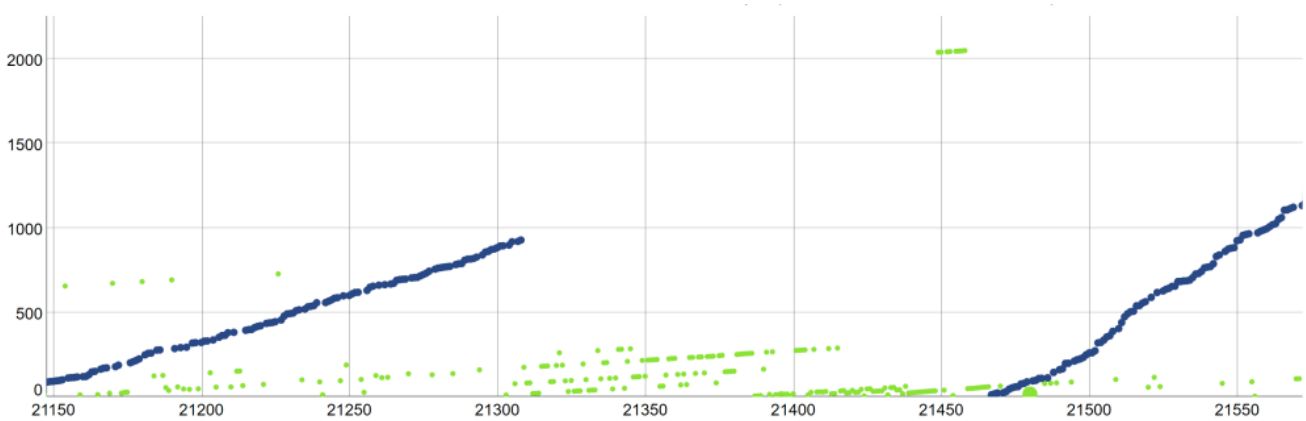
```
2190 CBigNum bnExtraNonce = 0;
2191 while (fGenerateBitcoins)
2192 {                                                          Flaw 1
2207         // Create coinbase tx
2212         txNew.vin[0].scriptSig << nBits << ++bnExtraNonce;
2218         // Create new block
2272         // Prebuild hash buffer
2297         tmp.block.nTime = pblock->nTime =
                max((pindexPrev ? pindexPrev->GetMedianTimePast()+1 : 0),
                GetAdjustedTime());
2308         unsigned int nStart = GetTime();
2311         loop // Search
2312     {
2313             // hash
2317             if (hash <= hashTarget)
2318             {
2319                 … // Process this block..
2342                 break;
2343             }
2345             // Update nTime every few seconds
2346             if ((++tmp.block.nNonce & 0x3ffff) == 0)
2347             {
2349                 if (tmp.block.nNonce == 0)
2350                     break;
2351                 if (pindexPrev != pindexBest)
2352                     break;
2353                 if (nTransactionsUpdated != nTransactionsUpdatedLast &&
                        GetTime() - nStart > 60)
2354                     break;
2357                 tmp.block.nTime = pblock->nTime =
                        max(pindexPrev->GetMedianTimePast()+1,
                    GetAdjustedTime());
2358             } // nNonce & 0x3ffff) == 0
2359     } // Loop
```

Bitcoin Client 0.1 Mining Loop

As soon as you look as the ExtraNonce/Time patterns you realize that the Patoshi chain of linked blocks is outstanding: about 22k blocks in total, high slope, dense chain. Both the naked eye and slope-tracking algorithms pinpoints this pattern immediately. The slopes break at some points, where extranonces restart from zero. The slope (the apparent mining rate) of blocks in this pattern is very different from any other chain of blocks and is quite stable except for three fast changes in two years. While there is a small probability that some blocks are incorrectly tagged by the algorithm, most of the blocks can be tagged without dispute. I estimate the tagging error is 0.1%.

The probability that the Patoshi pattern is formed by multiple miners with the same hardware (slope), each starting exactly when the previous one stopped is also astonishingly low (assuming miners can start mining at any random time). Also take

into consideration that the pattern slope does not represent its underlying hashrate. Therefore, the Patoshi pattern is “one thing”, not the concatenations of many separate things.



Patoshi Pauses Mining for 10 days, his longest pause.

There is Only One Patoshi

Some people accepted the existence of the Patoshi pattern, but at the same time refused the argument that a single entity mined the whole P set. Let’s review their arguments:

Main argument against single Patoshi: *The pattern is not created by a single miner but by many miners somehow synchronized.*

There are four strong reasons to reject this argument:

1. 99.9% of all Patoshi blocks are unspent. While only 10% of all non-Patoshi blocks are unspent. This means that the “synchronized” miners decided to spend only 0.1% of their bitcoins, while the remaining miners decided to spent 90% of them (or alternatively each spent 90% of their bitcoins, or each block has a 0.9 probability of being spent). Assuming no correlation between blocks, the probability that only 0.1% of Patoshi blocks being spent is close to 2^-76000. But we can assume high correlation: a miner either sells all his coins or no coin at all. The number of other miners went from 0 to about 25 by March 2010. But the number of synchronized miners in Patoshi pattern would have stayed almost intact, because the hashrate of the Patoshi pattern mostly decreases over time. If we assume the synchronized miners were 6, then the chance they didn’t sell their coins by chance is one in a million.
2. Each Patoshi block “links” to a block in the P set, but not to any of the remaining blocks. Somehow the information if a previous block was part or P

or not needs to have been communicated along the block. How was this communicated? Early blocks are all look similar. There is no pool signature, as there is today. For what reason would miners do this selective linking? What would they gain? Occam Razor would reject the existence of such system.
3. There are some time intervals where the Patoshi pattern interrupts abruptly (i.e. 07-18-2009 for a full day) and then continues from the point it has interrupted. How did all these separate miners coordinate the interruption, while other continued mining without problems? It may be the case that they were running the same version of the client, which failed. But there is no evidence of a special version of the software being distributed.

Second argument against single Patoshi: *There was a kind of heterogeneous mining pool formed since Genesis, and many independent users joined the pool.*

Strong rejections to this argument:

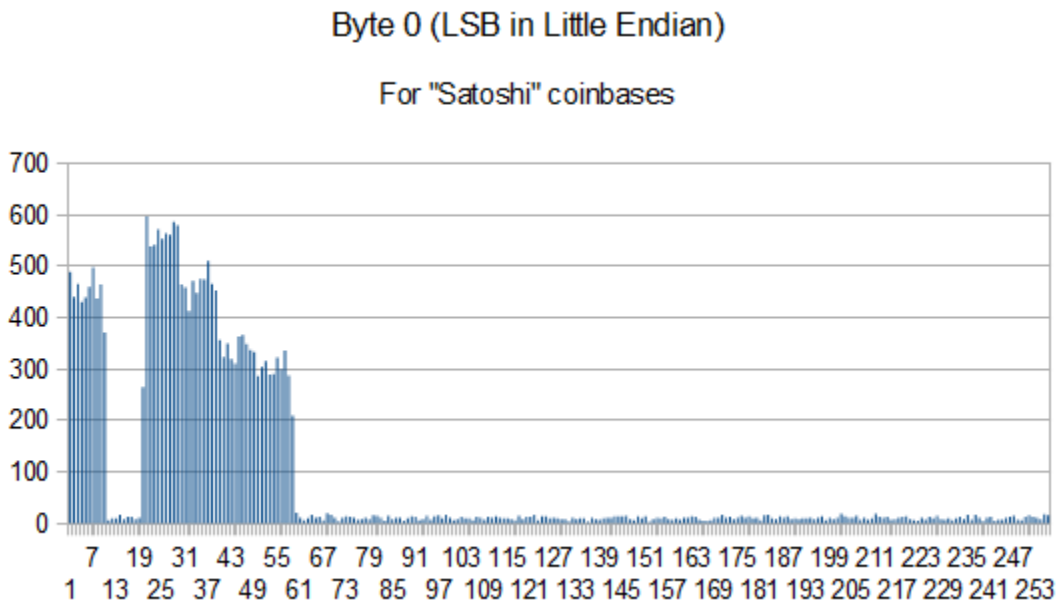
1. Mining pools were invented several years later
2. How was the existence of this mining pool secretly communicated before the Genesis block was even created? The Patoshi pattern starts right at Genesis.
3. Mining pools were created to reduce reward variance due to the low individual probability of solving a block, but during 2009 single miners could easily solve blocks frequently. Why to pool resources? There is no reason.
4. There weren't enough miners to incentivize pooling, as the Patoshi hashrate corresponds to one to six miners (depending on the assumed efficiency of the involved PCs).
5. It would have required specific software (that was never made public) to manage the pool and more software to use it.
6. All these being done in secrecy would imply some kind of conspiration, which seems ridiculous.

There is no technical reason, no software developed, no operational expertise at that time, no monetary gain, and no benefit at all for the creation of a mining pool when Bitcoin was launched. Therefore, we can assume there was no mining pool at Genesis time.

Based on the assumption that the pattern comes from a single entity you can directly conclude that this party was using a special mining software and/or hardware: fast as one or more state-of-the-art servers in 2009, and with slightly different rules governing how to mine.

Nonce Restriction in all Patoshi Blocks

Even if most people were convinced the Patoshi pattern was real, some people still weren't. But by the end of 2013 things got more interesting: I found proof, beyond any doubt, that the pattern was real, using a completely different method. I discovered that all Patoshi blocks were marked by a reduction of the range of nonces used in published blocks, to a specific range R. We can define R by restricting the least significant byte of the nonce field. This byte normally increments from 0 to 255, but in the Patoshi blocks is reduced to the range [0..9] U [19.. 58].



An Histogram of the LSB Byte of the Nonce Value in the Block Header

The fact that Patoshi nonces are in this range does not imply the miner of the Patoshi pattern only scanned nonces within this range. It could be the case that the network rejected the solved blocks having nonces out of this range, or the same Patoshi mining software did. This is not the case, as there is a direct relationship between the number of nonces scanned and the average time Patoshi took to solve a block. And the relation suggests the nonce space was reduced to R to create blocks at the rate Patoshi blocks were created. The nonces space scanned is about 1/5th of the full range, and the ExtraNonce increments about 5 times faster.

If you collect the set of blocks whose nonce is in range R, you'll find it contains 27.68k blocks. I call this set M. The blocks that are in M have the nonce in the R range. The set M is far bigger than one would expect from normal mining. The chances M contains 27.68k blocks assuming uniform nonces is negligible (less than 2^-36000). From the 50k blocks analyzed you would expect that only 10K blocks belong to M, not 28k. But we'll see this perfectly matches the anomaly of the Patoshi set.

If Q blocks had been marked by restricting the nonce range when scanning, and the remaining elements of M had nonces in R just by chance, then we could compute Q from the following equation (isolating Q): Q + (50-Q)/5 ~= 27.6. The solution is Q=~22k, exactly the size of the Patoshi set. It also indicates there are no other blocks were scanned within the restricted range R except those from Patoshi.

If you re-analyze the common arguments against single-miner for the Patoshi pattern considering this new discovery, the original arguments can't resist any probabilistic justification. Chances get far lower of what people consider just impossible.

Regarding why the nonce was restricted to the range R, I didn't know, and I still don't. These are some of the possible arguments I came up with:

1. **The restricted range was part of a "trapdoor" to mine blocks with higher probability of obtaining a hash digest below the target.**There is a plausible strong reason this to be false: mining faster by restricting the nonce range implies partially breaking SHA256 pre-image resistance. No scientific paper has ever mentioned such a devastating attack, neither for SHA256 nor for standardized hashing functions using the same Merkle–Damgård construction. Any party with the capability to find SHA256 partial pre-images would probably be able to break most commercial communications, from TLS to VPNs, and earn billions. But there is another reason which is mathematical: if you re-mine all Patoshi blocks, trying to find other solutions to the same block templates, will find that the amount of solutions in the R range compared to the amount of solutions out of that range matches the relation of relative range sizes. It was no "better" to mine within that range. The Patoshi set was simply marked to identify something. What? We don't know.
2. **The restricted range is user to indicate ownership.** If Patoshi were two people, maybe they agreed to give 80% of the block rewards to one of them, and 20% to the other. Then the final owner was marked by specific LSB of the nonce, before scanning the rest of the nonce. This can be proven false, as it would imply Patoshi miners had to increase the extra nonce 256 times more often, which doesn't happen during the first years. Maybe the restricted range is used to indicate probabilistic ownership: the range R is split into sub-ranges, and it's fully scanned. The party who gets the bitcoins is the one whose sub-range is randomly picked in the solved block.
3. **Sub-ranges of R were used to identify different mining hardware cores, where each core would scan a reduced nonce space**. This means that Patoshi created the first private homogeneous mining pool. By homogeneous I mean that either all mining machines were setup by a single entity, or a small group of people agreed to use the same type of hardware to fairly distribute earnings. This hypothesis has not been falsified.

At this point I've said just a little more from my previous research articles. And from 2014 to early 2019 I didn't have anything else to say (or to research) about early blocks. Several following studies repeated my research and arrived at similar conclusions. OrganOfConti's famous blog post contains even more data about Satoshi, describing how he reduced his hashrate in four steps. The last known study, by BitMex Research, comes to the conclusion that Satoshi probably mined 700k coins during 2009-2010. Sadly, they miss the LSB argument entirely (which is the strongest of all known).

But there are people, like nullc, that every now and then go public challenging all this research with old arguments. In a nutshell, I would say that nullc argues a Null Hypothesis: nothing is real. Which is silly because the research was validated by many independent academics.

Null hypothesis: *(in a statistical test) the hypothesis that there is no significant difference between specified populations, any observed difference being due to sampling or experimental error.*

The reasons why nullc argues this continuously escape my imagination. It's completely unscientific. The data is there in the blockchain. It doesn't need rocket science to collect and analyze it. All you need is to grab a Bitcoin blockchain parser. When some weeks ago I read the comments on reddit I felt compelled to refute him again, because … well, because I can. So here I am. Nullc argues that the Patoshi pattern is just the result of some kind of sampling trick. A human interpretation, like shapes in the clouds. He states:

" The million coins being discussed are all unspent coins from the first year, there is fairly strong evidence that they were not mined by a single party (because their nonce incrementing was consistent with multiple parties). If you refer to the lines on the left side of the graph on the page the involved coins there are more like 200k.". Nullc, 2019. Of course, he doesn't give any "strong argument" and the "nonce incrementing" is perfectly consistent with multiple parties plus a single party mining most of the blocks. The argument is just silly.

I have three new strong arguments that Satoshi mined close to 1.1M coins (even more than the initial 1M I discovered). I have a more precise figure now because I coded a more accurate pattern-following algorithm. But it's too much information for a single post, so I'll just present one argument here. Stay with me just a few more paragraphs. Let's focus on the first 50k blocks of Bitcoin, from January 2009 to April 2010.

A New Argument Based on Computer Clocks

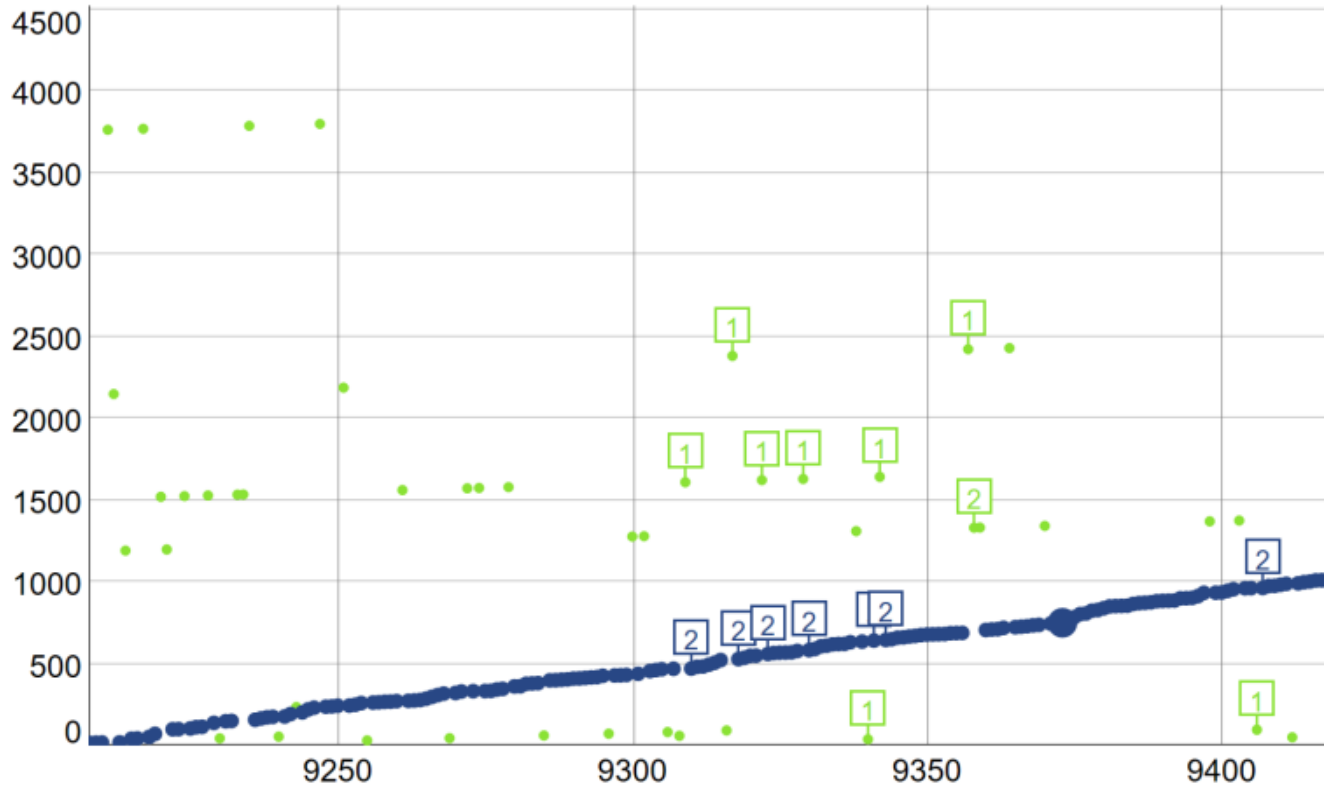
I'll prove with overwhelming probability that only a single miner has mined all coins in the Patoshi pattern. If you've studied the Bitcoin protocol, you'll know that block timestamps are not necessarily monotonically increasing. The miner uses its local computer clock to timestamp the blocks. This is true from the Bitcoin source code 0.1.0 to the latest version of Bitcoin Core that had an internal miner (before mining pools were created). There are three things that can affect block timestamps:

1. Computer clocks can be unsynchronized from each other. The computer clock is adjusted by most operating systems by slowing down or accelerating the clock increments, but it doesn't go back spontaneously. A computer that synchronizes with an Internet clock source (a time server) would never lag more than a few seconds.
2. Timestamps were not updated continuously during mining. They were only recomputed every 0x40000 nonces in the Satoshi client v0.1 (approximately once every 10 seconds). This means that a timestamp can lag. However, timestamps are always updated when a new best block arrives.
3. Block timestamps are adjusted by the Bitcoin software to match the median time of the peers that are connected to a node. The adjustment can be positive or negative. Negative adjustments could imply that future blocks may have prior timestamps. The algorithm used is a bit awkward, as it doesn't recompute the measurements after a correction. But as time passes, and more nodes have connected in the past, the effect of this adjustment diminishes (the vTimeOffsets vector grows). Therefore, after some time the full node internal time should stay without significative adjustments. Also, the peer to peer network, if highly connected, would converge to a global "median time".

Because of the reasons expressed in (1) and (3), the same computer will almost never reverse its own timestamps. If a miner creates a block with lower timestamp than its parent, and the time difference between the blocks is D, a small portion of D (such a few seconds) may be caused by (3) but the most part of D is an indirect measurement of the time it took the parent miner to complete the last (unfinished) nonce range scan of 0x40000 elements (~ 10 seconds), corresponding to the lag introduced by (2). In a way, the delta between inverted block timestamps indirectly measures the hashrate of the parent block miner (if all ExtraNonces were incremented at the same rate). Later we'll say more about these deltas.

If we scan the first 50k blocks to find blocks whose timestamps are lower than their parents', we should almost never find a case of two consecutive blocks mined by the same miner. If we found many, then that's an indication we were wrong to think they were from the same miner. And if we found too few compared to the average number of reversals, it would be an indication it's the same miner indeed.

I run a program to find such time inversions and to print when they happened between blocks in the Patoshi pattern, both blocks out of the Patoshi pattern, and between the Patoshi blocks and the remaining blocks. All the data and new nice graphs of every inversion event has been loaded into the new site satoshiblocks.info.



Some cases of Timestamp Inversions (1=Parent / 2=Child)

To see the complete list of timestamp inversions, go to the satoshiblocks website and click in the "Annotations" checkbox. Each parent is labeled "1". The corresponding child, which should be the next block, is labelled "2".

Here is the summary of all classified inversion events:

Case (parent and child)	Count	Average Time Between Blocks
Patoshi and Patoshi	**0**	—
Non-Patoshi and Non-Patoshi	224	642 s
Patoshi and Non-Patoshi	398	152 s
Non-Patoshi and Patoshi	72	1079 s
Total	694	

There are no time inversions between Patoshi blocks. Zero. This result is very relevant considering the Patoshi blocks account for 43% of all the blocks in the first 50k. I'm open to consider other explanations, but for me this can only mean one thing. There is a single PC clock whose time is stamped in the Patoshi blocks. A single software that controls how block templates are created. A single miner.

So who is Patoshi? The single miner that mined ~ 1.1M bitcoins?

There is evidence that links the Patoshi patterns to Satoshi, based on public information sources and the blockchain, of course. But I would prefer to stop here. Leave Patoshi alone once for all. I have too many things to build for Bitcoin, like RSK.

But I expect more denial posts in Bitcoin forums. And if that happens, then it's my call.

You can find more information about Satoshi blocks in the following articles:

- The Well Deserved Fortune of Satoshi Nakamoto, Bitcoin creator, Visionary and Genius (SDL, 2013)
- Satoshi's Fortune: a more accurate figure (SDL, 2013)
- A new mystery about Satoshi hidden in the Bitcoin block-chain (SDL, 2013)
- Satoshi's Machine: One Mystery is solved and another one opens (SDL, 2013)
- Reawaken interest in Chain-Archeology (SDL, 2014)
- July 2009 Mystery Solved (SDL, 2014)
- How you will not uncover Satoshi (SDL, 2014)
- Satoshi's hashrate (OrganOfCorti, 2014)
- A little more on Satoshi's blocks (OrganOfCorti, 2014)
- Another short post on mapping the historical hashrate distribution (OrganOfCorti, 2014)
- Does Satoshi have a million bitcoin? (BitMEX Reseach, 2018)

A few thoughts on what bitcoins are

By Joe Kendzicky

Posted April 17, 2019

There is no such thing as a bitcoin.

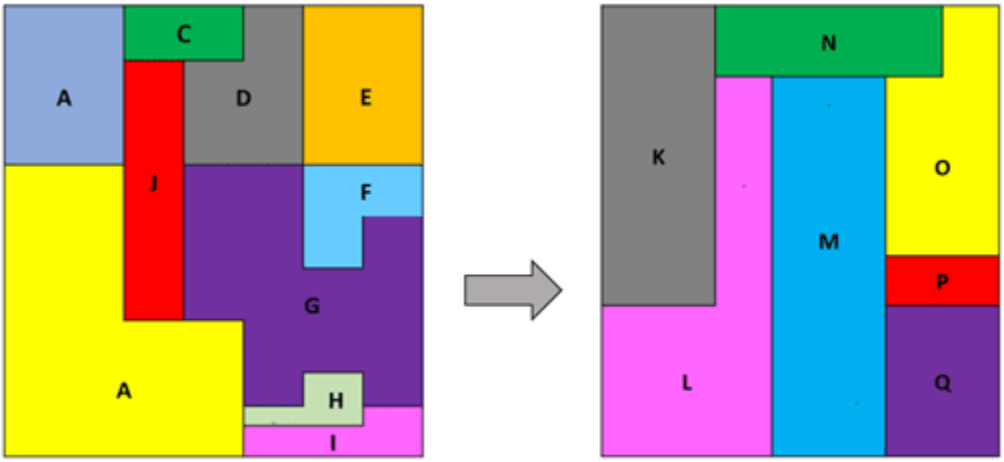
Even crazier, there is no “money” in the Bitcoin protocol; no BTC token, no virtual commodity, no accounts, no balances. All that exists is an accounting ledger.

When someone says “I have 5 bitcoins”, the classic image that comes to mind are shiny-looking digital tokens housed inside some digital wallet; like a dollar tucked away inside a leather purse. When sending bitcoin to a recipient, most believe that this virtual token departs from the program on their screen, traverses across the network at the speed of light, and lands in the possession of their recipient.

The truth is, bitcoins as a noun don’t even exist.

The assets of value people lust after are actually called UTXOs (unspent transaction output). Bitcoin can essentially be boiled down to a game where people compete for the right to scratch their name inside some digital ledger. The unique feature about this ledger space is that it is scarce, so there exists a limited number of people who can write their name inside of it.

Entitlement to this space is represented by virtual contracts known as UTXOs. We can think of this concept like a land title- it grants the owner legal right to a fixed plot of earth. What’s important to note about Bitcoin is that the total ledger space never changes; it sits there stagnant, like a parcel of land that never moves. So, when Bitcoin users broadcast transactions, they aren’t actually changing the ledger space itself. Instead, they are changing the *claims* to this space, by tearing up old UTXO contracts and drafting new ones that reassign it to a different owner.



Same aggregate UTXO value; different structure with different owners

So where do *bitcoins* (lower case b) come into play? By providing us with a novel measuring unit to numerically “weigh” any UTXO in question. We can think of bitcoins like an acre, inch or pound.

Bittrex UTXO transferred on March 31, 2019. The collective value of these bytes, specifically the ones outlined in blue, are worth ~$640M. Arguably, this string of characters is the single most valuable asset in the world.

We can say that a UTXO's value is a function of the ledger space it offers title to. But where does the ledger space derive *its* value? Why would anyone want it? It provides no "utility" in the manner we traditionally think of productive assets. Its only functionality is an ability to claim portions of meaningless digital "real estate".

Turns out this digital real estate provides a tremendous amount of utility in the context of digital scarcity. **Bitcoin's inherent value is the fact that it cannot be inflated.** Doesn't seem like much to the naked eye, but when we start experimenting, we quickly realize anything virtual is trivially replicated. 1's and 0's can be copied and pasted an infinite amount of times. If we can't introduce scarcity, a decentralized e-currency becomes an impossible feat.

Bitcoin's model is beautiful because proof-of-work, the mechanism by which all nodes update the ledger, bridges the virtual world and meatspace in sci-fi fashion. Validators using specialized computer hardware compete against one another in a game where they brute force cryptographic puzzles. These machines consume an enormous amount of capital (electricity and hardware) in the process. Some constitute this energy expenditure as wasteful; I would argue that it is transformative.

There is an unforgeable costliness associated with this structure as the destroyed resources embed themselves into the protocol, generating security and assurance. **This is what separates the authentic chain from an imposter.** I can trivially copy the bitcoin codebase, but I cannot copy the energy expended towards validating previous blocks.

In a way, we are “uploading” scarcity from the physical world to the digital realm. This allows us to numerically quantify the total Bitcoin network security in $ figures, and represents how much an attacker would need to spend to reorder the ledger. The larger this value is, the greater the assurances that the network provides, creating a reflexive feedback loop leading to more demand. Currently, we obsess over this security so greatly that we literally burn billions of dollars’ worth of natural resources in order to protect it. Think about how wild this is for a moment- and we do all this for possession of some virtual real estate inside a meaningless ledger (that itself doesn’t even really exist)!

So sure, you can try and secure money, produce, diplomas or Pokemon cards with your latest “efficient” or “eco-friendly” consensus algorithm. But these blockchains are only as strong as the opportunity cost of inputs forgone.

Like a cheap Chinese import, cost savings on the frontend reveal themselves on the backend; in our case, equally marginalized security. Owning bitcoins, in short, means possessing provably scarce lines of monetized code, tethered to billions of dollars in unrecoverable physical capital, all done as an effort to generate strong assurance.

Joe researches cryptographic protocols and is on twitter at @JKendzicky

---

How soft forks might work or fail

By Tamas Blummer

Posted April 17, 2019

Attempts to deploy a soft fork on the Bitcoin network might fail, and some will have to before Bitcoin ossifies.

I recently twitted about my anticipation of events as:

This sparked some curiosity how I meant competition and rejection, so I wrote this longer explanation.

What is a soft fork?

A soft fork is a change to network nodes such that they apply stricter rules to blocks that those that are already in effect on the network.

Nodes that do not apply the change will not technically recognize that a soft fork was deployed as blocks continue to obey all rules they know of.

Can a soft fork split the chain?

As soon as a miner produces a block that violates the stricter rules, other miners are presented with a choice, they could either:

- ignore (orphan) the offending block, means supporting the soft fork
- build on top of the offending block, means rejecting the soft fork

The chain forks once a miner choses to ignore the offending block. There is no technical difference between a fork and a split, the later merely refers to a situation where miner work on both sides of the fork for a longer period.

Such a split would be technically a really messy one, since both sides would share coins in existence before the split and use the same communication network. There would be no guarantee that a pre-fork coin would be spent only on one side (no

replay protection). An increasing and not obvious set of coins would become only valid on one side.

How splits compete and eventually resolve

Forks that are rooted in a block that is not acceptable by the soft fork will not be automatically resolved by the most total work rule. The reason is that validating nodes that support the soft fork will not even see blocks that are successors of the offending block.

The split chain can proceed on both sides until some miner work on both. The proportion of mining power is technically irrelevant to their existence. Miners will however constantly re-evaluate the situation and may with time settle on only one side, which would resolve the split.

We have not yet seen a soft fork split as recent soft fork activation via UASF successfully moved miners in sync.

A miner activated soft fork is unlikely

There are powerful arguments against supporting a soft fork by a miner

1. Avoid operational risk: A miner that does not know or care about the soft fork does not have to upgrade its systems and will reject the soft fork by just doing what it used to do.
2. Avoid financial risk: Supporting the soft fork means ignoring offending blocks, which comes with the risk that others that did not care to upgrade will build on the ignored block and thereby more likely win the race for most total work in the next round. A miner will therefore support the soft fork only if there are good reasons to assume that most other miner will also do so.
3. Avoid network disruption: An split is potentially disastrous to the value of the asset produced by the miner.

Above explains why the latest 'segwit' soft fork activation did not happen until miner were forced by UASF.

How a user activated soft fork (UASF) works or fails.

A credible threat such as the one imposed by the famous UASF (BIP148) can push miner instantly to one side and thereby avoid a chaotic resolution of a temporary split. The threat of the first UASF was that validating nodes would stick to the side of the soft fork even if majority of miner would not apply BIP141 (segwit). Miner's new coins would not had been accepted by UASF nodes if they were mined on the other side of the fork. The first UASF threat worked so well that no miner created a block offending segwit rules, the upgrade was so seamless that some think it was not soft fork (event) at all.

Orchestrating such a credible threat will get harder as the network grows. The case supporting a soft work will be less convincing for a miner and at some point they will stop considering one, at latest after one that creates a split.

And then the soft fork window will close for ever, just like that of the hard forks is closing now with the demise of the Bitcoin XXX fork coins.

The Road to $1m per Bitcoin

By Genesis Node on ALTCOIN MAGAZINE

Posted April 17, 2019

Since the peak of the Bitcoin price at around $20,000 in late 2017 and the subsequent move down to a $3,100 to $4,000 range by March 2019 much has been written and discussed about the volatility of the most established cryptocurrency. Media outlets and Nobel prize winning economists have enjoyed producing ill-informed clickbait suggesting that 'The Bitcoin Ponzi is over' or that 'The Bitcoin bubble has burst'. Over time the world will start to understand money and Bitcoin in more detail but for now, reporting and analysis by the mainstream media remains self-interested and rather sensationalist.

<Cue open-minded, altruistic sensationalism>

At Genesis Node, we believe **Bitcoin will eventually be used as a global reserve currency**and that it has the potential to either replace government-issued fiat currencies entirely or be the base money used all over the world that governments issue their own currency on top of—in other words, we see a situation where all money will be backed by Bitcoin and that Bitcoin will also replace monetary metals including gold as a key store of value and all pricing and mental calculations will be undertaken in 'Satoshis' rather than native currencies.

In our view, Bitcoin represents a fundamental global paradigm shift and to give it some form of analogy to bring this narrative to life a little it can be thought of as a monetary glacier….a gigantic force that is slowly moving through the global economic terrain, flattening and accumulating all other forms of global money and wealth storage as it goes. Bitcoin could very well culminate as a single, stable, unstoppable form of value transfer that we as a human race need to harness so we

can rebuild a better economic and financial system upon which to continue our development and societal progress.

Photo by Alto Crew on Unsplash

Now that the awkward glacier analogy is out of the way, let's explore some sensationalist click bait of our own and analyze how Bitcoin could possibly reach a **$1m per Bitcoin price or in other terms $0.01 per Satoshi**. The following article assumes that the reader has a rudimentary understanding of sound money and the challenges with the current global economic and central banking systems. If not then please take some time to read our previous article, the work of Austrian economists and the Mises Institute publications regarding sound money and the issues with government controlled money and central banking.

The following article groups the rationale for a situation where Bitcoin reaches $1m per coin as follows:

1. **Bitcoin technical enhancements and global infrastructure**
2. **Forthcoming global economic collapse**
3. **Separation of state and money**
4. **Bitcoin mass adoption**

5. **Investor speculation and return on investment shift**

A return to sound monetary measures and a separation of state-controlled money in favor of a free market approach is likely to redress the imbalances of a system that has gone horribly wrong over the last 100 years.

Quick maths (TLDR)

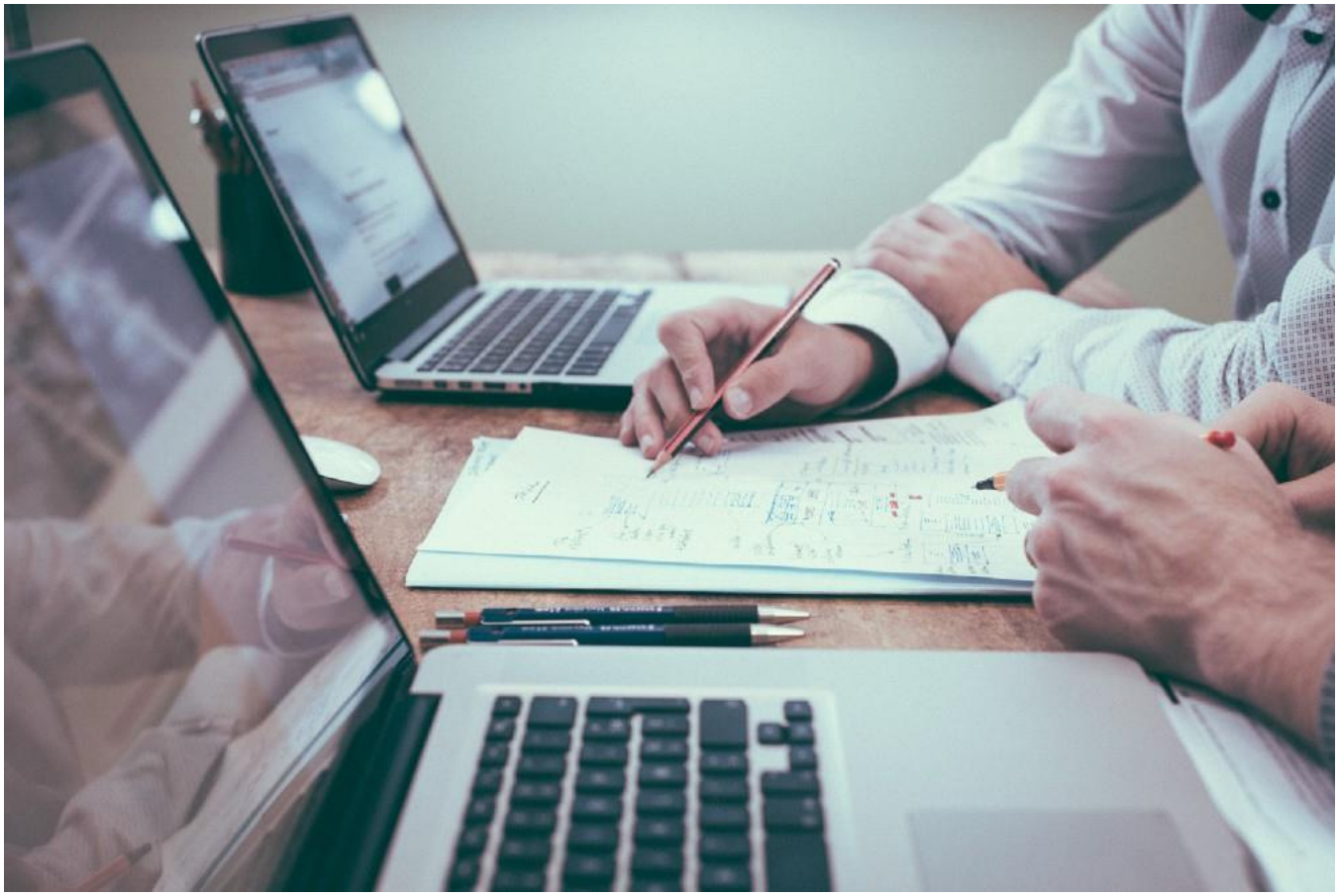


Photo by Helloquence on Unsplash

Let's apply some simple maths to the Bitcoin realm.

A $20 Trillion market cap against a Bitcoin supply of 18m coins gives a price of over $1m per Bitcoin. The current market cap of Bitcoin as of the end of March 2019 is circa $80 Billion with around 17.5 million circulating coins and the price is around the $4,500—$5,000 mark (as of April 2019). Let that sink in for a moment.

As Vijay Boyapati stated in his article 'The bullish case for Bitcoin'

"This case was made even more trenchantly by the brilliant cryptographer Hal Finney, the recipient of the first bitcoins sent by Nakamoto, shortly after the announcement of the first working Bitcoin software:" [I]magine that Bitcoin is successful and

becomes the dominant payment system in use throughout the world. Then the total value of the currency should be equal to the total value of all the wealth in the world. Current estimates of total worldwide household wealth that I have found range from $100 trillion to $300 trillion. With 20 million coins, that gives each coin a value of about $10 million.

At this point, we need to explore how the roadmap from $80 Billion to $20 Trillion and beyond might pan out and why.

1. Bitcoin technical enhancements and global infrastructure

Bitcoin is an emergent form of global money and is most easily thought of as digital gold. However its potential is far greater than that limited analogy and once certain challenges and limitations in the cryptocurrency market as a whole such as regulation, currency on/off ramps and user interface and experience (UI/UX) are overcome, the road to a $20 Trillion market cap will really begin to open up.

Photo by Bernard Hermant on Unsplash

First, the Bitcoin protocol and surrounding cryptocurrency ecosystem need to address some current limitations which will most certainly happen over the coming years. The points below explore these in more detail:

a) User interface and user experience:

The current user interface and overall user experience regarding Bitcoin are somewhat complex and to achieve full global adoption and usability this needs to improve. The current experience is akin to using dial-up internet and email for the first time in the early 1990s but as the entire industry continues to advance the end to end usability will become as simple and seamless as one-click payment solutions are today. When the experience doesn't include having to explain the importance of private keys and using cryptocurrency is as simple as connecting to free WiFi is today then we will reach the mass adoption tipping point.

b) On and off ramps:

It is getting easier to convert fiat currency into Bitcoin and vice versa and it will continue to improve as more exchanges come online and the growth of Bitcoin as a payment mechanism seeps into the mainstream. A more favorable regulatory environment will help here as will a clearer government stance on retail and institutional investing in Bitcoin and digital assets alongside a well-defined tax framework.

c) Payment use cases:

Some governments and US states have started to accept Bitcoin as a means of paying taxes already and for large scale, non-time critical purchases the use case for Bitcoin payments already exists—remember Nic Carter's analogy of Bitcoin as a ship transporting goods across oceans rather than the final mile postman delivering letter and parcels.

d) Transaction speed via Lightning network:

Micropayments will be enabled through the proliferation of the lightning network and further layer 2 and 3 solutions that help Bitcoin move up the monetary ladder from being a means of a final settlement to an effective network for transferring small, instantaneous payments from one party to another...globally.

e) BTC halving and supply model:

As the 2020 halving approaches there will be a realization that Bitcoin holds the same scarcity level (stock to flow ratio) as gold and by 2024 will be more scarce than gold. Scarcity is a key part of the Bitcoin proposition and as 1 Bitcoin can be divided into 100 million Satoshis and then grouped as required for any value of transaction it can, therefore, operate effectively as a means of exchange and unit of

account….however before that can happen the price needs to stabilize so it can pass the 'store of value' function of money.

f) Global telecommunications infrastructure:

As 5G technology starts to roll out and we see companies such as Blockstream enable Bitcoin payments via satellite it is not difficult to imagine a world where there is wireless communication capability covering every square inch of the planet. If you are able to make this mental leap and assume it happens in the next 10 years then the possibility of Bitcoin becoming a global payment system for micro-purchases with near real-time final settlement becomes a reality.

2) Forthcoming global economic collapse

Photo by Ehud Neuhaus on Unsplash

Next, we need to consider the real possibility of a forthcoming economic crash that could make 2007/2008 look nothing more than a short term set of 'bad economic data'. At present, fiat currencies fulfill the store of value, medium of exchange and unit of account functions of money however when the government and central banks operate ineffectively, fraudulently or under the illusion that printing money

through quantitative easing, undertake massive bond purchases "to increase liquidity" or other expansionary means then their currency no longer operates as it was intended—see Argentina, Zimbabwe, Venezuela, Weimar Republic and even the Roman Empire for cautionary tales and evidence on the destructive effects of currency debasement.

In essence, we believe that the world is in uncharted territory regarding debt and the burden is growing too heavy—at some point the last 100 years of Keynesian and expansionary monetary policies may fail completely and could cause one or more of the IMF SDR (Special Drawing Rights) reserve currencies such as GBP, USD, EUR, Yen or Yuan to go into a high or hyperinflationary spiral and eventually collapse. The Modern Monetary Theory view that a sovereign nation can always pay debts denominated in its own currency because it can simply print more money to do so is a catastrophically flawed argument as Economist Daniel Lacalle outlines in an enlightening interview on his website.

We are also on the precipice of banks implementing centralized digital currencies and when that happens there will be no escape for citizens to safely store their savings in the legacy retail banking system and negative interest rates are likely to be imposed, the ethics of personal privacy will be challenged significantly if not completely eroded and the opportunity to implement greater state control over citizen actions will be in place—see China right now for an example of social credit scoring initiatives that could easily be implemented in other nations;

"If an individual has a lower social credit score, they might find their ability to purchase what they want such as high-quality goods or a new home to be restricted. They might also be prohibited from buying airline and train tickets or renting an apartment. Some people with low social credit scores can expect to be blocked from dating sites and not be able to enroll their children in a school of their choice." Forbes, 21 January 2019

With state-issued digital currencies, there is also the increased risk of one-off taxes such as that experienced by Cyprus residents in 2013 to fund bailouts or any kind of national initiative against the will of the citizens without them being able to do a single thing about it.

"Under an emergency deal reached early Saturday in Brussels, a one-time tax of 9.9 percent is to be levied on Cypriot bank deposits of more than 100,000 euros effective Tuesday, hitting wealthy depositors—mostly Russians who have put vast sums into Cyprus's banks in recent years. But even deposits under that amount are to be taxed at 6.75 percent, meaning that **Cyprus's creditors will be confiscating money directly from pensioners, workers and regular depositors to pay off the bailout tab**." NY Times, 16 March 2013

This series of factors is probably the most important in the likely rise of Bitcoin as a globally accepted, sound money. As discussed in our previous article, there are significant shortcomings with the Euro currency and it is not inconceivable to think that these could well see a further fragmented and divided Europe for economic reasons. As the abstract from the paper below covering the little known 'Target2' system outlines, the debt owed by other Eurozone member states to Germany is so vast (approx €1 Trillion) that they are unlikely ever to be repaid and as such there is a real risk of significant political repercussions and a possible breakup of the Eurozone;

"Target2 is the Eurozone's cross-border payment system and is mandatory for the settlement of euro transactions involving Eurozone central banks. It is being used to save the Eurozone from imploding. A key underlying problem is that the Eurozone does not satisfy the economic conditions for being an Optimal Currency Area, a geographical area over which a single currency and monetary policy can operate on a sustainable long-term basis. The different business cycles in the Eurozone, combined with poor labour and capital market flexibility, mean that systematic trade surpluses and deficits will build up—because interregional exchange rates can no longer be changed. Surplus regions need to recycle the surpluses back to deficit regions via transfers to keep the Eurozone economies in balance. But the largest surplus country—Germany—refuses formally to accept that the European Union is a 'transfer union'. However, deficit countries including the largest of these—Italy—is using Target2 for this purpose. Further, the size of the deficits being built up is causing citizens in deficit countries to lose confidence in their banking systems and they are transferring funds to banks in surplus countries. Target2 is also being used to facilitate this capital flight. However, these are not viable long-term solutions to systemic Eurozone trade imbalances and weakening national banking systems. There are only two realistic outcomes. The first is full fiscal and political union—which has long been the objective of Europe's political establishment. The second is that the Eurozone breaks up." Blake, D. (2018). Target2: The silent bailout system that keeps the Euro afloat. London: City, University of London.

In a situation where we see global stocks and bond markets starting to stall and major issues with reserve currencies such as the Euro, we may see a significant flight of capital from retail and institutions into traditional safe havens such as Gold. At this point, it will be interesting to see whether Bitcoin has done enough to demonstrate its store of value function to carve out a portion of the 'safe haven' market.

a) Government debt levels:

Global government debt levels are now at a level that cannot be repaid. The US alone has $22 Trillion in govt debt. Keynesians and MMT advocates often argue that a sovereign nation can just print money to pay off its debts but this is simply not true

for the levels of debt governments now find themselves in and would cause a massive devaluation in the currency.

b) Expansionary monetary policies:

Since 2008 the Federal Reserve has injected $4.5 Trillion into the US economy through QE. In Europe, the ECB bought $3 Trillion of government bonds between 2015 and 2019 and in Japan the experiment with 'Abenomics' left Japan with a struggling economy and a government debt to GDP ratio of 220%. Despite all of these ineffective measures, China has now started playing the same game as the rest and in January 2019 it injected $83 Billion directly into the banking system in one day. If monetary history has taught us anything it is that printing money and debasing the value of the currency does not lead to sustained growth, it leads to the collapse of a state or even an empire.

c) Eurozone and Target2:

Target2 has become the bailout system that keeps the Euro afloat. The German Central bank (Bundesbank) is owed almost €1 Trillion and Luxembourg is owed c€200 Bn by Eurozone member states as a result of the Target2 system. Italy, Spain, Greece & Portugal owe the most and it is not clear whether these figures can be repaid. It is possible that a default by these countries to the European Central Bank could take place and they would, in turn, struggle to meet obligations to creditor nations such as Germany. Trillions of debt contracts would be called into question. There are two possible options: (1) A full political European Union with common fiscal and monetary policy is implemented; (2) The Euro currency failings drive political divisions and an eventual break up of the Eurozone

d) Household debt:

At the end of 2018 US household debt stood at over $13 Trillion with around $4 Trillion of that figure relating to non-mortgage related debt. Warning signs are creeping into the economic forecasts through record levels of automobile loan defaults. Whilst unemployment is at record lows, wages are stagnant and exposure to debt is increasing, the horizon is not looking good.

e) Negative interest rates and central bank stock purchases:

Central banks are running out of tools and options to stimulate growth in flagging economies worldwide and many Economists argue that the next step should be to print more money to purchase stocks and shares directly—a false underpinning of a broken system. With proposals to implement negative interest rates being

considered to encourage savers to take their money out of banks and spend or invest it or risk it being eroded away there appears now to be little room on the runway.

3) Separation of state and money

Photo by mahdis mousavi on Unsplash

It was only during the early part of the 20th Century that there was a real unification of state and monetary control. It is true that the ruling classes of old taxed their citizens to raise funds for the crown and subsequently wage wars and build infrastructure. However, alongside this direct taxation, money operated in a free market environment which allowed the commodity with the most attractive qualities fulfilling the store of value, medium of exchange and unit of account functions to be selected for use by the market.

Often, there were many localized markets and thus, localized, free market selections of 'commodity money' such as Yap stones on an island the Pacific Ocean, glass beads and seashells in West Africa and many societies often used salt as a means of payment. So the modern concept of a centrally managed economic system with control of the currency linked directly to the whims of government and central

banking authorities is a relatively new phenomenon that has led us to the edge of another global economic crisis (see section 2).

The time is now right for a separation of state controlled money and a return to a free market economic system that allows governments to tax their citizens but not to control the output and quantity of currency available in the economy—a return to sound money.

It is not obvious where the incentive is for a government to support a return to sound money as they have a much greater sphere of influence and control over the citizens living within their borders if they retain a state influenced money through a central banking entity. Some nations may start to stockpile gold and Bitcoin as a hedge against a failing global system but this is different to supporting a full move to a 1–1 link between the hard currency (Gold/Bitcoin) and a state-owned fiat currency that they can print and devalue at will at the expense of the citizens.

As Economist Daniel Lacalle states in his book 'Escape from the Central Bank trap', "The search for ways to preserve wealth in a society which owns most of it in deposits makes citizens seek any way to avoid the assault on their savings from the massive printing of money through increase of money supply. For this reason, the search for a currency whose control is not in the hands of States has been a constant in preserving capital for many years now"

4) Bitcoin mass adoption

Photo by Tom Grimbert (@tomgrimbert) on Unsplash

At present Bitcoin is complex to understand, difficult to use for everyday purchases and puts the security of wealth storage entirely in the hands of the user without legal recourse or insurance protection (NB: Some custodian services do exist that offer a level of insurance against loss or theft). As the technical enhancements are deployed and the benefit of a sovereign, uncensorable, uninflatable currency start to become more evident then we will see a gradual rise in the number of people who store their wealth and choose to transact in Bitcoin. For people in countries where their currency becomes an ineffective means of wealth storage due to high or hyperinflation, it is likely that we will see a greater rate of adoption and day to day use—see the current situation in Venezuela. In addition, countries facing sanctions and embargoes by other nations may choose to adopt Bitcoin as a store of value alongside gold or encourage their citizens to transact and pay their taxes in Bitcoin. Ultimately a bottom-up (people led) adoption of Bitcoin is more likely to occur than a top-down (government-led) approach but once one central bank and government

announces that they recognize Bitcoin as money and a legitimate currency then this is likely to cause a significant global institutional race to acquire Bitcoin and use it in a mix of sound money with central bank gold reserves.

A recent essay by Wences Casares, CEO of Xapo covers a detailed overview of Bitcoin and his belief that in 7–10 years Bitcoin could be worth $1m per Bitcoin.

“In a world in which Bitcoin succeeds all currencies may be quoted in satoshis (the smallest fraction of a Bitcoin). When your granddaughter asks what is the price of the New Zealand dollar she may receive an answer in satoshis: the New Zealand dollar is 72 satoshis today. And the price of the Turkish Lira? 21 satoshis today. The US dollar? 107 satoshis today. A barrel of oil? 5,600 satoshis today. Global GDP? 97,356,765 bitcoins. The GDP of Indonesia? 1,417,007 bitcoins. The reserves of the South African Reserve Bank? 53,230 bitcoins. You get the idea. Then all of these values would be easily comparable across time and across geographies.”

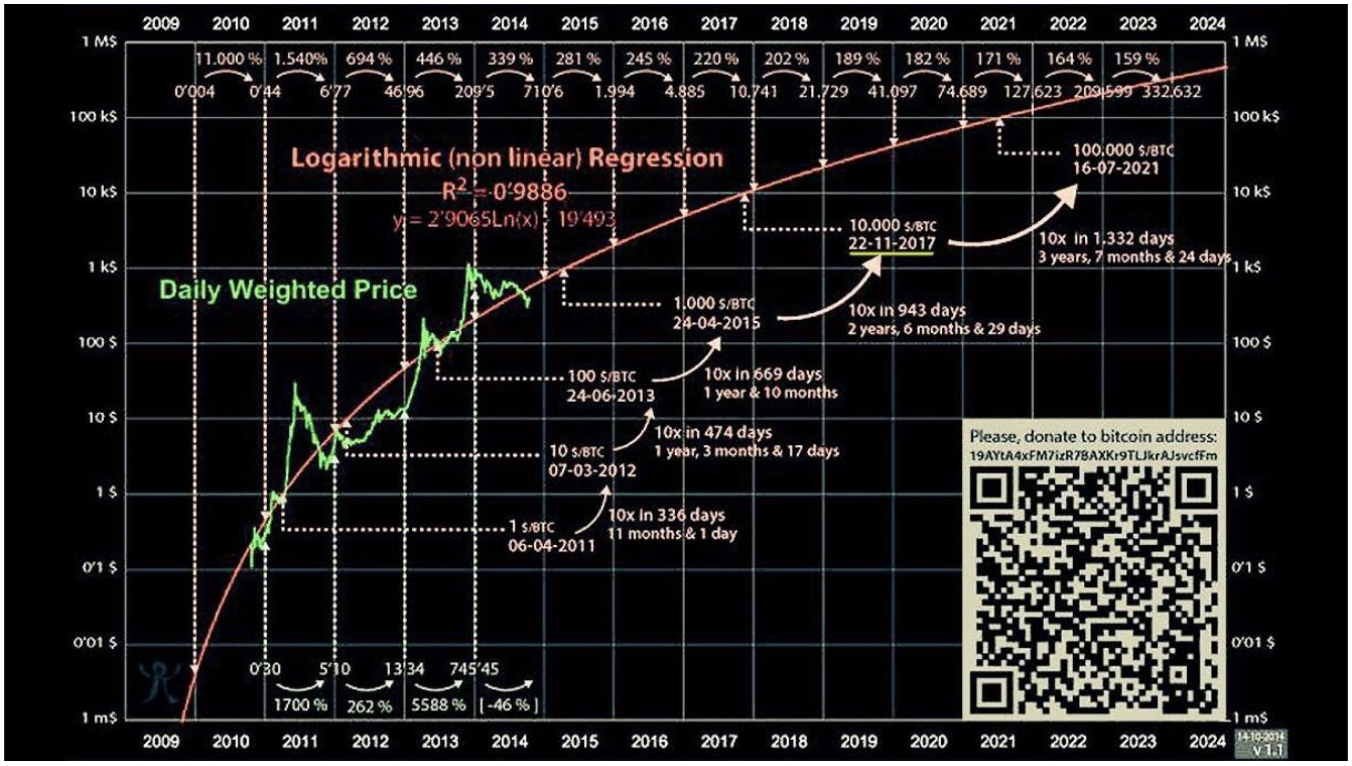
5) Investor speculation and return on investment shift

All the above could well lead to a reduced role for the government from a fiscal policy and planning perspective as less central co-ordination would be needed and citizens would be able to save their wealth in an uncensorable currency that does not have its value eroded through inflation or unsanctioned government taxation. Furthermore, all kinds of speculative investment sectors start to lose their shine as there is no longer the need to risk capital in the stock market, real estate or other markets and instead, global citizens can store their earnings in their private wallet and watch it retain its value or even appreciate in value over time. This could, in turn, lead to an exodus of investment and a global rebalance of real estate values to a more normalized market-driven level reflecting the cost of production, quality, scarcity, location, and desirability instead of artificially inflated markets due to speculation-driven price rises. Speculation will remain prevalent, however, it is simply the volume of speculation that could reduce as investors chase and are able to achieve a higher and safer return by storing their wealth in Bitcoin rather than real estate.

Photo by Benjamín Gremler on Unsplash

Underlying number assumptions

The chart below is from 2014 (unknown creator) and outlines a simple path to almost $1m per Bitcoin, the scary part is that it accurately forecast a $10k price in November 2017. As of March 2019, the forecast is behind this view however it will be interesting to see if price catches up to this projected trend line over the coming months and years—one to keep an eye on.



Unknown creator — please advise and we will credit them

If we look at some potential scenarios we can see different implied market capitalization values and subsequent Bitcoin prices. The low scenario models Bitcoin capturing a 20% market share of each of the sectors on the left, Medium a 50% market share and High a 100% market share.

		Scenarios		
Sector	$ value	Low (20% market share capture)	Medium (50% market share capture)	High (100% market share capture)
Currency	7,600,000,000,000	1,520,000,000,000	3,800,000,000,000	7,600,000,000,000
Central Bank gold holdings	1,300,000,000,000	260,000,000,000	650,000,000,000	1,300,000,000,000
Global stock markets	69,000,000,000,000	13,800,000,000,000	34,500,000,000,000	69,000,000,000,000
Professionally managed global real estate	8,500,000,000,000	1,700,000,000,000	4,250,000,000,000	8,500,000,000,000
Art investment market	63,700,000,000	12,740,000,000	31,850,000,000	63,700,000,000
Classic car investment market	880,000,000	176,000,000	440,000,000	880,000,000
TOTAL	**86,464,580,000,000**	**17,292,916,000,000**	**43,232,290,000,000**	**86,464,580,000,000**
Bitcoin price	Assuming 18m circulating supply	960,718	2,401,794	4,803,587

Copyright Genesis Node 2019

The low figure is in our view a possible scenario that could occur. This would see Bitcoin absorbing 20% of global coinage and currency (paper and digital), 20% of the existing gold reserves held by Central banks or instead of buying more gold year on year central banks could switch strategy to start accumulating a position in Bitcoin on top of their current gold holdings. Stock market values reflect the value of all the public listed companies in the world—whilst in reality, this figure will not reduce completely as companies will always retain value based on assets, financial performance and returns to shareholders and investors. We could, however, see an ***exodus of speculators*** as previously mentioned who could keep their savings in a lower risk commodity such as Bitcoin (not yet but in time as the volatility decreases) which over a longer timeframe is likely to outperform the stock market—we therefore feel a 20% shift of capital out of stocks and into Bitcoin is achievable, after all, Bitcoin is the single best-performing asset in the last 10 years. It is inaccurate to include the full $69 Trillion market cap of global stock markets though so let's rule out the high column of $4.8m per Bitcoin in this analysis.

The $960k figure in the low scenario would increase to $1.2m per Bitcoin if it was to absorb the full $7.6 Trillion in circulating currency and all goods and services worldwide were priced in Bitcoin or Bitcoin were used to back fiat currencies.

Whilst this is incredibly high-level analysis/numberwang it outlines the monumental steps and hurdles that Bitcoin needs to take to meet targets such as $1m per Bitcoin

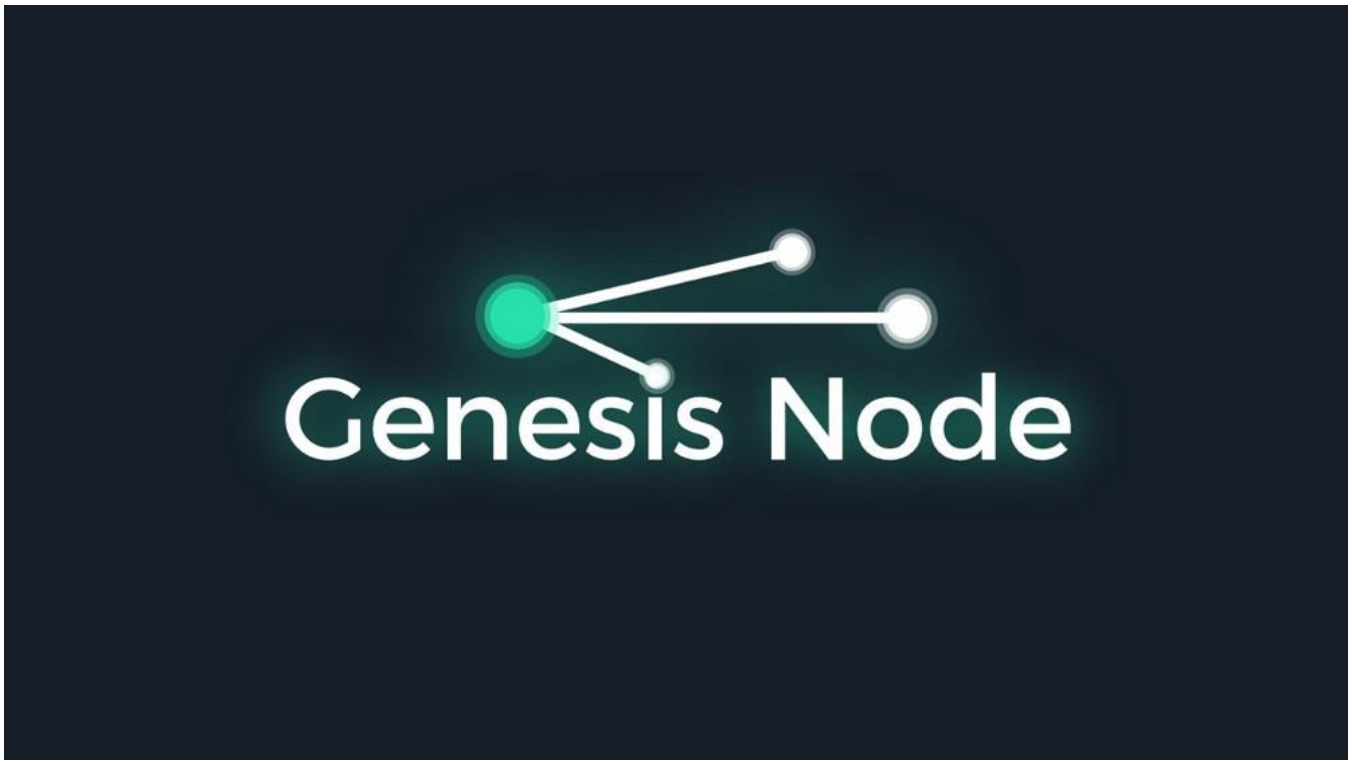
and beyond. That said, the fact that Bitcoin has survived 10 years already, is now next to impossible to hack, has suffered nation states banning their people from using it and poorly claimed links to money laundering and criminal activity there is a very high chance it will survive indefinitely.

Whilst that seems challenging at present, to believe that Bitcoin can reach $1m it may ***only***take the collapse of the Euro, a devaluation and rapid global sell-off of the USD and other currency capitulations in light of the massive economic risks and global debt bubble for Bitcoin to acquire 20%-50% of the global value of circulating currency which would propel it well on the way to a $1m per Bitcoin valuation. These things do not have to happen all at once or even over a short timeframe, but history and current economic policies worldwide suggest that there is a chance that they will happen and if they do we will gradually see Bitcoin acquire more and more value for the long term. It would be wrong to double count the allocations of institutional investors into the calculations above but if you assume that at present they do not yet have an average position of 10% (most are likely to be at 0–1%) of capital under management due to a lack of understanding and the challenges of approving investment decisions through boards and trustees into an asset class that is not well understood and highly volatile then the subsequent price rise that will come when institutions start to buy in via small positions will be enormous. An ETF approval by the SEC in the US is likely to start this wave of investment and whilst no firm date is confirmed it is likely that by the end of 2020 an institutional grade ETF investment vehicle will be in place.

Using different metrics and rationale the Xapo CEO, Wences Casares outlines his views on the future potential for Bitcoin in his essay '[The case for a small allocation to Bitcoin]';

"How much a Bitcoin may be worth if Bitcoin succeeds is pure speculation. Today Bitcoin is worth a total of ~ $70 billion (~ 17.5 million bitcoins in circulation x ~ $4,000 per Bitcoin). If Bitcoin ever becomes the world's standard of value and settlement it may have to be worth more than gold and less than the world's narrow supply of money. All the gold that was ever been mined is worth ~ $7 trillion the world's narrow supply of money is ~ $40 trillion. If Bitcoin is ever worth as much as gold each Bitcoin would be worth ~ $300,000, and if Bitcoin is ever worth as much as the world's narrow supply of money it would be worth ~ $2 million."

The table above and comments from the CEO of Xapo is nowhere near exact science however, they are simply an illustration of the steps that need to be taken for Bitcoin to reach certain price levels. On one hand, the current $4,500—$5,000 price per Bitcoin looks like a snowball when compared to the slow moving but non-stop all-consuming glacier that is Bitcoin but on the other hand, it can be argued that the price of Bitcoin is the least interesting aspect about it.



Copyright Genesis Node 2019

References

- Blake, D. (2018). Target2: The silent bailout system that keeps the Euro afloat. London: City, University of London
- Escape from the central bank trap—Daniel Lacalle
- The bullish case for Bitcoin—Vijay Boyapati
- The case for a small allocation to Bitcoin—Wences Casares

Chinese Social Credit Score: Utopian Big Data Bliss Or Black Mirror On Steroids? *By 2020, the Chinese social credit score system will be fully operational and have searchable records and a social...* www.forbes.com **Facing Bailout Tax, Cypriots Try to Get Cash Out of Banks** *For an updated version of this article, click here . ATHENS - In a move that could set off new fears of contagion...* www.nytimes.com

Sources for the Bitcoin price table:

Home - The Money Project _ All of the World's Money and Markets in One Visualization_money.visualcapitalist.com **Global real estate investment market increases to $8.5t in 2017 | News | Institutional Real Estate...** *The size of the professionally managed global real estate investment market increased from $7.4 trillion in 2016 to...* irei.com **Art Market Grew to $63.7 Billion in 2017, and Other Key Takeaways from Art Basel Report** *Some of the more intriguing findings are mined from the data on Artfacts.net, which has tracked openings and closings...*

www.artsy.net **Classic cars top alternative investment asset classes, with 192pc growth in 10 years** *Classic cars continue to power ahead as one of the top-ranking alternative investment assets, with growth of 192pc over...* www.telegraph.co.uk

---

An Open Letter On Scaling Bitcoin

By Joseph Dallago

Posted April 22, 2019

This is in response to Nic Carter's piece, How to scale Bitcoin (without changing a thing).

Open letter to @nic__carter,

I just got around to reading your piece on scaling Bitcoin via institutions, and it has quickly skyrocketed to one of my favorite essays in the space in recent memory. I think it's a brilliant piece of work. It distills a lot of the current conversation around an important question:

What role do institutions play in the future of sending and storing cryptocurrency?

I have pondered this question a lot, as I operate a regulated cryptocurrency exchange in the Middle East(@rainfinancial). This question contemplates the role of my business 10–20 years from now, so you can be sure that our team has thought this through carefully. Hal Finney's predictions about "Bitcoin banks" had an influence on me personally as well, and I still find his opinion to be the most practical/realistic take on how to scale this technology.

For me, this conversation mainly starts with what consumers need and want. I also tend to draw heavily from the historical context that we are operating in, as I have found that companies that ignore past learnings tend to repeat them. A position that Hegel knew well and would respect.

The idea that everyone is going to want to embrace the "not your keys, not your coins" mantra has always been impractical for today's market, in my mind. Many people lack the technical expertise to setup a hardware wallet/non-custodial wallet

or care to take on the cognitive load of learning to do so. In our user research at Abra, we found that having users manage the security of their money via backup phrase is not a light ask for the great majority of the population. I remember one person in particular saying something along the lines of "So you are telling me that if I lose my phone, I will lose all of my money? Are you kidding me?" As an industry, we cannot ignore that holding custody of one's own money can be a huge barrier to entry for people.

In summary, I tend to believe that:

Most people do not want to manage the security of their money.

I think this is true today and barring any major unforeseen technological advances, I think this will be true in the near-term future as well. The great majority of people do not want to even confront the possibility of their hard-earned savings being lost or stolen. Safeguarding customer money is probably the most valuable service that banks provide, and I think consumers will continue to expect and favor it. This is especially important for high net individuals and institutions. If you have 50 MM under management, you absolutely want a team of people who are skilled enough to ensure that it cannot be lost or stolen and who have insurance to cover losses if something were to go wrong.

You could look at the growth of retail banking over the last 500 years as being a testament to this. I would love to see what the reality was like before banks were the main custodians of money. It would probably enlighten us to the market forces that resulted in people trusting banks with custody of their money in the first place.

This custodial model is not unique to financial markets. The technology market has also converged on such a model for our data. Think about:

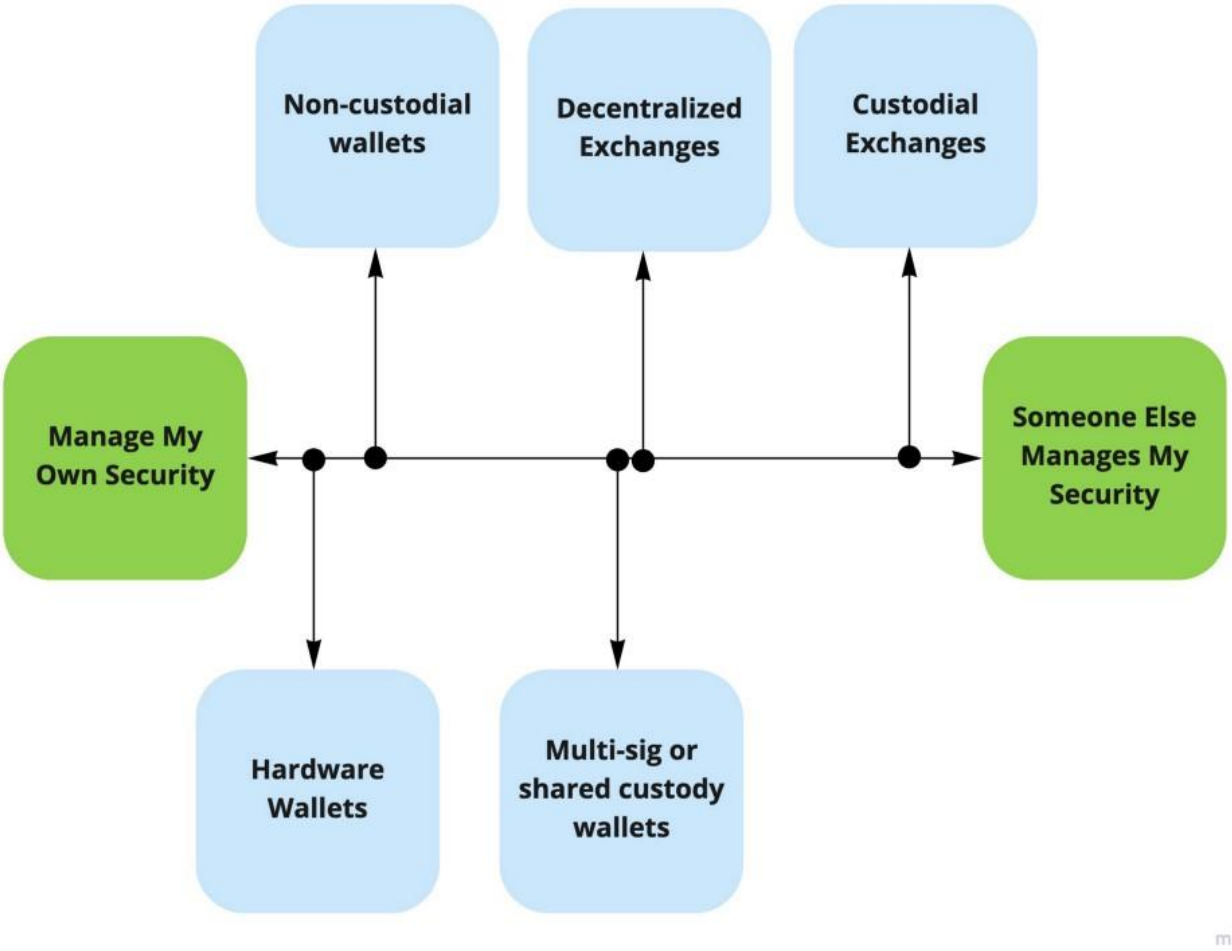
- AWS storing data for some of the world's largest companies
- Cloud services like Dropbox, iCloud, and Google Drive backing up all of our company files and data
- Most social media, email, and video content being hosted by centralized parties like Twitter, Google, and Facebook
- Most games now auto-save to the cloud instead of having manual save points stored on memory cards

Many in the community would decry this list as the source of an underlying problem, but let's not forget why we ended up here. Do you remember what it was like having a computer die or your phone fall in a pool before cloud backups? It sucked. Two anecdotal stories:

- Growing up, I used to write a lot on my mother's old HP laptop. Eventually the laptop did not start one day, and I lost a good deal of my writing from elementary and Middle School. I also cannot tell you how many times I had to save incrementally, for fear of a crash annihilating all of my previous work.
- I was mugged in Chicago one night and had my phone stolen. iCloud was not as popular back then, so I lost a good portion of the pictures from the first 6 months of my relationship at the time. Not fun.

This was the reality before cloud backups. We have spent the last 20 years developing easy ways for people to backup their data in the cloud for a reason. It is much more convenient and means that data loss happens far less often. It is hard for me to imagine a world where we just reverse all of that learning. I will not belabor the point by bringing up the countless stories of the elderly, unsavvy, or unlucky losing access to huge amounts of Bitcoin over the last 10 years.

All of this being said, I think one of the reasons cryptocurrency is incredibly innovative is that it provides people with a **diverse spectrum of options** between managing your own security and taking on unnecessary custodial risk:



Do not think too deeply about the relative placement of each option, I am more so just highlighting that it's a spectrum.

I think we have yet to discover the distribution of people within this spectrum, but I appreciate that it gives people options, as opposed to a system that presents only one option which is "trust me with all of your money". I have faith that non-custodial and hardware wallets will continue to get easier and serve the "manage my own security" crowd better and better. With new UX paradigms being discovered and technology developed, I believe they can even start serving a larger percentage of the masses as well. At the same time, I believe that a portion of users will always want to have someone else manage the security of their money.

The problems with traditional banks do not stem from the fact that they provide custodial services to customers, they stem from the monetary policy underneath. As you mention in your piece and as Hal Finney mentioned, the problem with banking is not inherent in fractional reserve, it stems from the fact that there are no penalties for big banks behaving badly. Fractional reserve should be far a more risky practice

than it currently is. In fact, the current financial system does not stop nations from behaving badly either. If a scarce asset were backing the entire system, banks and nations would be held accountable like individuals are. Your suggestions on Proof of Solvency could be a great method of holding such institutions accountable.

Put another way, the value of cryptocurrency is so much more than the ability to hold custody of your own money.

Although I believe that institutional scaling is a very practical way to scale the system, I think the designers of most cryptocurrencies have their head in the right place. I think we need to shoot for the moon in terms of decentralized custody, especially when it comes to money. We will undoubtedly fall amongst the stars due to consumer demand, but at least we are able to achieve the greatest spectrum of options available to us. Which is why I completely support the work of groups like BRD, Blockstream, and Lightning Labs who are making cryptocurrency reliant on centralized custodians as little as possible.

P.S.—I did not focus on the sending of cryptocurrency, as I interpreted your piece as mainly focusing on how institutions could store cryptocurrency, while also not repeating mistakes of the traditional system around accountability. I think it is clear that we will need layer 2 solutions to achieve the level of transaction volume and to support micro-transactions no matter what. It is merely a question of if individuals or institutions will be the predominant users of such a system.

This Key Part Of Bitcoin's History Is What Separates It From Competitors

By Kyle Torpey

Posted April 23, 2019

There are thousands of different cryptocurrencies in existence today, but bitcoin is still king. In addition to a community ethos that prioritizes stability and soundness over implementing experimental new features, there is one particular event in Bitcoin's history that clearly illustrates why it is still viewed as the gold standard of cryptocurrencies. In 2016, code that was intended to lead to the activation of a Bitcoin improvement known as Segregated Witness (SegWit) was made available via a new release of Bitcoin Core. At the time, this was mainly viewed as nothing more

than a technical upgrade (although there was some disagreement regarding how the upgrade should be implemented) that would bring a variety of benefits to the network, including laying the foundation for layer-two payment protocols like the Lightning Network.

However, the activation of this seemingly innocuous technical improvement eventually became highly politicized. This politicization of SegWit was recently discussed during a panel at the Understanding Bitcoin conference in Malta.

SegWit Gets Political

"I would say overall that SegWit itself, even among miners, was not really all that controversial in it of itself so much as some miners also wanted a hard fork block size increase at the same time, which is for a number of reasons much more difficult than a soft fork. Hard forks require — there's a lot more things that can go wrong essentially there," explained James Hilliard, a bitcoin mining software developer and consultant.

It was Hilliard's Bitcoin Improvement Proposal 91 (BIP 91) that would eventually help prevent a split of the Bitcoin network caused by differing visions of how the system should scale to accomodate more users. The two main scaling proposals at the time were (1) a user-activated soft fork (UASF) of SegWit via Bitcoin Improvement Proposal 148 (BIP 148) or (2) a combination of a soft fork activation of SegWit once 80 percent of the network hashrate had signalled their readiness for the improvement combined with a hard-forking increase to the block size limit.

The second of those two proposals came out of an infamous meeting of bitcoin stakeholders and company representatives during the Consensus 2017 conference. Other individuals and companies eventually announced their support for the proposal by adding their names to the public version of the so-called New York Agreement.

BIP 148 on the other hand was a proposal from a single pseudonymous developer named Shaolinfry.

Shaolinfry's proposal to simply activate SegWit won out over a plan from some of the largest companies in the Bitcoin ecosystem.

Hilliard's solution combined these two proposals on the basis of what they had in common: the activation of SegWit via a soft fork.

"[BIP 91] was designed to activate, assuming enough miners ran it quickly, before the user-activated soft fork date," said Hilliard. SatoshiLabs CEO Marek "Slush" Palatinus, who created the world's first bitcoin mining pool known as Slushpool, agreed with Hilliard's assessment of how SegWit became politicized.

"We were in favor of UASF because we believed that SegWit is actually not controversial and it was just misused for some political gain," said Palatinus.

Bitrefill CCO John Carvalho also agreed and explained that the key mistake developers had made was to use Bitcoin Improvement Proposal 9 (BIP 9) for SegWit's activation process.

BIP 9 is an activation method for soft fork upgrades that requires 95% of the network hashrate (miners) to signal support for an improvement before it activates. Although this was mainly intended to be a mechanism to ensure that miners were upgraded before a soft fork was activated (non-upgraded miners could end up mining invalid blocks after activation), some miners took this as an opportunity to reframe the

process as a vote among miners to decide whether or not SegWit should be allowed to activate on the network.

“It put too much power in the hands of the miners. And so, this caused political tension,” said Carvalho.

Due to these issues with BIP 9, some Bitcoin Core contributors have indicated this activation mechanism may never be used again.

UASF Defines the Roles of Miners and Node Operators

According to Carvalho, the initial UASF proposal for SegWit was a response to the politicization of the activation process by miners.

“UASF was basically a way for the nodes to express themselves and say, ‘Miners, we only want these kinds of blocks, and if you don’t give us these kinds of blocks, your blocks will be rejected,’” explained Carvalho.

In Carvalho’s view, this clearly defined the roles of miners and node operators in the Bitcoin network.

“Nodes are demanding blocks from miners and miners are supplying blocks — nothing more . . . If the market decides that it wants certain types of blocks with new rules, added rules, then the miners have to capitulate. And UASF never actually had to activate. They capitulated before because they knew that if they let it actually happen, there would be chaos for themselves,” explained Carvalho.

No2x

While Hilliard’s BIP 91 solution allowed everyone to stay on the same page over the short term, those who had signed the New York Agreement were still planning to push forward with a hard fork attempt later in the year. However, the planned hard fork attempt was abandoned after it was made clear via a futures market on bitcoin exchange Bitfinex and other data points that the new 2x chain forked from Bitcoin would not have sufficient economic support.

According to Bull Bitcoin CEO Francis Pouliot, this was the moment in time that made it crystal clear all users, not just miners, are in control of Bitcoin’s consensus rules (see this previous post from that time period on this point).

“We now can point to a specific point in time, an actual event (No2x). It’s proof. It’s proof that the miners don’t decide the rules,” said Pouliot during the Understanding Bitcoin panel.

“As far as I’m concerned, conceptually, the main difference between Bitcoin and, for example, Ethereum in terms of consensus is No2x,” Pouliot continued. “2x would

have happened on any other blockchain, and it didn't happen on Bitcoin. And it was a very defining moment for Bitcoin in terms of that aspect of the governance."

In other words, Bitcoin has proven itself sufficiently decentralized in order to resist perceived corporate takeovers by the largest wallet software providers, exchanges, and miners in the industry (see this point for an explanation of this point in further detail). No other cryptocurrency has faced this sort of test up to this point.

The closest thing to an equal test experienced by an altcoin would likely be the pressure Ethereum users faced to hard fork in reaction to the hacking of The DAO. In the end, the hard fork was implemented and the vast majority of users followed (leaving a minority on the chain now known as Ethereum Classic).

It should be noted that Ethereum's test was relatively early in the development of that particular cryptocurrency network, so it's possible Ethereum has become more resistant to these sorts of social or political pressures. Having said that, it's difficult to judge how much sway important actors in the network, such as the Ethereum creator Vitalik Buterin and blockchain technology firm Consensys, still have when it comes to hard forks.

Bitcoin fundamentals continue to strengthen

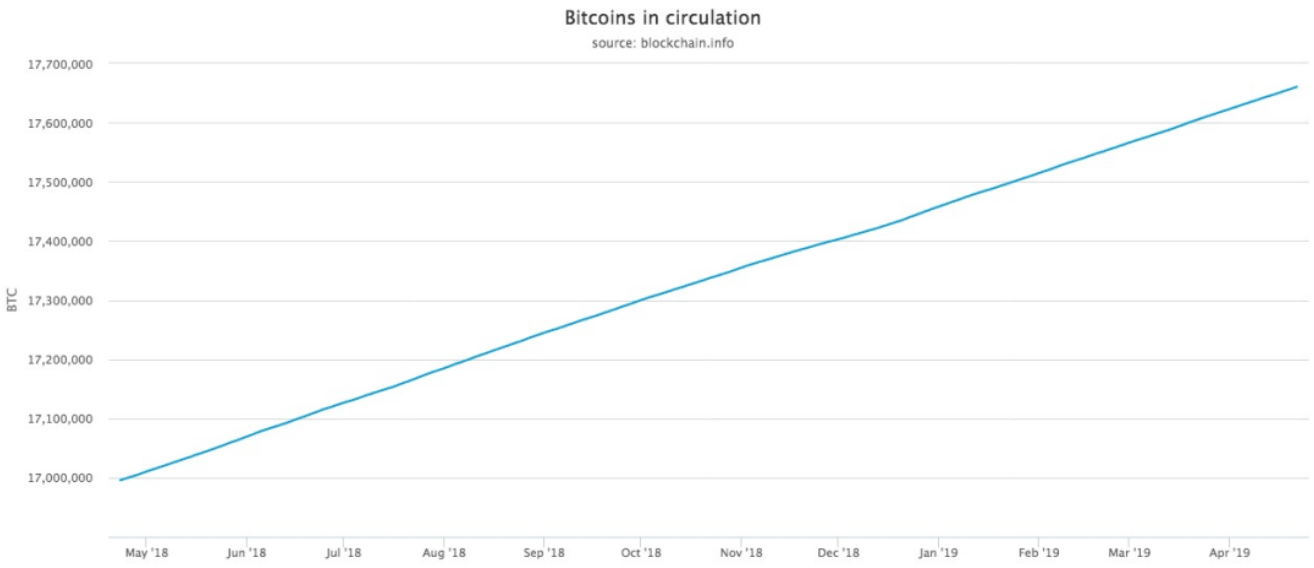
By Anthony Pompliano

Posted April 23, 2019

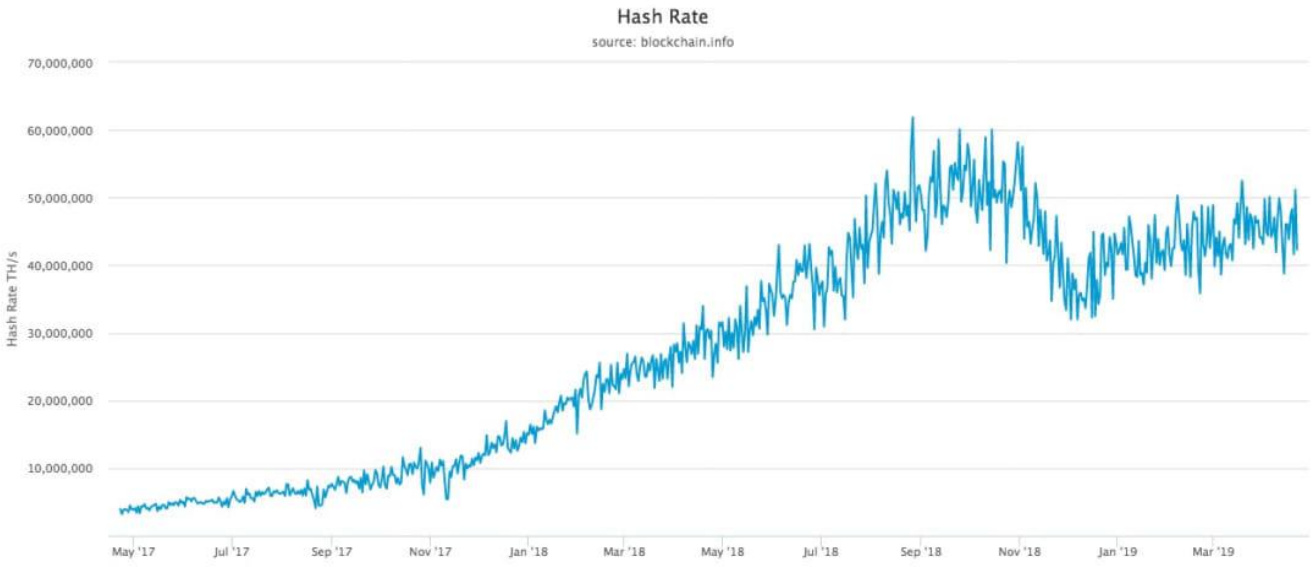
Bitcoin's price is up almost 50% since the start of 2019. Instead of obsessing over the volatile price movements, it is important to stay focused on the underlying fundamentals of the transaction settlement network.

Here is the current state of Bitcoin's fundamentals:

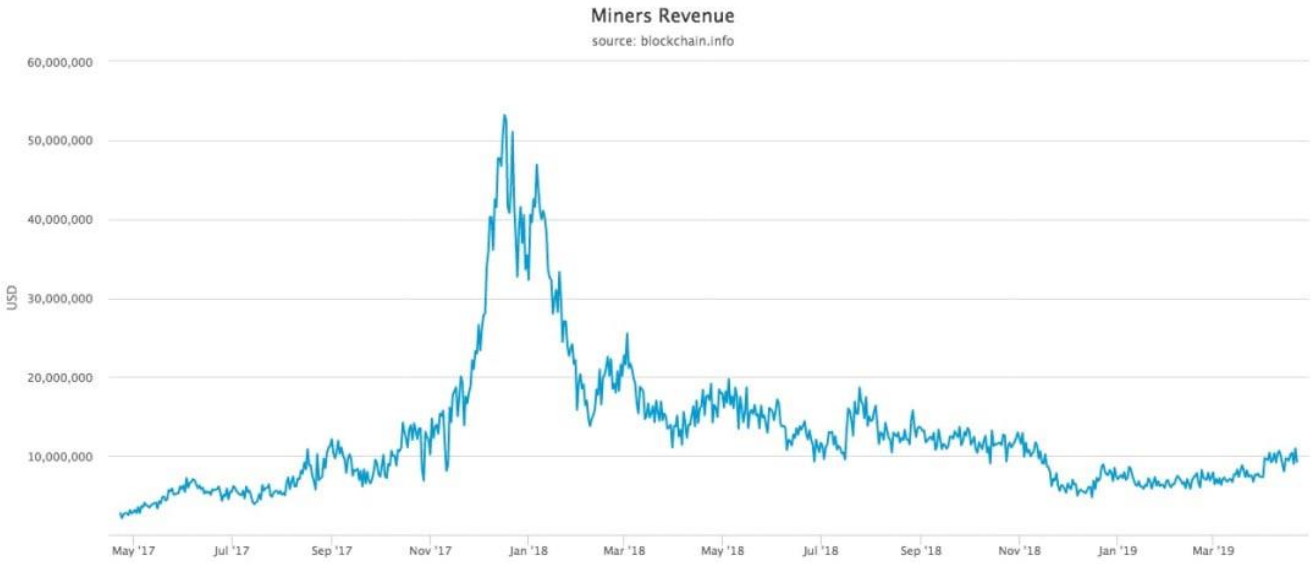
There are just under 17,700,000 of the 21,000,000 total Bitcoins in circulation.



The hash rate securing Bitcoin's network has increased more than 10x over the last two years.



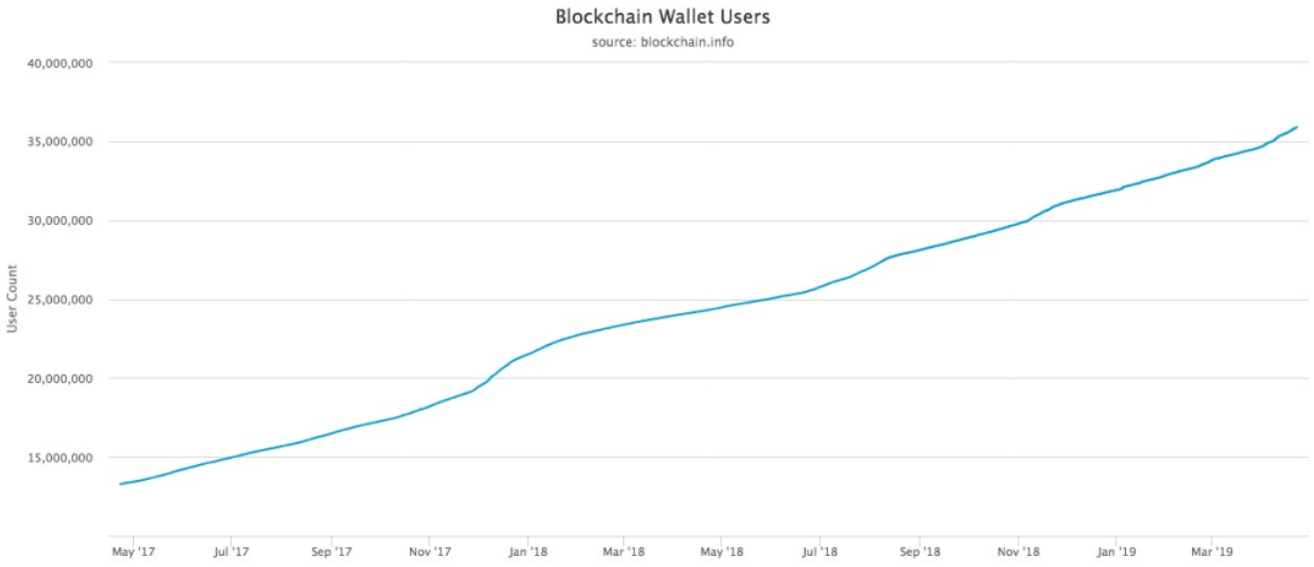
Miners are making almost 3.5x more Bitcoin (in USD value) on a daily basis than they were two years ago.



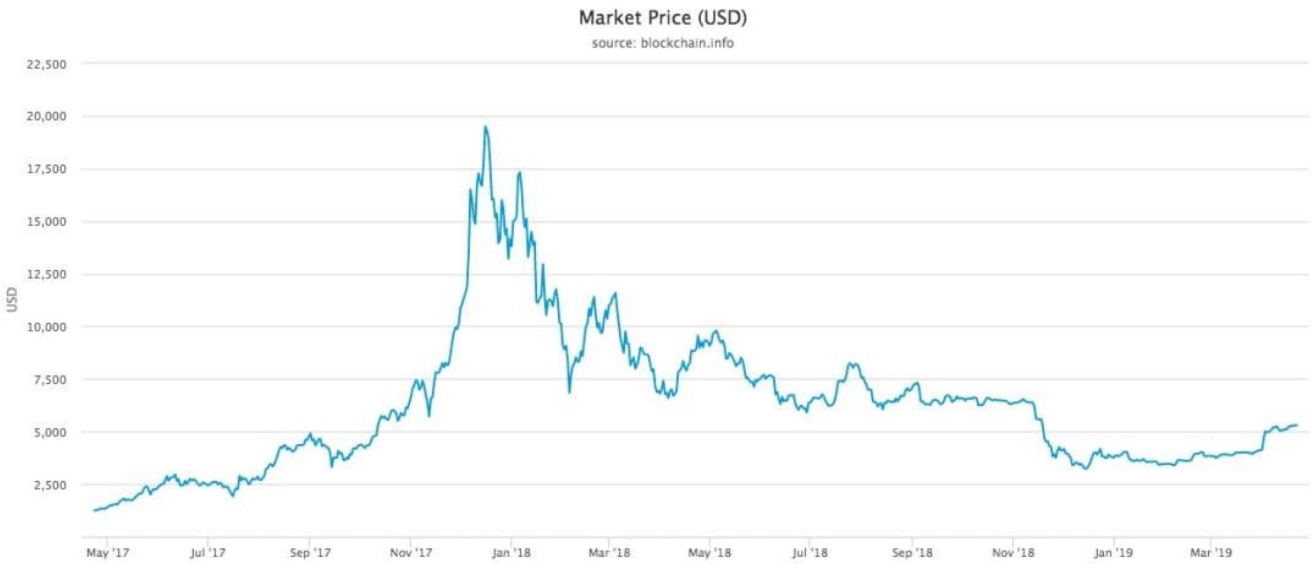
The cost per transaction has more than doubled in the last two years, but has fallen more than 60% over the last 12 months.

The number of transactions per day on the Bitcoin blockchain have increased over 70% in the last two years and continues to rise over the last 12 months after hitting a local low point in May 2018.

The total number of Bitcoin blockchain wallets has increased over 2.5x in the last two years.



With more computing power securing the network, and more users holding & transacting the scare, decentralized digital currency, it is no surprise that an individual Bitcoin is worth more than 440% today than it was two years ago.



Bitcoin is a highly volatile asset. It is misunderstood by many. But one thing is certain, the digitally native currency continues to strengthen over time. As with anything important in life, the maturation and mass adoption of Bitcoin will take time.

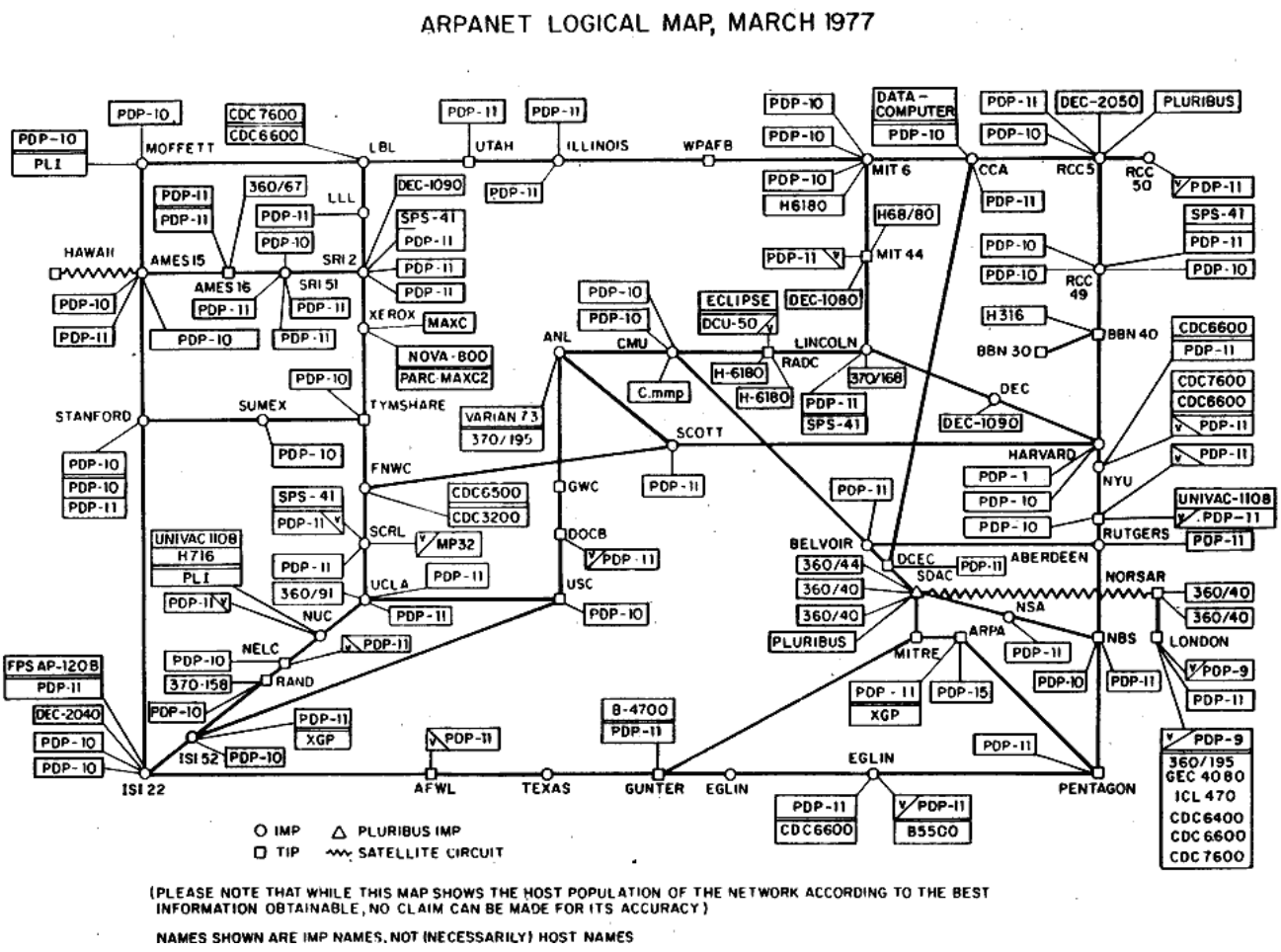
Those that have the patience and discipline to stick around will be rewarded handsomely.

-Pomp

A Monetary Layer for the Internet

By Thib

Posted April 24, 2019



Source: Wikimedia

ARPANET's First Mark into Networked Computing

Created in February 1958, the Advanced Research Projects Agency (ARPA) was a response to the Soviet launch of Sputnik 1, the first artificial Earth satellite, to research and develop projects in technology and science, beyond direct US military applications. Bob Taylor, an ARPA computer scientist convinced a colleague to support a research project using funding from a ballistic missile defense program. Following three years of research, the ARPANET project was launched as the first network to connect two geographically-distinct computers. In 1969, on October 29th at 10:30 PM PST, the first successful message '*LO* ' was sent from UCLA in Los Angeles to Stanford in Silicon Valley. The message was supposed to be '*LOGIN* ' but the system crashed. Over 7 years later, Queen Elizabeth II was sending her first email from a computer installed in the UK. The ARPANET was morphing into a small but fast-growing global network of connected computers.

Rising Computer Network Protocols

The ARPANET was the first public implementation of TCP/IP, two major protocols that now form an integral part of the Internet Protocol Suite. Taken together, this suite constitutes what we know as "the Internet", the global interconnected network that hundreds of millions of humans use daily without ever being aware of it.

As additional computer nodes joined the ARPANET in different countries, novel technologies were developed to make the growing network more usable, notably standard network protocols.

Public computer protocols were created to govern how data is created, exchanged and interpreted between clients and servers on the same interconnected network, including Simple Mail Transfer Protocol (SMTP) to send and receive emails, File Transfer Protocol (FTP) to exchange and read files or Hypertext Transfer Protocol (HTTP) to structure and display web pages that we browse today.

HTTP is one of the most well-known public protocols. It turned ARPANET into the World Wide Web that is now commonly called the Internet or the web and established a standard for computers to communicate on the application layer of the Internet, having built on other layers of public protocols and open-source technologies.

The Internet's Onion Shape

The Internet is built in layers, abstracted in a framework called the Open Interconnection System (OSI) model. It is a logical construction that defines network communication used by various computer systems that interact with each other.

As the Internet morphed into a more sophisticated global network of computers, the OSI model was published to help decouple seven distinct layers of public protocols useful in the creation, exchange and interpretation of data flows.

As a hierarchical system, public computer network protocols coordinate how data moves across the Internet's seven layers. Each layer is solely responsible for performing assigned tasks and transferring completed tasks to the next layer for further processing.

This clear specialization ensures performance, reliability and scalability of the Internet.

Layer	Function	Example
Application (7)	Services that are used with end user applications.	HTTP, FTP, DNS, SMTP
Presentation (6)	Formats the data so that it can be viewed by the user. Encryption and decryption.	JPG, GIF, SSL, TLS
Session (5)	Establishes/ends connections between two hosts exchanging data.	NetBios, PPTP
Transport (4)	Responsible for the transport protocols and error handling.	TCP, UDP
Network (3)	Reads the IP address from the incoming data packet.	Routers, Layer 3 Switches
Data Link (2)	Reads the MAC address from the MAC address	Swtiches, Ethernet, Wi-Fi
Physical (1)	Send the data on the physical wire.	Hubs, NICS, Cables

Source: Cloud Scanner

The Internet is a multi-layered global distributed network of computers that we use every day for many things without ever questioning its existence. Though only 20 years old, the Internet powers an immense amount of trades between an ever-growing number of consumers, companies and nations, accounting for roughly $28 trillion in 2016.

Long before Amazon was a thing, in 1972, students from Stanford and MIT conducted the first ever online transaction using ARPANET. The first good ever sold on the Internet was marijuana.

Many projects followed as commercial and academic attempts to create electronic cash making commerce native on the Internet. All incommensurably failed from the late 1980s to the early 2000s, including B-money, Digicash, Hashcash, and BitGold.

Technology, regulation and centralisation prevented mainstream digital currencies from ever taking off.

The Missing 'Monetary Layer' of the Internet

Regardless, for users to directly trade with geographically-distinct neighbours on the Internet, one essential component has been absent: a monetary layer to store, exchange and measure value natively on the web without being required to use legacy financial institutions.

Over two decades, failed attempts at creating digital money paved the way to a reckoning and the silent launch of an open-source software project on a cypherpunk mailing list, back in 2008. Satoshi Nakamoto was the unknown pseudonym who posted about the Bitcoin project with a link to its white paper explaining how it works.

It was initially understood as yet another doomed attempt to construct a digital currency by the disillusioned cypherpunk community. Without anyone's permission, Bitcoin slowly emerged and diligently grew to be adopted by a small group of computer researchers, cryptographers and engineers curious to decipher the technology.

Bitcoin P2P e-cash paper

Satoshi Nakamoto satoshi at vistomail.com
Fri Oct 31 14:10:00 EDT 2008

- Previous message: Fw: SHA-3 lounge
- **Messages sorted by:** [date] [thread] [subject] [author]

```
I've been working on a new electronic cash system that's fully
peer-to-peer, with no trusted third party.

The paper is available at:
http://www.bitcoin.org/bitcoin.pdf

The main properties:
 Double-spending is prevented with a peer-to-peer network.
 No mint or other trusted parties.
 Participants can be anonymous.
 New coins are made from Hashcash style proof-of-work.
 The proof-of-work for new coin generation also powers the
    network to prevent double-spending.

Bitcoin: A Peer-to-Peer Electronic Cash System
```

Source: Bitcoin P2P E-Cash Paper Mailing List

Fast forward 10 years, Bitcoin proved to be resilient to attacks, bugs and serious technical or political crises. There are hundreds of developers actively working on this project worth billions of dollars of market capitalization.

Bitcoin's latest running software (0.17.1 released in December 2018) has created and maintained the world's first form of digital scarcity. Without ever breaking the integrity of its underlying ledger, it does not rely on trusted third parties to verify everything is running well.

Everyone and anyone can take the role of verification. This had never been achieved in the past. Bitcoin solved a multi-decades long problem in computer science called the Byzantine Generals' Problem.

BTC/LN as Public Network Protocols

Bitcoin is growing into the Internet's native monetary layer. Functioning as a suite of public network protocols, BTC/LN, Bitcoin has undeniably scarce units of value. It is a network of storable, movable and quantifiable value.

As a self-contained economic system on the Internet, Bitcoin is powered by energy and protected by a global network of computing power that voluntarily regulates the integrity of Bitcoin's ledger and its digitally-scarce monetary units. That self-organized configuration is unbreakable and decentralized like the internet itself.

Bitcoin and its Lightning Network (BTC/LN) are joining the ranks of other open network protocols akin to TCP/IP. Bitcoin (BTC) has movable units of scarce value that can flow within its network, similar to the Internet Protocol (IP).

The Lightning Network (LN) acts as a second layer built on top of BTC, which permits nearly instant, friction-free, and anonymous exchange of smaller units of BTC, similar to the Transfer Communication Protocol (TCP).

BTC/LN is the suite of protocols responsible for the rise of a native monetary layer of the Internet, adding a division to the OSI model's current stack. Bitcoin represents the world's first bytes of data with an intrinsic financial value priced by the physical world, in the form of energy and perceived market value.

Software now has a built-in price tag. Code is valuable without any specific application because of its remarkable scarcity. Scarcity isn't a concept that is limited by physical boundaries anymore. Scarcity can provably be digital. It now exists in the most intangible form–bytes–digital binary digits.

A Silent Monetary Evolution

Bitcoin is agnostic of any traditional institutions such as governments, central banks or for-profit corporations. Internet users can simply acquire, trade and use bitcoins as they see fit. No single entity controls its protocol. It is governed by open-source software, which is voluntarily run by tens of thousands of independent computers.

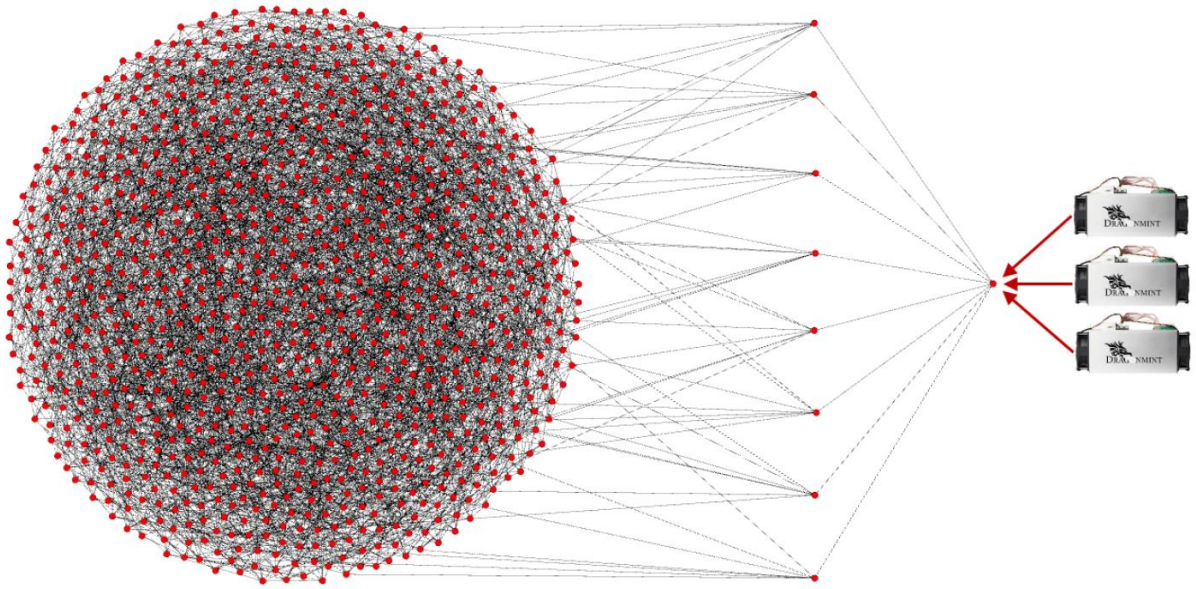
Computers in the network play two roles around Bitcoin's ledger, called the Timechain, by either writing or reading transactions. Bitcoin's Timechain is a chain of blocks, which transcribes a suite of bundled transactions that are recorded by one set of computers: miners.

Often coined 'the blockchain', which is for other cryptocurrencies trying to mimic Bitcoin, the Timechain is more accurate to describe Bitcoin's ledger as it ties to the original semantic used by Bitcoin's creator, Satoshi Nakomoto.

A Free Market of Rational Volunteers

Miners are powerful computers with specialized hardware dedicated towards writing transactions to Bitcoin's ledger. In a collective computational contest, vast amounts of energy are expensed by miners to brute-force random alphanumeric strings in an effort to guess a random code. It's akin to a digital lottery.

Bitcoin miners' contributions to the network are measured as hash rate, which is a function of computational power.



Source: *Bitcoin Miners Beware: Invalid Blocks Need Not Apply*

Once that random code, called a 'nonce' is found by a computer in the network, it proves that the miner has completed enough work in the form of energy and time expended. This is commonly referred to as Proof of Work, which allows all computers in the Bitcoin network to verify that the system stays fair and honest.

The lucky computer, or mining pool as they often combine computing power for efficiency, can then gather a batch of unconfirmed transactions from a queue called the 'mempool' and bundle them into a block to permanently write that block of transactions into Bitcoin's ledger.

To be granted permission to write on Bitcoin's ledger, there is no shortcut such as political influence, hierarchy or seniority. Each participant adding information to Bitcoin's ledger needs to earn it through proven work that they must show to the network using the random nonce.

In return for their service to the network, miners receive a 'block reward' with new bitcoins, including transaction fees that users previously paid to have their transactions recorded. This is the only way for new bitcoins to be created. It must be earned via provable energy expenditure.

Since 2018, Bitcoin has shifted the world into an era of exahash computing. If one were to gather the 500 top supercomputers, altogether they would only represent 1.6% of Bitcoin's hashrate. It is dwarfing the world's computing horsepower by multiple orders of magnitude, creating a robust computational defense mechanism, preventing malicious actors from controlling the network and double spending bitcoins using the majority of the hashrate (often called a 51% attack).

A Self-Managed Computing Organism

Bitcoin's ledger is secured and managed by cryptography. On average, a new block of transactions is added every 10 minutes, no matter what. Each time, this creates new bitcoins on the network, in the form of a block subsidy for the lucky miners.

The block subsidy used to be 50 bitcoins, which got cut in half in 2012, in 2016, and soon will be cut in half again in 2020, bringing the next block subsidy down to 6.25 bitcoins. This process is called halving.

Halving events happen every 210,000 blocks that are added to Bitcoin's ledger. It is the only rule that controls the issuance of new bitcoins. It will continue roughly every 4 years until all 21 million bitcoins are mined, which should happen approximately in the year 2140.

The creation rate of new bitcoins slows down over time, until it ultimately turns to zero. No new bitcoins will be created after that moment. As new adoption increases demand, bitcoins' price goes up too. Opportunistically, new computers are attracted to the Bitcoin network to mine blocks of transactions and receive the valuable block reward.

As more computers join the network and produce larger collective hashrate, Bitcoin is automatically adjusting the difficulty of the mining lottery. Roughly every 2 weeks, or 2,016 blocks, mining either becomes harder or easier based on how much hashrate there is.

It is the most reliable way to have new blocks mined roughly every 10 minutes, which keeps new bitcoins' issuance highly stable and predictable, regardless of the network's collective hash rate.

Towards Universal Financial Integrity

Since its first block mined on January 3rd, 2009 by Satoshi Nakamoto, Bitcoin has been up 99.98% of the time, and has never validated a malicious or wrong transaction, which is unprecedented for financial institutions.

This is only possible because verifying Bitcoin transactions is very accessible. While writing new transactions on the ledger is extremely costly, reading them to verify the integrity of the ledger is easy and accessible to all.

Full-validating nodes can be operated on computers less powerful than what anyone has at home or at work, making it trivial and affordable to verify the history of the Bitcoin transactions. Anybody can run them. This makes Bitcoin an impenetrable fortress of security as everyone can check every single transaction that ever happened in Bitcoin. It's an openly auditable ledger.

Miners and full-node operators voluntarily run a version of the Bitcoin software that is compatible with the majority of the network. This maintains a general consensus on the shared rules of the network such as the block size, which dictates how many transactions can be included in a block by miners.

Large miners are incentivized to grow the size of blocks to include more transactions, gaining additional fees and making it more costly for newcomers and small participants. Full node operators choose voluntarily to run a version of the software to keep block size small to make verification accessible to everyone.

Miners have to be compatible with full-nodes to have the mined blocks be verified and approved. If Bitcoin's block size grows, more powerful computers are required to run full-nodes with extra memory and bandwidth, which will centralize verification, adding a level of trust in the system, especially around miners.

Bitcoin's current block size is 1MB, and has been challenged many times in the past. The most serious attack was in 2017 under the form of a fork, called Bitcoin Cash (BCH), which copied Bitcoin's software and transaction history, and adjusted the code to raise the block size to 4MB.

Deviations such a Bitcoin Cash are the unavoidable by-product of the open-source nature of Bitcoin, which lets anyone create forked projects of Bitcoin's Timechain, though the market continues to value these forked tokens at a substantially discounted value.

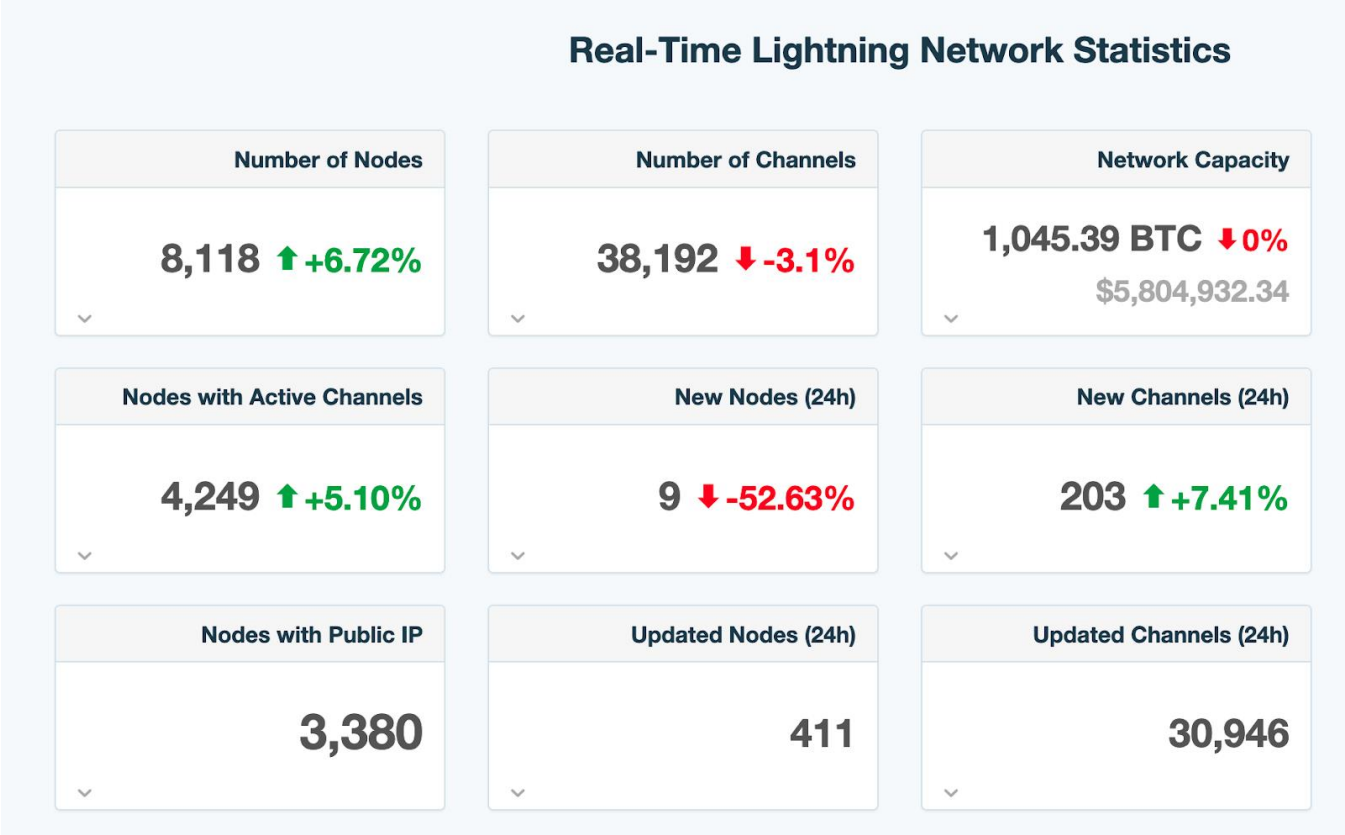
The Internet-Native Monetary System

Bitcoin (BTC) has recently seen the deployment of Lightning Network (LN), which is a layer built on top of Bitcoin to enable fast, cheap and anonymous payments. BTC is the base layer, or Layer 1. LN is the second layer, also referred to as L2. BTC and LN interoperate in a cryptographically secure manner.

LN is a network of nodes for routing payments that lets people send sats (subunits of bitcoins) where 1 BTC = 100,000,000 sats. It is much cheaper to use LN for smaller amounts instead of using BTC's on-chain network because transactions aren't replicated by a global system of miners and nodes to be preserved for eternity in the Timechain.

On the Lightning Network, transactions occur directly between peers, and only occasionally settle on-chain if needed as an arbitration system.

Under beta release, the Lightning Network was deployed in 2018 and has since seen a massive growth in its utilization with over 8,000 public nodes connected to the network, around 40,000 channels connecting them and more than $5 million of liquidity. One day, as LN matures, it may very well power the world's commerce, exchanging trillions of dollars of value in today's terms.



Source: 1ML

Intrinsic BTC/LN properties let people store, exchange, and measure value on the Internet. These three functions are the primary use cases for standard money we use today for our everyday lives. It just exists natively on the Internet, available to anyone with a connection.

Bitcoin and Lightning Network are two public protocols that are undeniably morphing into native Internet money, but it is still incredibly early.

Infrastructure is in its infancy, following a steady increase in global adoption with now a few millions of people using Bitcoin. Many improvements on both the base and second layer are made around privacy, security, and performance.

Beyond Bitcoin and Lightning Network

As the Internet liberated free information between global peers, Bitcoin is liberating capital exchange, creating open, fair, and social markets in which anyone can participate.

New companies exclusively built on Bitcoin's base layer and/or Lightning Network are making it safer and easier for sovereign people to opt-out of the legacy banking system.

As trust-minimized agents, companies building the "Layer 3" of Bitcoin and Lightning Network are pushing for reasonable adoption with ethical principles and a core focus on security, usability and sovereignty.

Whether working on non-custodial private key management, LN channel capacity distribution, protocol implementations, or peer-to-peer BTC exchanges, L3 companies make the capital flow from the legacy banking system into Bitcoin possible.

L3 companies are creating massive economic upside potential for this new Internet monetary layer and will be building a Bitcoin-based economic system in the next 20-30 years without a doubt.

As always, major thanks to a few Bitcoiners who helped out with reviews, edits and suggestions. @mrcoolbp @zanepocock @theonevortex @alan_btc @Joss_do_it_BTC @anbuteau @allenshashaty

---

Tweetstorm: Adoption by number of users

By Nic Carter

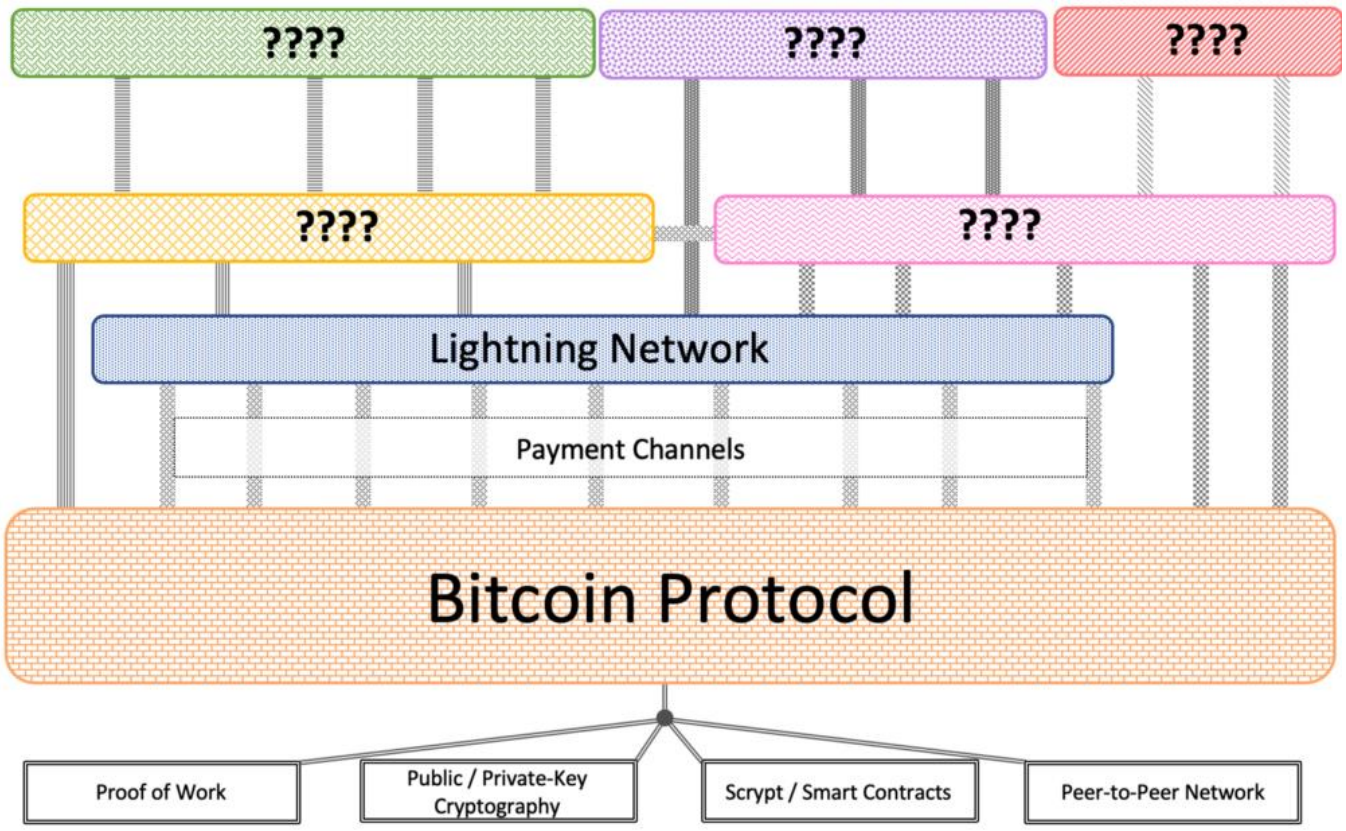
Posted April 24, 2019

[Link to tweetstorm]

Lightning is Only the Beginning: The Emerging Bitcoin Stack

By Spencer Bogart

Posted April 25, 2019

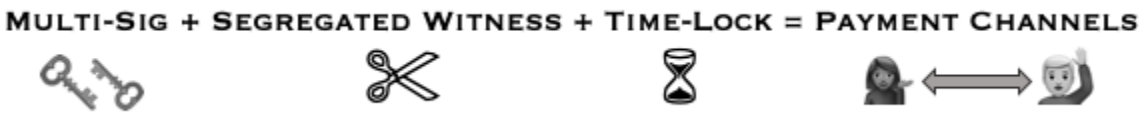


For the past year or two, Bitcoin's lightning network has been one of the most closely watched developments in the crypto industry and while I'm very excited about the new possibilities enabled by the Lightning Network, I can't help but ask: What about the other layers?!

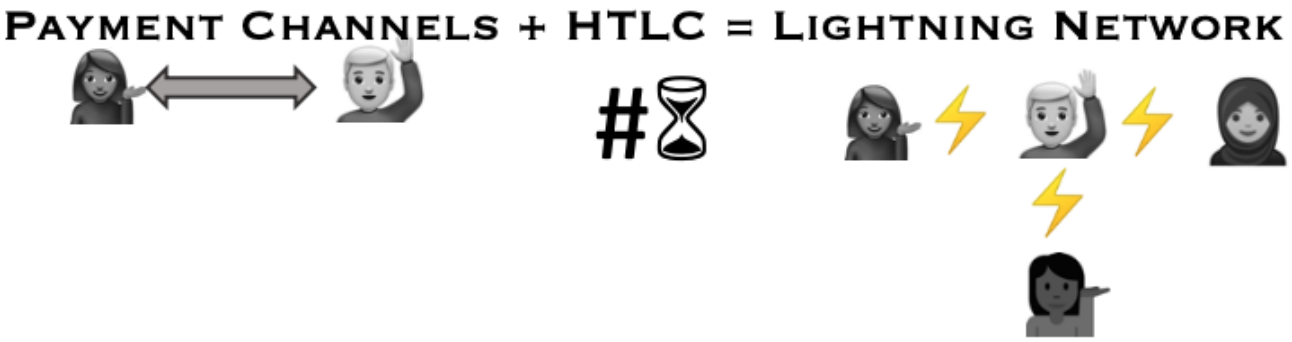
After all, the Lightning network is just one layer in the emerging Bitcoin stack. These various layers, or protocols, will likely all serve different functions but with one underlying commonality: they all exist to make Bitcoin even more useful than it already is.

The Bitcoin stack is a set of building blocks that can be assembled in unique ways to deliver novel and compelling functionality.

For example, payment channels leverage the Bitcoin network and multi-sig transactions as building blocks to enable people to quickly, cheaply, and reliably transact Bitcoin directly between one another without incurring the costs of on-chain transaction fees and delays from block times.



Building up the stack, the lightning network made payment channels even more useful by enabling multi-hop payments on a network that connects otherwise disparate payment channels. So, instead of opening a separate channel with every transaction counterparty, you can open a single payment channel and leverage the lightning network to transact with others.



However, if Bitcoin becomes the multi-trillion-dollar asset that we think it will become, Lightning is only the beginning. As the number of building blocks grows, the number of unique combinations from that suite of building blocks grows exponentially and the probability of useful combinations of those building blocks increases significantly.

After all, Bitcoin is programmable money—and while it remains to be seen * *what exactly** people will create up the stack, I have no doubt that human ingenuity coupled with an open permissionless network of programmable money will create incredible functionality that delivers compelling utility to holders and users.

Some of this functionality will be enabled by decentralized networks and protocols like Lightning, others will be enabled by centralized companies built atop these protocols and others will reside somewhere on the spectrum between the two (e.g. federated models like Blockstream's Liquid or Rootstock's RSK network).

Regardless, to think that lightning will be the only layer, and that fast & cheap transactions is all we'll be able to do with programmable money is like thinking that the internet will only be used for sending messages faster—that email is the only use case and the internet is really just a replacement for the post office or the fax machine.

To be fair though, when you're in the dial-up era—which is probably where Bitcoin is today—it's tough to anticipate Spotify, Facebook and Twitter.

And while it's tough to anticipate exactly what people will create, it seems reasonable that up the stack there could be protocols that do things like enhance privacy, offer more expressive functionality, or facilitate the lending/borrowing of Bitcoin—among many other potential purposes.

Ultimately, lightning is an important building block in the emerging Bitcoin stack—but it's only the beginning. As we see momentum coalescing around the Bitcoin protocol, we're entering a unique period in Bitcoin's history with compelling opportunities to deploy capital with teams that are building on Bitcoin.

Along these lines, we're sponsoring and hosting the Lightning Developers meetup group in San Francisco. Please sign up here if interested in attending future events: https://www.meetup.com/Lightning-Developers/events/260891282/ . You can also sign-up for our monthly newsletter at the bottom of the page here: https://blockchain.capital/

Disclosure: I own Bitcoin personally and have exposure via Blockchain Capital's venture funds.

Note: Special thanks to Derek Hsue for feedback and help thinking through the Bitcoin stack.

Bitcoin is a Demographic Mega-Trend: Data Analysis

By Spencer Bogart

Posted April 30, 2019

What follows is data and analysis from a survey of American adults regarding general sentiment toward Bitcoin—the survey was conducted by Harris Poll, on behalf of Blockchain Capital, from April 23–25, 2019 and consisted of a representative sample of 2052 American adults. The survey was an augmented version of one we ran in October 2017 (we added a few questions).

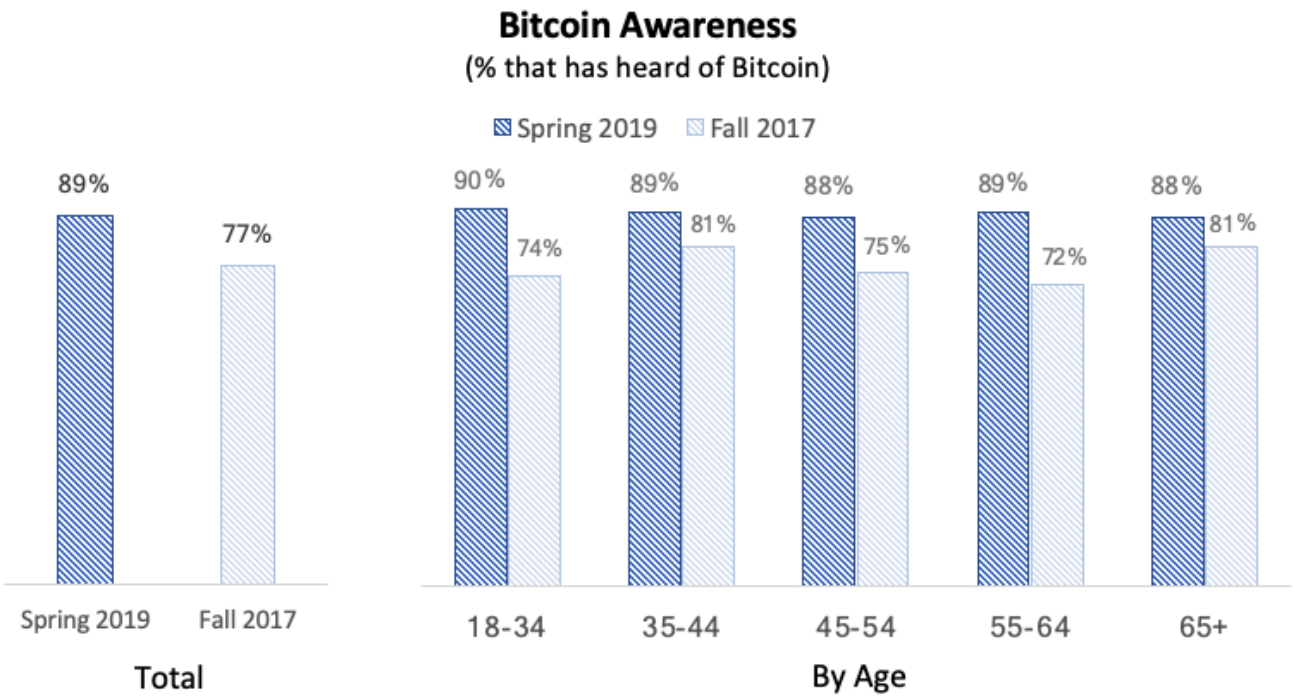
For context and because it's material in considering the results, **the survey in October 2017 was conducted in a bull market**—Bitcoin was up over 800% YoY—whereas **the most recent survey, in April 2019, was conducted in a bear market**—price was down roughly 75% from all-time highs.

We suspect that the difference in market environment between the two surveys would have a negative impact on Bitcoin sentiment in the most recent survey. **Despite the bear market, the data shows that Bitcoin awareness, familiarity, perception, conviction, propensity to purchase and ownership all increased/improved significantly**—dramatically in many cases.

The results highlight that Bitcoin is a demographic mega-trend led by younger age groups. The only area where older demographics matched younger demographics was awareness: Regardless of age, the vast majority of the American population has heard of Bitcoin.

Awareness

The percentage of people that have heard of Bitcoin rose from 77% in October 2017 to 89% in April 2019.

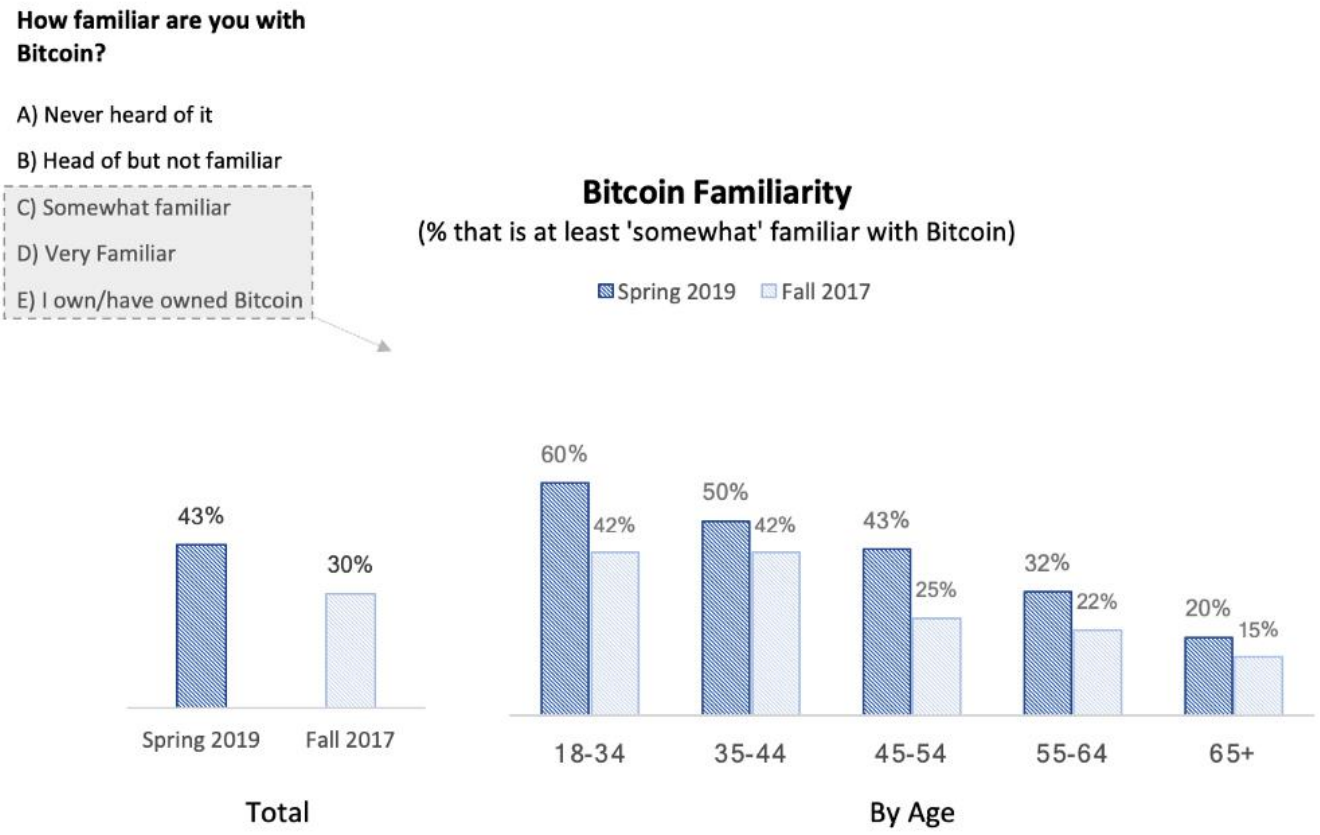


Awareness of Bitcoin is strong across all age groups—those aged 18–34 have the highest rates of awareness at 90% and those aged 65+ have the lowest at 88%.

Overall, **the percentage of people that have not heard of Bitcoin fell by more than half**—from 23% in October 2017 to 11% in April 2019.

Familiarity

The percentage of people that are 'at least somewhat familiar' with Bitcoin rose by nearly half—from 30% in October 2017 to 43% in April 2019.

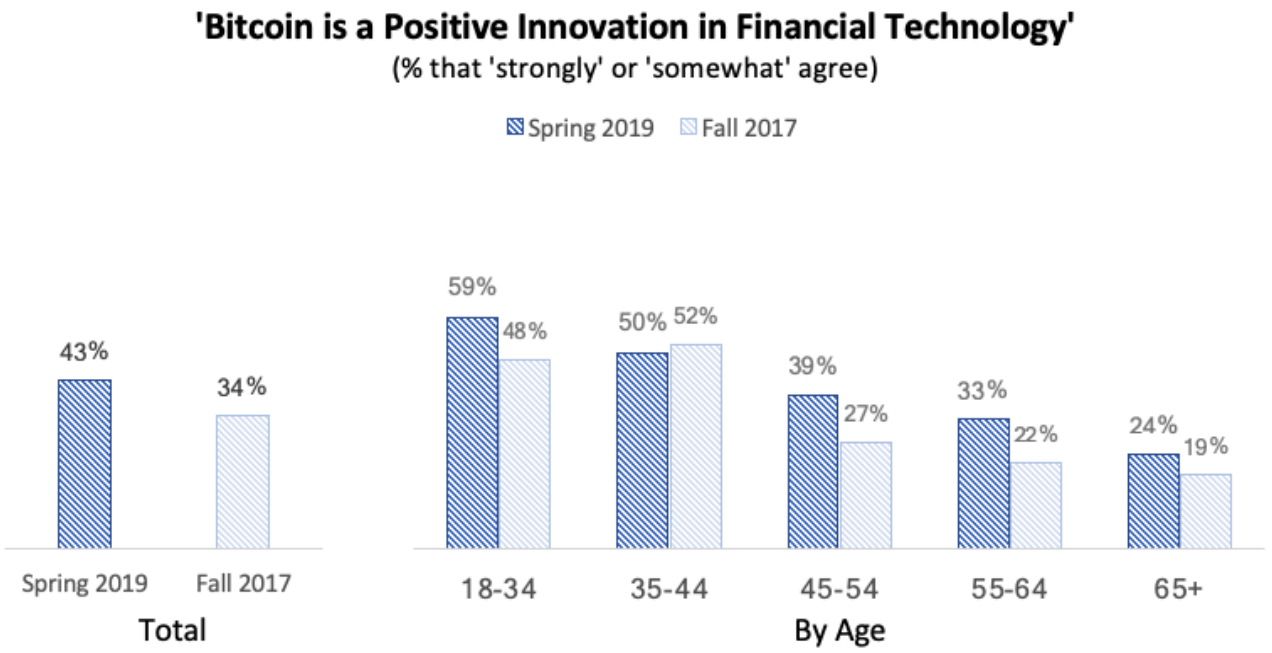


Among those aged 18-34, a full 60% described themselves as at least 'somewhat familiar' with Bitcoin—up from 42% in April 2019. Relative to older segments of the population, those aged 18–34 are 3x as likely to be at least 'somewhat familiar' with Bitcoin as those aged 65 and over.

The natural follow-on question is how perception is affected by rising awareness—as people become more familiar with Bitcoin do they think of it more positively or negatively?

Perception

The percentage of people whom 'strongly' or 'somewhat' agrees that ' **Bitcoin is a positive innovation in financial technology**' rose 9 percentage points—from 34% in October 2017 to 43% in April 2019.

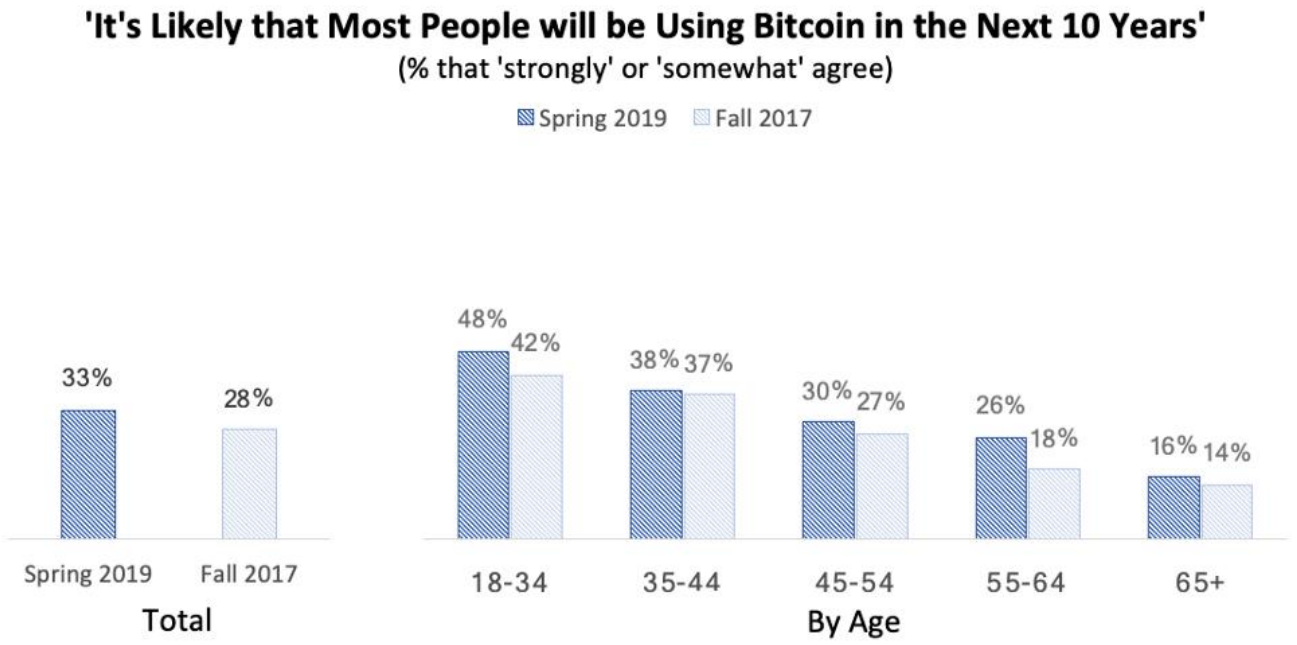


Younger demographics were most inclined to have a positive view of Bitcoin: **59% of those aged 18–34 'strongly' or 'somewhat' agree that ' Bitcoin is a positive innovation in financial technology**—up 11 percentage points from October 2017.

But even if an increasing percentage of the population has a positive perception of Bitcoin, does that translate to increased conviction in future adoption?

Conviction

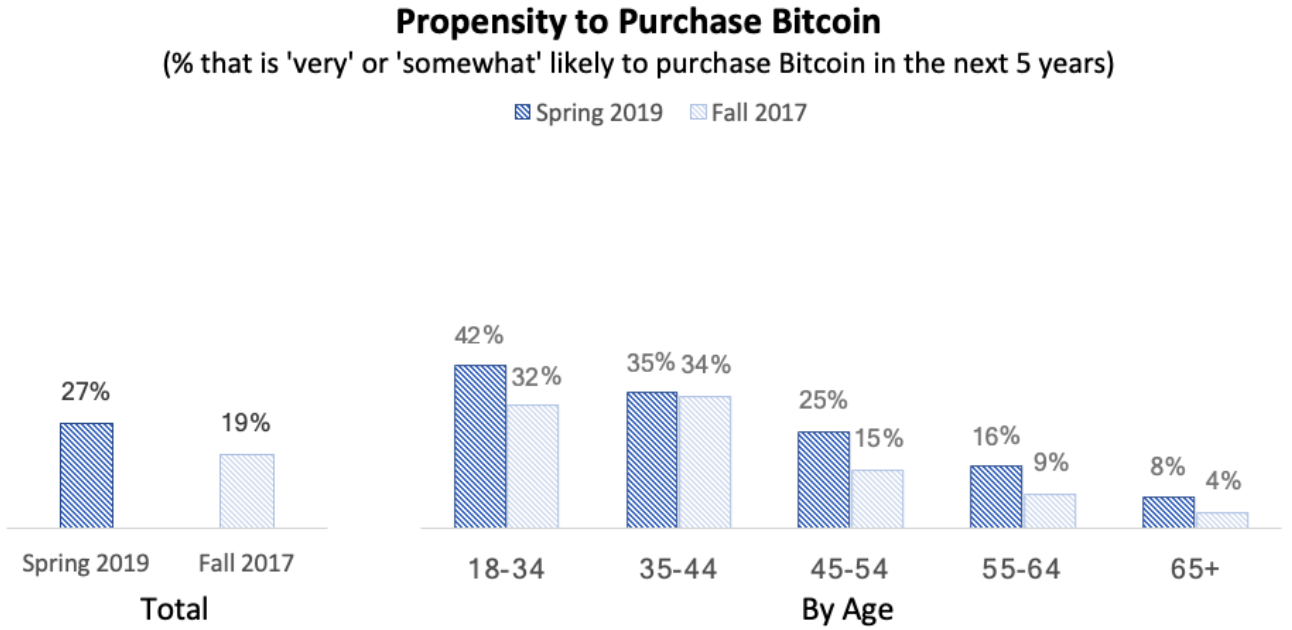
The percentage of people that 'strongly' or 'somewhat' agrees that ' **most people will be using Bitcoin in the next 10 years**' rose 5 percentage points—from 28% in October 2017 to 33% in April 2019.



Younger demographics have the most conviction in adoption over the next 10 years: **Nearly half (48%) of those aged 18–34 'strongly' or 'somewhat' agree that 'it's likely most people will be using Bitcoin in the next 10 years'**—up 6 percentage points from October 2017.

Propensity to Purchase

Despite the bear market, **the percentage of people that indicated they are 'very' or 'somewhat' likely to buy Bitcoin in the next 5 years rose by nearly half**—from 19% in October 2017 to 27% in April 2019.

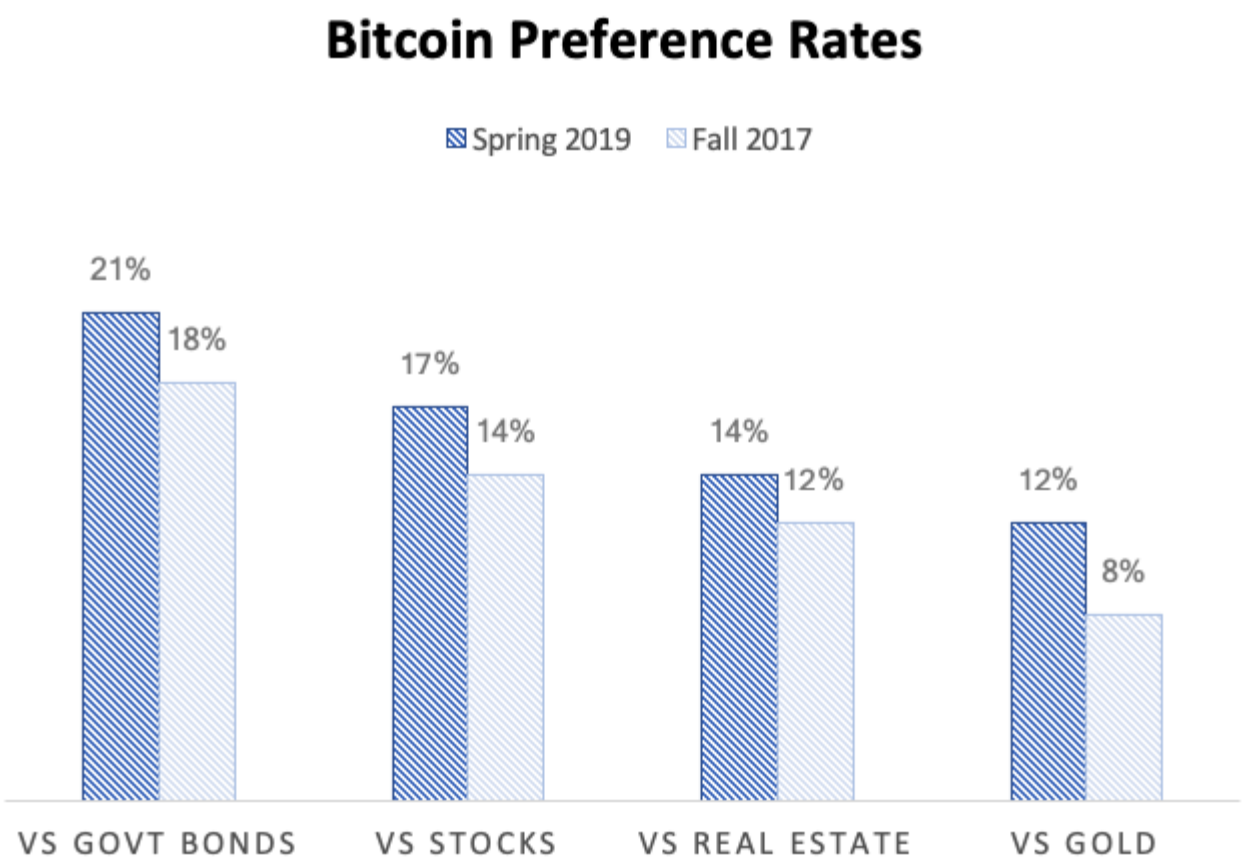


Younger demographics appear most inclined to purchase Bitcoin: 42% of those aged 18–34 said they are 'very' or 'somewhat' likely to purchase Bitcoin in the next 5 years—up 10 percentage points from 32% in October 2017.

It's also helpful to consider how people think about Bitcoin relative to other investable assets.

When asked which they'd prefer to own $1k of:

- **21%** of people said they would **prefer Bitcoin to government bonds**—up from 18% in October 2017
- **17%** of people said they would **prefer Bitcoin to stocks**—up from 14% in October 2017
- **14%** of people said they would **prefer Bitcoin to real estate**—up from 12% in October 2017
- **12%**of people said they would **prefer Bitcoin to gold**—up from 8% in October 2017



Focusing on those aged 18–34, when asked which they'd prefer to own $1,000 of:

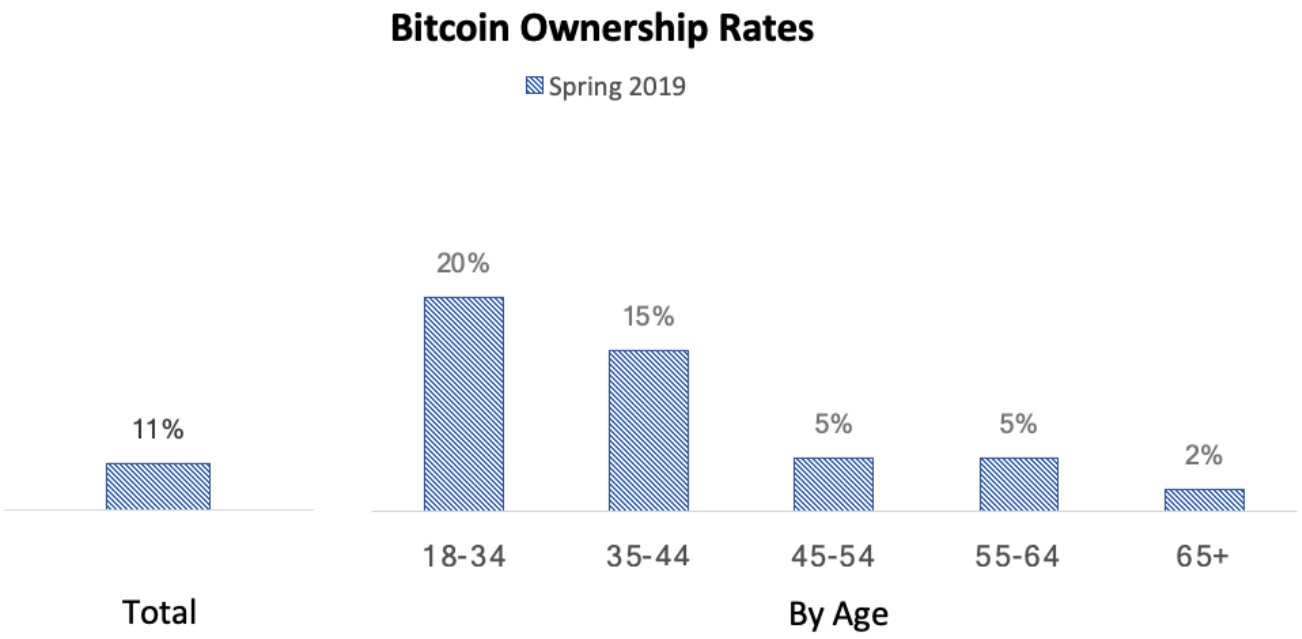
- **30%** said they would prefer Bitcoin to government bonds—flat from October 2017
- **27%** said they would prefer Bitcoin to stocks—flat from October 2017
- **24%**said they would prefer Bitcoin to real estate—up from 22% in October 2017
- **22%** said they would prefer Bitcoin to gold—up from 19% in October 2017

Said differently, among those aged 18–34: Nearly 1 in 3 prefers Bitcoin to government bonds, more than 1 in 4 prefers Bitcoin to stocks, nearly 1 in 4 prefers Bitcoin to real estate and more than 1 in 5 prefers Bitcoin to gold.

The biggest increase in preference rate for Bitcoin was relative to gold—perhaps the byproduct of Bitcoin's growing acceptance as 'digital gold'.

Ownership

In total, 11% of the population owns Bitcoin—including 20% of those aged 18–34 and 15% of those aged 35–44.



To help put the millennial proclivity to Bitcoin in perspective: Only 37% of people under 35 are invested in the stock market (source)—so the data point that 20% of those in the same group own Bitcoin is particularly surprising.

Ultimately, Bitcoin is a demographic mega-trend: Younger demographics are leading in terms of Bitcoin awareness, familiarity, perception, conviction, propensity to purchase, and ownership rates.

Blockchain Capital, founded in 2013, is one of the oldest and most active venture investors in the blockchain industry and has financed 75+ companies and projects since its inception. Our mission is to help entrepreneurs build world-class companies and projects based on blockchain technology. We invest in both equity and tokens and are a multi-stage investor. Blockchain Capital also pioneered the world's first ever tokenized investment fund and the blockchain industry's very first security token, the BCAP, in April of 2017.

Sign-up for our monthly newsletter at the bottom of this site: http://www.blockchaincapital.com/

Thanks to Derek Hsue.

Disclaimer:

THANK YOU, CREATORS.

WORDS

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

This Journal does not contain reference to any of the investment products or services currently offered by members of the any specific business, that means any business I am associated with. Bitcoin, shitcoins, and related technologies can be volatile, Don't fuck around with this stuff because you might get burned.

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

This Blog Post fairly represents the opinions and sentiments of its author at the date of publishing but it should be noted that such opinions and sentiments may be revised from time to time, for example in light of experience and further developments, and the blog post may not necessarily be updated to reflect the same.

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

DYOR | BTFD | HOLD