WORDS

March 2019

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

Contents

Goals and Scope

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

History

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

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

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

Support WORDS

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

Spread the word

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

Follow us on social media

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

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

Subscribe to our newsletter

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

Our pledge

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

Bitcoin Timestamp Security

Jameson Lopp

Posted March 3, 2019

Bitcoin is often referred to as a secure timestamping service. We never had a global record of truth with trustworthy timestamps, so how did this come about? It's generally due to Proof of Work being combined to a few simple rules by which miners must abide. The primary functions of miners are to:

- Take unordered unconfirmed transactions and put them in a specific order
- Bundle up the transactions into a valid container (block)
- Timestamp the block within an acceptable range of time
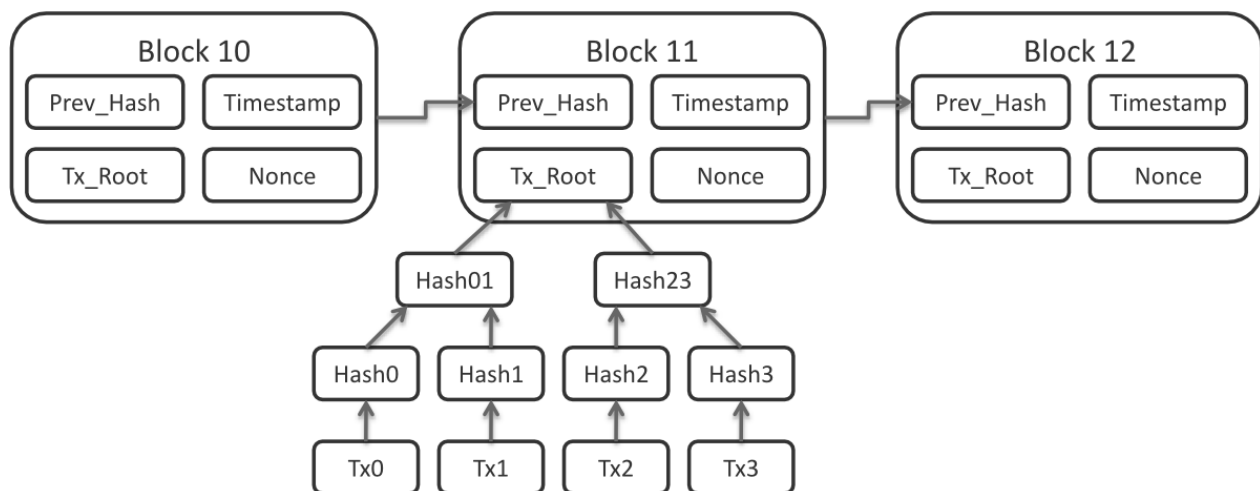
This final attribute is what enables Bitcoin to have a controlled release of the supply of bitcoins. Otherwise Bitcoin would suffer from rapid inflation whenever the hashrate increased. But it turns out that this attribute assigns quite a bit of utility to the Bitcoin protocol and also makes it possible for folks to use Bitcoin as a data anchor for other services. Because we have reasonably strong assurances that timestamps fall within a given range and we have mathematical assurance of the amount of energy required to rewrite the blockchain history, Bitcoin provides a sound anchor for timestamping of data. But how reliable is it?

Bitcoin's Timestamp Flexibility

In order for the time field of a block header to be considered valid by nodes it must meet two criteria:

1. Be less than 2 hours in the future from your computer's current time

2. Be <u>greater than the median timestamp</u> of the <u>past 11 blocks</u>

The first rule makes sense—we obviously don't want anyone claiming to be from the future and it's very easy for nodes to reject such claims because we're all in general agreement about what time it currently is. There are a variety of ways that one can check the current time, though a very popular means of computers syncing their clocks is via the <u>Network Time Protocol</u>.

However, ensuring that the time isn't too far *before* a sensible point is harder. This is because we can't assume that a node is validating the block anywhere near the time it is initially created. Nodes need to be able to leave and rejoin the network for any reason or no reason. A node that was too far behind the tip of the chain would start rejecting historical blocks if they had to be created within a few hours of the current time.

"Nodes can leave and rejoin the network at will, accepting the proof-of-work chain as proof of what happened while they were gone."—Satoshi Nakamoto, Bitcoin Whitepaper

Perhaps counterintuitively, there is no rule requiring that a block's timestamp has to be *after* the timestamp of the previous block. If you think about it, such a rule could cause problems—if a miner created a block with a timestamp nearly 2 hours in the future, the next block would also have to be far in the future—it would be harder for other miners to self-correct the median time of the past 11 blocks.

Also, recall that while blocks are expected to be produced about every 10 minutes, there is no real guarantee. Blocks could range from anywhere from several milliseconds to several hours apart. While the expected median time of the past 11 blocks should be 1 hour ago, it could be far more or far less.

Source:
https://en.bitcoin.it/wiki/Confirmation

Pushing the Window

If you think about how an adversary might try to expand the acceptable timestamp window, it's pretty clear that no adversary will be able to push the timestamps to be more than 2 hours in the future, no matter how much hashpower they have. However, an attacker with sufficient hashpower
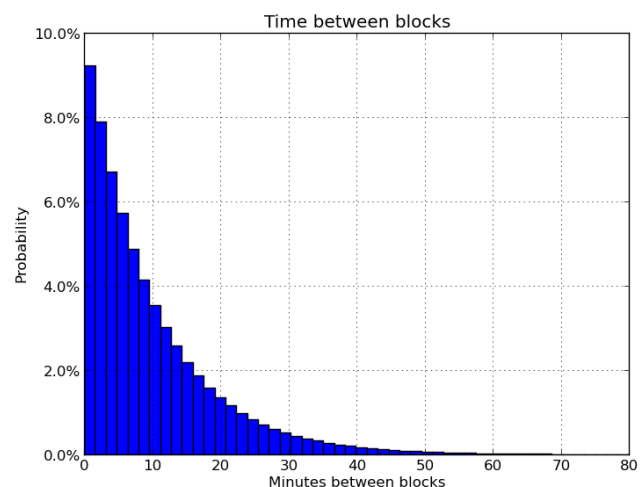
could put some drag on the progression of "bitcoin time" by only minting blocks with timestamps that are barely valid—that are just one second after the median time of the past 11 blocks.

Are there incentives to do this? In the extreme case a "time warp attack" offers short term financial incentives that we'll discuss later. It's less clear what incentives may exist for only dragging the timestamps by a few hours here and there. Though considering that other protocols can be built on top of Bitcoin (such as Lightning Network) and can involve time locks, there could be other protocols in the future that can be gamed by slowing the progression of timestamps on the blockchain.

Hashpower Time Dragging

Since the earliest valid block time is based upon the median time of the past 11 blocks, an adversarial miner needs to generate a lot of blocks in order to induce any noticeable drag on the MTP.

Let's assume a situation where all miners are roughly in sync via NTP but there is one adversarial miner who is trying to drag the median time of the past 11 blocks as much as possible.

One point is quite clear: it was a smart decision by Satoshi to use the median timestamp of the past 11 blocks rather than the average, as average would be more manipulable. Another way to think of "median time past" is that it basically means the timestamp of the 6th most recent block if all of the timestamps are in order. If they aren't, the algorithm just re-orders them. As such, *if you want to have a non-negligible effect on this value* you need to have solved 6 of the past 11 blocks. In order to sustain such an attack you'd need 55% hashpower, at which point one of the main assumptions of Bitcoin's thermodynamic security breaks down. But a miner with less hashpower *could* still achieve this on occasion if they have a streak of luck.

How hard is it to find 6 out of 11 blocks? Well, the chance that a given miner will solve the next block is basically the same as their percentage of the total network hashrate. Thus, if you only have 1% of the hashrate (which is still quite a lot) then your chance of minting 6 out of any 11 contiguous blocks = $(0.01^6 0.99^5)(11!/(5!6!))$ = *about one in 2 billion. If you maintained 1% of the hashrate then the expected number of blocks that would need to occur before you found 6 out of 11 would be over 43,000 years.*

A more generalized formula for the expected wait time to pull off a successful time drag attack would be:

$(1 / (462 * (\%\ hashrate^6 * (1- \%\ hashrate)^5))) / 144$ blocks/day = # days
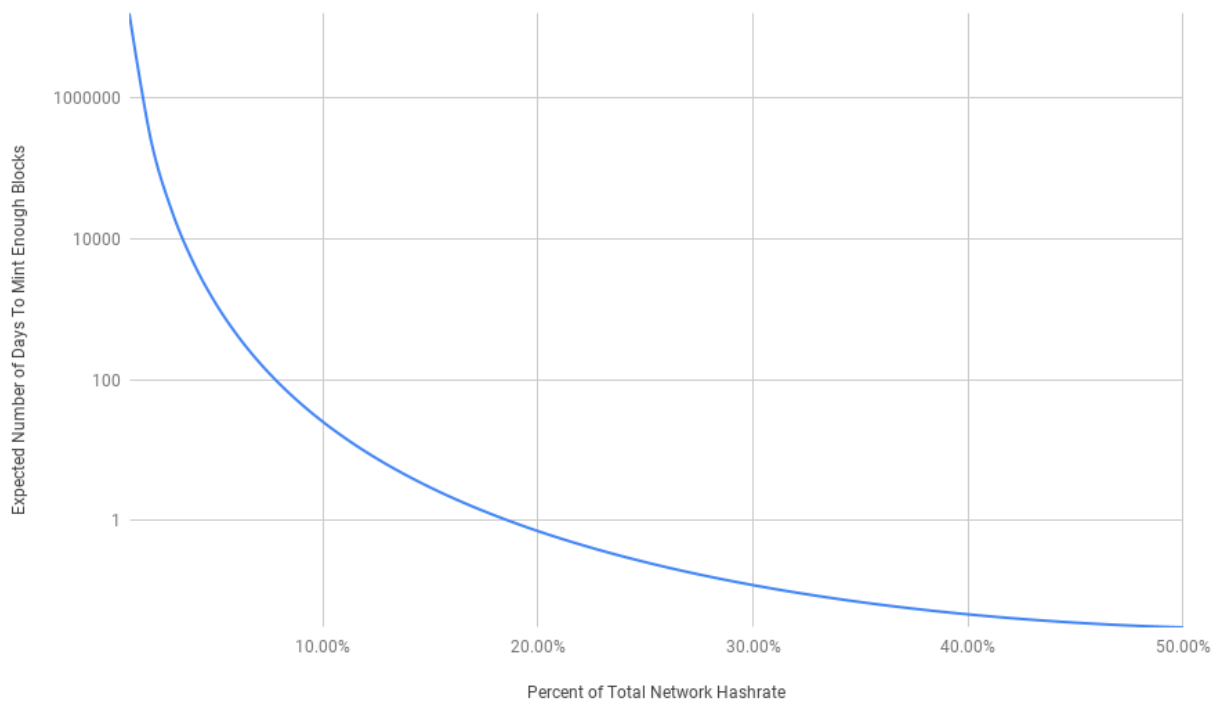
As we can see, for attackers to conduct such an attack on any meaningful timescale then they'd need a decent size mining pool with at least 10% of the total network hashrate.

Maximum Drag

However, in order to induce the **maximum** drag on the MTP a miner would want to solve 6 blocks in a row. If their 6 of the past 11 blocks are not all in order, then time gaps created by other miners would force the adversarial miner to set the timestamps of their blocks more than one second after each other because the MTP for each block would jump forward significantly as honest miners place more accurate timestamps on their blocks.

How hard is it to solve 6 blocks in a row? If we once again assume a miner with 1% of the network hashrate then the chance of minting any given streak of 6 blocks in a row is 0.01^6 = roughly one in a trillion. If you maintained 1% of the hashrate then the expected number of blocks that would need to occur before you found 6 in a row would be nearly 2 million years.

A more generalized version of the expected time to successful time drag attack formula would be:

(1 / % hashrate^6) / 144 blocks/day = # days

This attack is even more difficult to pull off, requiring more like 20% or 30% of the network hashrate to occur in a reasonable timeframe. As you may imagine, this happens quite rarely and when it does, people notice. The last times it happened were in July 2014 by GHash, which had over 40% of the hashpower for a while and even touched 51% for a short time. It also happened 9 months earlier when BTC Guild had nearly half of the hashpower. If you have 50% of the hashpower then your chance of minting 6 blocks in a row is 0.5^6 = one in 64. If you maintained 50% of the hashrate then you could expect to find 6 blocks in a row nearly every 12 hours.

It's clear that it's not possible to sustain a drag on Bitcoin's Median Time Past on a long term time scale without majority hashpower, but you could drag it by as much as several hours for a short period (a block or so) with the right combination of luck and patience. If you assume that other miners are fairly accurate with their timestamps, then the median time past should be approximately 1 hour ago, though it could be several hours more due to the variability in blocks being found. If you manage to mint 6 blocks with timestamps of 1 hour ago plus 1 second, 2 seconds, 3 seconds, etc then at the 6th block the MTP would be approximately 2 hours ago. If we assume an extreme condition of 1 hour gaps between blocks, then the MTP would be 6 hours ago.

By allowing a reasonable amount of flexibility with block timestamps and then taking a median time of recent blocks, we end up with an algorithm that is pretty hard to game but is not so brittle as to adversely affect miners who are somewhat out of sync with the real time.

Let's Do the Time Warp Again

What if an attacker did have more than 50% of the network hashpower and they wanted to slow the passage of Bitcoin time? They could do some pretty nasty stuff. Such an adversarial miner could prevent the timestamp from advancing by more than 1 second with each new block. If they did this for a long enough period of time and ended up creating blocks on the difficulty retarget intervals with timestamps that made it look like the previous 2016 blocks took far more than 2 weeks to create, they could game the retargeting logic to decrease the mining difficulty by up to 75% every 2016 blocks. Eventually with the difficulty low enough, they could mint as many blocks as they wanted in a given time period and thus receive more mining reward than expected. An optimized time warp attack could mine all the remaining bitcoin in 18.7 days. We've actually seen similar behavior occur on Bitcoin's testnet3 due to a quirk in the difficulty retargeting and now testnet3 has minted 1,482,878 blocks in 8 years, about 350% of the expected emission.

Time warp attacks are nothing new. Such an attack was first performed against a coin called "Geist Geld" in 2011 and it was discussed as being a "variant of the 51% attack" on BitcoinTalk. Geist Geld was intended to test out the upper limits of block

generation rate via very short block times, as well as the behavior of a cryptocurrency with (almost) stable generation rate and no upper limit or alteration to supply.

Whitecoin appears to have also suffered from a time warp attack that was conducted in 2014.

In 2018 Verge was hit by such an attack. And then 6 weeks later it was hit again!

In general, cryptocurrencies that have a minority of hashpower for a given style of hardware (ASICs or GPUs) are vulnerable to time warp attacks because they are inherently vulnerable to 51% attacks.

Interestingly, while time warping is often referred to as an attack because it results in unintended behavior of the system, some people have shown that it can be exploited for potentially desired uses. In 2015 Vitalik Buterin described a way to speed up blocks via a soft fork and thus increase on-chain capacity. In 2018 Bitcoin developer Mark Friedenbach made a proposal for leveraging this unintended behavior in order to add new functionality to Bitcoin. In his "Forward Blocks" proposal, Mark states that his method enables scaling up on-chain transaction volume to 3584X current levels, changing the proof-of-work algorithm in a backwards compatible way, sharding, a rebateable fee market for consensus fee detection, and smoothing out drops in miner subsidy along with prerequisite protocol pieces for confidential transactions, mimblewimble, unlinkable anonymous spends, and sidechains.

Such proposals are contentious, however, and would likely force anyone building systems reliant upon the timestamps in the Bitcoin block headers to look elsewhere for that data. It would also be fairly easy for such a change to be blocked, as Greg Maxwell stated on the Bitcoin developer mailing list:

```
It can be fixed with a soft-fork that
further constraints block timestamps,
and a couple of proposals have been
floated along these lines.
```

In Conclusion

Bitcoin's timestamp security and the simple rules constraining the window of acceptable timestamps have withstood 10 years in an adversarial environment despite their known weaknesses. We know that a 51% cabal of miners could wreak havoc on the network, at least for a short time, but this has never happened—likely because the incentives are not aligned for miners to do so. Rational miners would not choose a short term gain in return for killing the long term golden goose.

Thanks to Jimmy Song and David A. Harding.

Bitcoin Has a Branding Problem — It's Evolution, Not Revolution

For technologists and historians, it may well be a revolution; but for everyone else — it's an evolution in personal finance.

By Ryan Radloff

Posted March 6, 2019

Before we get started I've broken this post out into two parts to address the point, so please bear with me regarding format.

Part 1 — I take a look at how our financial lives trend towards convenience (and as a result, dependence on intermediaries); and whether we should expect that to change anytime soon.

Part 2 — I look at the larger evolution of assets from physical to 'digital' over the last 35+ years; and where bitcoin fits in that trend.

Both parts are important to illustrate a critical point — for the end user, bitcoin doesn't exist in a vacuum. It exists on a spectrum of evolution for consumers and the best thing we can do to drive adoption is acknowledge this nuance.

Langley, N., Garland, J., Morgan, F., LeRoy, M., Ryerson, F., Haley, J., Bolger, R., ... Baum, L. F. (1939). _The wizard of Oz_. Hollywood, Calif.: Metro Goldwyn Mayer.

Part 1: Trending Towards Convenience (Dependence)

As an American residing in London, it takes me around two weeks from the moment I walk into a local bank branch to complete the arduous and highly manual process of verification (a.k.a. **K**now **Y**our **C**ustomer) in order to become an account holder.

This system is so inefficient that it has birthed a new array of challenger banks (e.g. Revolut, Monzo and Starling Bank). These banks focus on eliminating the

inefficiencies and friction of traditional banking, and claim to put us more in control of our finances than ever before.

This model and mission has driven rapid growth for the aforementioned companies, and altered our notion of what a bank looks and feels like.

Yet at the same time, it's a model and mission which, to borrow from *The Wizard of Oz*, asks us to " *Pay no attention to that man behind the curtain…* "

...and perhaps more than ever before, that is the paradox at play here.

Pay No Attention to That Man Behind the Curtain

While new Fintech banks/platforms provide the illusion of closer proximity to our finances, in many cases these platforms are nothing more than a re-engineered interface for the traditional financial system, with new branding.

For example, Yolt is really just a slick front-end for Dutch multinational bank ING; Wealthify, a brilliant UI owned by Aviva; Zelle — founded by Bank of America, Wells Fargo and JPMorgan Chase — backed by even more banks; and Nutmeg, the mobile choice for investment management, is substantially owned by Goldman Sachs.

Sure, with a few taps I can send £4 I owe you for that latte faster than ever before. But the net result (trade-off) of the rapid digitalisation of the financial system is a requisite increase in specialised financial intermediaries layered on top of each other, built to eliminate the 'friction' points of the legacy world.

And here lies the paradox:

While we've been hit with slogans like ' *New Money'_as we venture deeper down the path of convenience banking, we're really just interacting with a new facade of the legacy financial system.*

With that context, it's easy to understand why people are confused when a truly digital, fully bearer asset enters the picture — ' *New Money'* incarnate.

We don't initially understand 1) how it's different than what we already have and 2) why we should ever be concerned about what is going on behind the curtain of our new digital banks.

After all… we're in control of our finances, not them — so who cares?!

To the second point, what most people don't realise is the unfortunate reality that the existing system has 'evolved' into an incredibly complex web of financial intermediaries built on top of and around each other. All meant to distribute risk more evenly (yet rarely do), the actual result is an opaque fiefdom for risky (and unscrupulous) behaviour.

Look no further than some of these headlines from the last few years…

- HSBC to pay $1.9 billion U.S. fine in money-laundering case
- Watchdogs impose $3.4B fines in bank forex probe
- Deutsche Bank settles silver, gold price manipulation suits
- Banks face $1bn bill over fees-for-no-service scandal
- JPMorgan to pay more than $135 million for improper handling of American Depositary Receipts (ADRS)
- Wells Fargo is paying $575 million to states to settle fake account claims

This isn't even to mention banks' central role in the 2008 financial crisis, the lasting effects of which have been well documented and which no doubt impacted countless families in immense ways — my own included.

As Elaine Ou opined for Bloomberg:

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

And to the first point regarding how digital assets are different than what we already have… those outside of crypto-land have their PayPal app, their Venmo accounts and can easily send $4 internationally to a friend without using Bank of America or Barclays. **Why do they need anything new, *much less a revolution?***

Revolution is a rallying cry for early adopters, and a historians' view on what is actually evolution, in real-time.

Revolutions are inconvenient, messy and disruptive to the status quo, a default which we are unfortunately biased towards.

Revolutions often only happen as an absolute necessity, when 'society' has exhausted all other options and tensions have evolved to a breaking point.

So when outsiders (read: people we would like to eventually opt-in to this new system) hear the "revolution" declaration from bitcoiners, it simply doesn't resonate.

Humans are wired to seek confirmation of our own biases and be sceptical of new ideas that challenge or threaten our worldview.

The Evolution Amidst the Revolution

Challenger Fintech banks are winning hearts and minds by capitalising on the weaknesses of bigger, bulkier competitors. Legacy banks are now 'evolving' with their own facades meant to capture those same hearts and minds.

Consumers are loving the evolution toward convenience and 'control.'

I would argue that Bitcoin is simply part of this larger migration away from our parents "brick and mortar" banks toward more nimble, digital financial services.

While Bitcoin is a revolution with respect to approach, infrastructure and (dis)intermediation; to the consumer, it will (and should) feel like it is part of the same evolution that they have been part of all along.

Although Bitcoin does indeed seek to revolutionise the financial industry by separating money and state, "revolution" doesn't need to be the lede.

From most people's perspective, we've gotten along just fine paying no attention to that 'man behind the curtain.' Why should we expect to change that behaviour en masse all of a sudden?

Part 2: Reframing Bitcoin in the Progression to Digital Finance

In an effort to track the larger progression towards digital finance (an evolution over 35+ years in the making), our research team at CoinShares developed a qualitative approach that plots the dependency of an asset on financial intermediaries against how digital an asset is (as defined below).

As I touched on in the previous section, we witnessed an explosion in the number of financial intermediaries as we've moved towards 'convenience banking'. The truth, however, is that the number of intermediaries has been mushrooming for much longer, coinciding with a shift in preference towards digital proxies for financial assets.

For the purposes of this exercise, we defined "dependency" as an asset's dependence on — or independence from — third-party intermediaries in order to buy, sell, and custody said asset. We've plotted this on the y-axis in the charts below.

On the X-axis, we plotted how "digital" an asset has become. This was measured by tracking the preference to interact with that asset in a non-physical, 'proxied' format

(i.e. digital) — whether it be an ETF, option, future, etc. — rather than the underlying asset itself.

For both of these measures, we used quantitive data whenever available, and supplemented with qualitative observations when it was not. In these instances, we identified specific inflection points to warrant movement on the 'dependency' y-axis.

For example, fine wine is generally considered an illiquid asset. In 1982, it was tradable in rare circumstances when a buyer and seller were paired. Yet in 2000, Liv-ex launched to bring transparency and efficiency to fine wine trading via an electronic exchange. A few years later, they launched the Liv-ex 100 Fine Wine Index. Today, there are a number of structured investment vehicles (e.g. the Vinculum Wine Fund) that offer exposure to this asset class — beyond purchasing the wines themselves; but this also introduced new intermediaries to the process.

CoinShares Independence Analysis
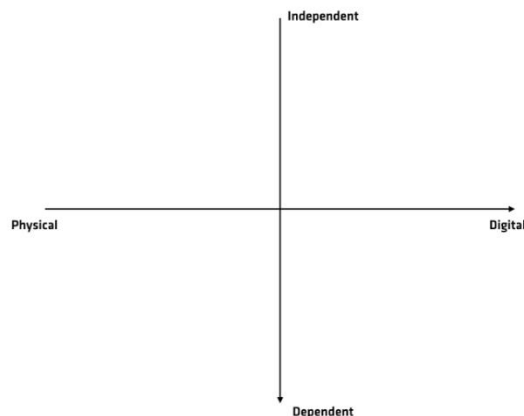
Methodology

x-axis = digital
Ratio derived between physical traded and futures (as a proxy for digital volume)

y-axis = dependency
Scoring derived from dependency on financial intermediaries, custodians, and average correlation of assets

Indices used:
Equity = MSCI World Index
Debt = FTSE G7 Index
Oil = European Brent Spot/Futures
Base Metals = Bloomberg Base Metals Spot
Gold = Gold Spot/Futures
Real Estate = FTSE EPRA Nareit Developed Index
Wine = Liv-ex 100 Benchmark Fine Wine Index
BTC = Bitcoin spot

CoinShares Research

Across nearly all asset classes, as transactions shifted to the digital sphere, they required more intermediaries; and as a result, rendered assets 'more dependent.' The exceptions were equities and real estate, which involved a number of intermediaries even before this shift to digital.

As a part of this mini-survey, we also looked at the shift in transaction volumes from physical trades to electronic ones. This became one of our proxies for the digitalisation of assets — the transition of exchange volumes from open outcry to electronic trades.
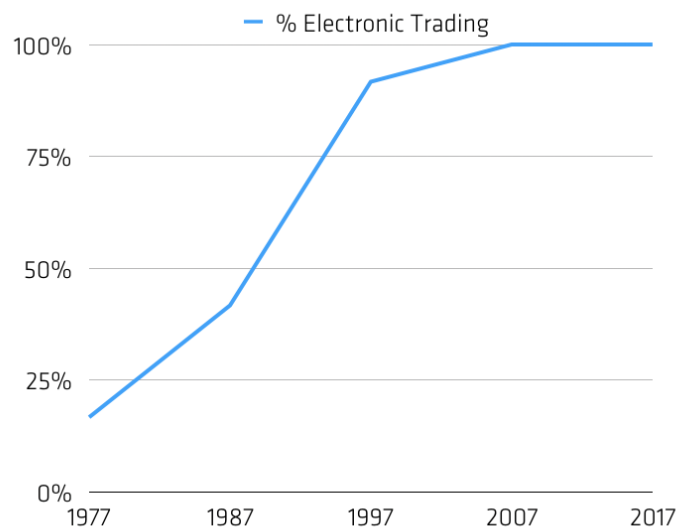
Open Outcry trading versus electronic — CoinShares Research

In a short amount of time, digitised, electronic trading accounted for more than 50% of all bids placed. By the early 2000s, open-outcry trading was effectively extinct.

This same evolutionary phenomenon is particularly well illustrated by commodity trading, which saw a quick proliferation of interest in synthetic derivatives compared to the previously dominant physical volume. The below graphs show the relative growth in futures markets versus physical volumes for Gold and Oil.
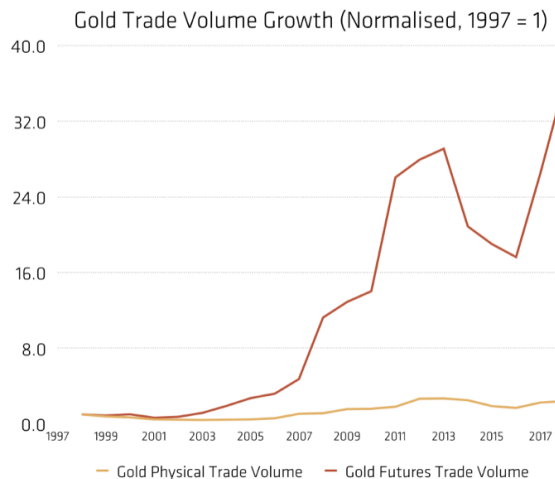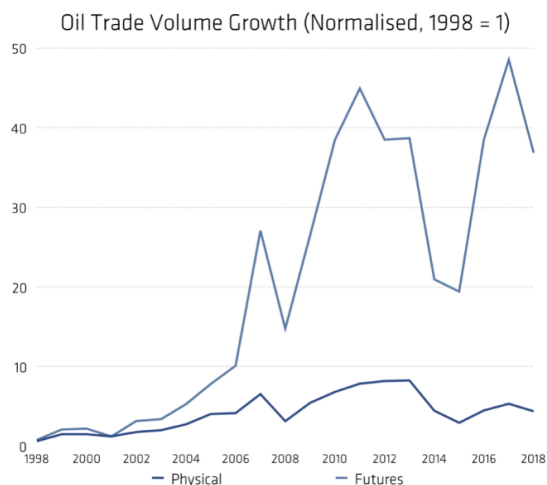
Please note that while there are many Gold and Oil derivatives, we have used futures as a proxy to represent this digital shift. Had we included the market for Gold ETPs, this shift would be even harder to deny.

Having plotted dependency and digitalisation on these axes, the changes between years is interesting to track (shown below from 1982–2017):
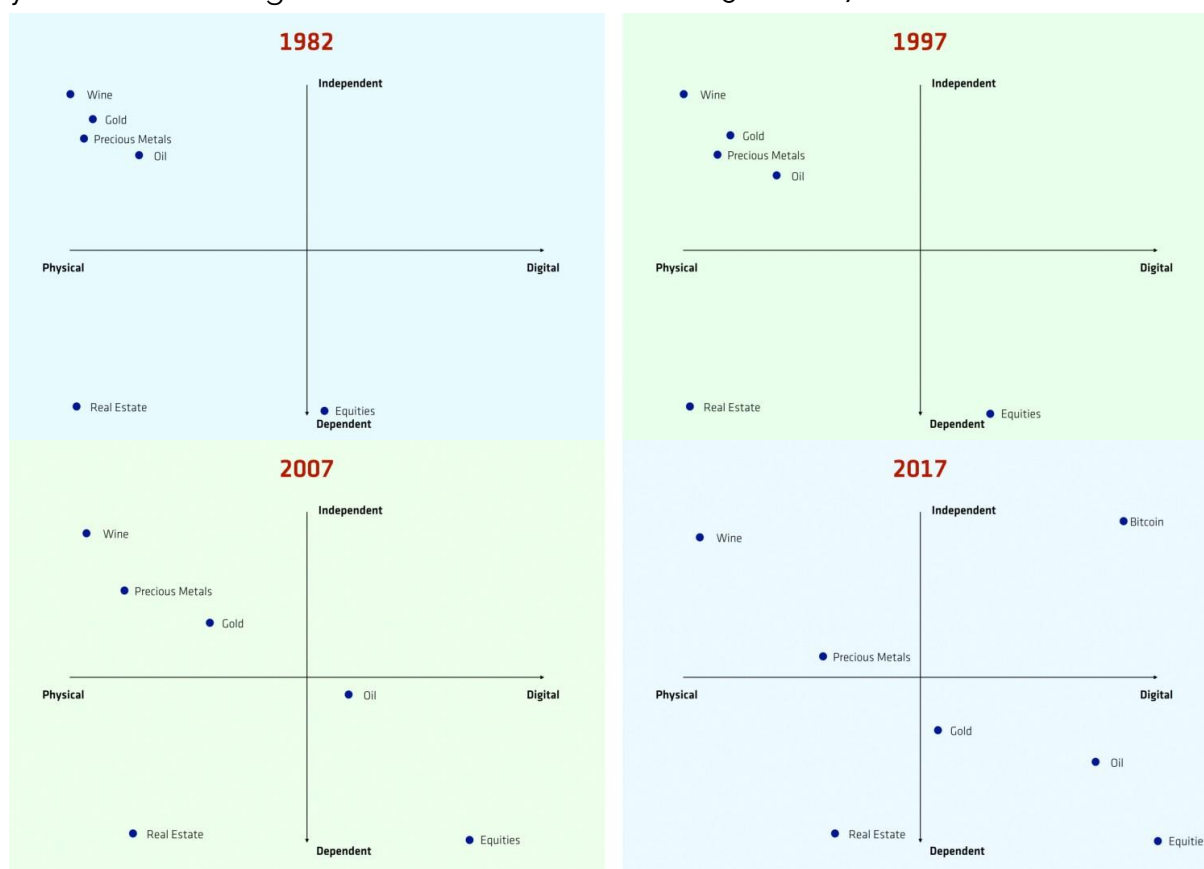
Representational Figures. CoinShares Research.

Throughout each phase of this trend, it seems that one asset leads, or paves the way, and others follow. I expect bitcoin's emergence as a new type of asset, which lives in the top right quadrant, to have a similar effect and pull other assets in this direction as well.

I believe it is likely this will occur within the 'second layer' infrastructure that is being built on top of the bitcoin blockchain. There is already technology being deployed which facilitates 'tokenisation' of real-world assets, in a format compliant with existing regulations — as my business partner Danny Masters has touched on.

In the meantime, however, this category represents a tiny fraction of global assets, and in any case has clear potential for substantial growth.

So why does this matter?

Until Bitcoin was introduced, we never had a functional way to operate independently from this web of financial intermediaries in the digital sphere; no way

to hedge against financial intermediaries in the same way that we could with our physical offline portfolio (e.g. physical gold, fine art, wine).

Before Bitcoin, digital investments always required a trusted third-party for settlement, clearing, and custody.

Bitcoin's 'why' is that it removes the *need* for intermediaries and provides an alternative choice to the system — not simply a spiffy facade.

That choice is an ***evolution*** of a trend which dates back over 35+ years now.

If we want consumers to consider adoption, we need to start thinking about how this fits in the larger context — bitcoin does not exist in a vacuum.

One of the most important features of Bitcoin is that it gives users the choice to hold a completely digital bearer asset, and manage the keys for themselves to eliminate counter-party risk.

Don't get me wrong — I still expect intermediaries, lots of them in fact.

The business I run on a daily basis acts as an intermediary, offering convenience and a familiar format (ETP) in exchange for control over the underlying assets the product track. Many exchanges offer a similar proposition, acting at least as a temporary custodian for customer funds.

Custodian / Owner / Source	Amount of BTC	Current Value (USD)	% of current bitcoin supply	Date of Ref
Coinbase	856,000	$3,259,836,320	4.875%	12/19/18
Xapo (discounted for GBTC & COINXBT)	826,997	$3,149,386,154	4.710%	5/9/18
Grayscale Bitcoin Trust	206,525	$786,491,342	1.176%	1/31/19
Binance	194,479	$740,618,398	1.108%	2/26/19
MT. Gox Trustee	137,891	$525,119,264	0.785%	9/25/18
Bittrex	130,005	$495,087,451	0.740%	2/26/19
Bitfinex	119,538	$455,227,307	0.681%	2/26/19
Bitstamp	108,848	$414,518,197	0.620%	2/26/19
Huobi	108,135	$411,801,870	0.616%	2/26/19
Kraken	79,103	$301,239,989	0.451%	2/26/19
XBT Provider Bitcoin ETPs	53,937	$205,405,162	0.31%	2/26/19
Bitmex	35,482	$135,123,262	0.202%	2/26/19
Coincheck	29,838	$113,630,506	0.170%	2/26/19
Bitmex Insurance Fund	21,719	$82,710,893	0.12%	2/25/19
			TOTALS	
Current BTC Supply (Uknown Custody)	14,649,953		BTC In Other Hands	2,908,497
Current BTC Price (Messarl)	$3,808		Current Value (USD)	$11,076,196,115
Current BTC Supply (Messari)	17,558,450		% of current supply	16.6%

The above table is only in regard to bitcoin holdings, not other crypto assets. Please feel free to drop a note in the comments of any products we may have missed. You can also view our full data and sources here.

A quick scan of the publicly reported bitcoin being held by an entity that is not the ultimate beneficial owner shows that at least 17% of the currently circulating bitcoin supply is likely custodied by a third-party.
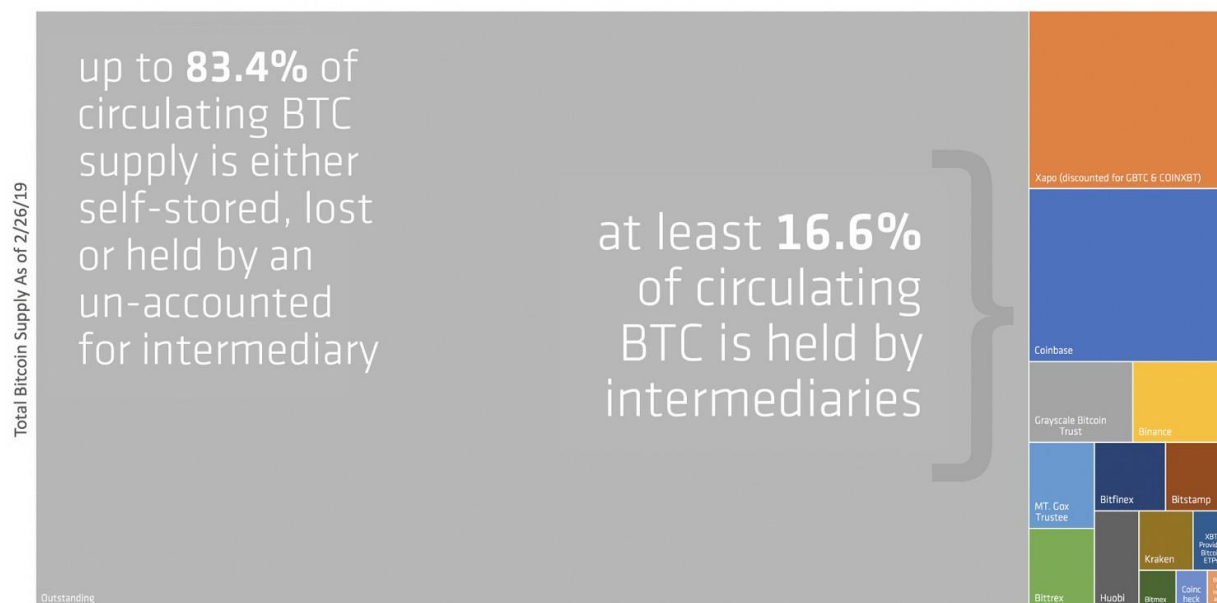
Coinshares Research

Third-parties offer convenience, alleviate the hassle of key management and custody, and can streamline compliance requirements. Third-parties are not inherently good or bad; they simply offer a service to which users have grown accustomed.

But what is different about Bitcoin and this new digital paradigm is that these users finally have a choice. They have an option to utilise the convenience of these intermediaries, and the security trade-offs (risks) are clear.

In other words, with Bitcoin the risks are right there in front of you, and each individual has the opportunity to choose how much of that risk to take.

This is a huge leap forward in the evolutionary progression of our digital financial lives, especially when we consider the web of complexity and blind trust that consumers are required to place in our current financial system.

Personally, I could not be more excited for what comes next. But I'll conclude by asking a favour…

Right now, too much of Bitcoin's "viva la revolución" mantra feels like this:

Do us all a favour — help Bitcoin, and please STOP SCREAMING ANARCHY AND REVOLUTION. We might just help the world evolve — and drive bitcoin adoption — in the process…

Much credit to many members of the CoinShares team for the contributions, edits and comments — getting this right is always a team effort.

Skeptic's Guide to Bitcoin: Investing in Bitcoin

By Su Zhu & Hasu

Posted March 6, 2019

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

We don't talk much about price in this blog, but we will make an exception today to show how to value bitcoin using a high-level approach. We'll highlight three significant trends in the world and suggest how either one of them could lead to increased demand for neutral, private money in the future.

How to value Bitcoin

On a long enough timeframe, valuing bitcoin is straight-forward. The market finds a price based on available supply and demand. When more people want to buy bitcoin than sell it, the price goes up and vice versa. For most types of assets, a price increase entices producers to make more of it, pushing the price back down. Likewise, a price decrease leads to a decrease in supply, making the price go back up. As a result, most goods tend to be relatively price-stable near their cost of production.

Bitcoin has a fixed supply. There will only ever be 21M units, and we always know how many of them exist. The market can still try to create
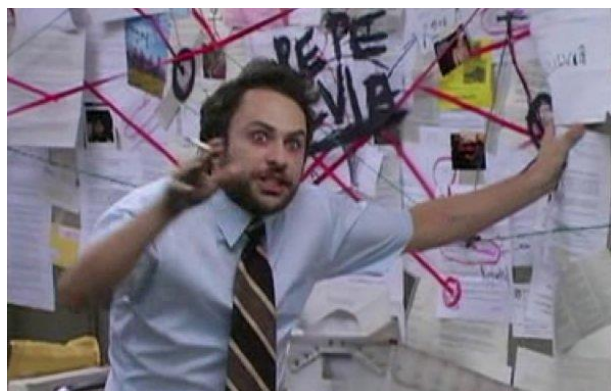
"substitute goods" (other cryptocurrencies with similar properties) to increase the supply. We fully expect this to (continue to) happen, but money has immense "brand value" in the form of network effects, liquidity, and integration in existing financial infrastructure. Bitcoin's supply isn't entirely inelastic to changes in demand, but certainly less so than other assets, leaving upside to be captured by existing owners rather than producers.

The sum of all bitcoin multiplied with their price is called market capitalization. Comparing "market caps" of assets like fiat currency, real estate, stocks or commodities allows us to see how much value people store in them at any given time. Bitcoin's market cap today is $80b, which is small compared to what we could see as potential target markets to disrupt:

- US dollar notes held abroad: around $1T, including over 75% of all $100 bills in existence ([source](#))
- Global base money: $19.6T ([source](#))
- Gold held for investment purposes: around $1.1T privately held (excluding jewelry) and $1.3T held by central banks ([source](#))

Since the supply side of bitcoin (and substitute goods) is less responsive to changes in demand, we expect rising demand to manifest in a higher exchange price. We see three primary sources of such future demand.

Demand for digital cash

90% of all money today is virtual. It is created when someone takes a loan and henceforth lives on a bank ledger—until the debt is paid and the money destroyed or it is withdrawn as cash.

The growing trend away from physical cash to digital payments is understandable. Cash has the annoying property that you need to be in the same location to exchange it. Most of us are also paid digitally for the work we do, so to pay in cash one would have to constantly replenish it.

Countries that have abandoned the use of physical cash altogether are called "cashless". It can happen without coercion, like in Sweden. In other countries like India, the government has demonetized larger denomination banknotes. In China, digital payments serve as a tool of social control and the backbone for a new social credit system.

Central banks around the world are enthralled by the idea of negative interest rates—the ultimate holy grail of monetary control. In a cashless society, they can directly tax people's bank accounts to disincentivize saving and encourage "aggregate spending" in the form of consumption and investment.

Digital payments are highly efficient and convenient, but they are not "money" when it comes to the properties that our parents and their parents have been used to. It is a new form of money that makes very concrete tradeoffs. Digital payments receive their efficiency gains from including a trusted third party in every transaction that maintains a central ledger that it can much easier update when told to. This arrangement doesn't come without drawbacks: The intermediary monitors all financial activity, can refuse transactions he disagrees with, or even confiscate funds altogether.

Cash, on the other hand, can be exchanged peer-to-peer between people. The transactions are permissionless, private and immediately final (no one can revert them after the fact.)

As our reliance on financial intermediaries grows, so does the importance of who controls them. Today, a small number of payment companies have a disproportionally large impact to define what speech is acceptable online and what businesses should be allowed to operate. Money is the lifeblood of the economy — someone who is cut off by payment processors loses his autonomy and almost any chance to run his business.

Every year, the world is moving closer towards going "cashless". The reason, in our opinion, is that the benefits of digital payments are immediate and visible to the user, while the downsides are invisible until they matter. As a consequence, the global supply of physical cash will continue to drop. This drop, however, is not an accurate reflection of the demand to hold it. Governments, central banks, and large corporations have an incentive to push for a <u>cashless society</u> (though not all of them do), while cash has no coordinated, commercial interests backing it. Demand for cash is also underrepresented as long as financial intermediaries can be wholly trusted, which isn't guaranteed to last forever. It seems unnecessary like fire insurance — until it burns.

Bitcoin is the first and only form of money that offers cashlike properties but can be stored and transferred digitally. When governments no longer provide physical cash, there could be a lot of excess demand for an asset with cashlike properties looking for a release valve — and bitcoin is in a unique position to offer that.

Demand for a global, neutral settlement network

Digital payments work for parties who have a middleman they can trust. Since WW2, the US has been this trusted middleman for most of the developed world. Lately, the US has shown they are willing to weaponize the financial system to command their political will (by pressuring SWIFT into cutting off Russia and Iran as part of their sanctions). It is not well received by their allies.

Additionally, political moods in many countries are turning towards isolationism, both in Europe (Brexit, revolts in France) as well as the US (trade war with China, threats to leave nuclear arms treaty with Russia). US-led soft power institutions like the WB, IMF, and WTO are gradually losing their influence. These were the main tools for projecting US power abroad, and their disenfranchisement will leave power vacuums and uncertainty in their wake. We believe the world is currently moving away from having one trusted protector and intermediary, to a multipolar world order.

As frictions between world powers increase, the willingness to trust financial infrastructure controlled by someone else will decrease. That creates demand for a financial network that is not controlled by one party but is politically neutral. Even online, censorship is on the rise. China's internet is effectively cut off from the rest of the world, and Russia is <u>planning</u> to follow suit.

Bitcoin fulfills the conditions of being neutral and censorship-resistant. While in the past, controversial activity found a home in Bitcoin (like Silk Road and Wikileaks), the world could wake up to the benefits of censorship-resistance as a positive trait that is no longer "just for criminals."

Demand for a hedge against failure of the existing system

Many people are worried about the overleveraged state of the world economy and our financial system. Both consumer and sovereign debt levels are at all-time highs relative to GDPs, while interest rates, especially in Europe and Japan, are still zero. When the economy slows down, there is little that central banks can do to ease the pain and kickstart the economy.

Further, a widespread shift in demographics has created a massive gap between future government liabilities and income from taxes. For example, the US government doesn't "just" owe $20T in sovereign debt but <u>ten times as much</u> in domestic debt, in the forms of entitlements programs. Many believe that the only way to pay up is by throwing the US dollar under the bus and devalue it to meet at least nominal obligations.

Given, this is a doomsday scenario and not very fun to think about, but it's a reality that any investor has to deal with today. Gold has traditionally been a trust anchor when investors flee out of fiat currency, but it is also highly co-opted by governments, hard to secure and repatriate—as some countries <u>experience today</u>. We believe that over a long enough timeframe bitcoin can become the gold of the internet-native generation and take its place as a hedge against government and central bank failures.

"Bitcoin as doomsday insurance" is a narrative that is picking up steam and that is now commonly cited even by skeptics such as Ken Rogoff as a primary use case of bitcoin. As more people are getting worried about systemic risk, demand for bitcoin as limited "insurance tickets" could rise accordingly.

That bitcoin does, in fact, work as an exit ramp for weak local currencies can be seen in Venezuela and other South and Central American countries, where bitcoin is increasingly adopted "on the ground" as an alternative to the US dollar. A recent study about global data from the peer-to-peer exchange LocalBitcoins found that "*in the 4th quarter of 2018, as Bitcoin price and interest seemed to hit their doldrums, 23 countries on LBC had their best quarters ever. Almost all of these countries are in the developing world.*"

The US dollar is still the most sought after black market currency, but bitcoin is better at some things that make it an attractive alternative for people in developing countries. It's easier to protect against confiscation (for example using a brain wallet) and transfer digitally—especially across borders. Skeptics of bitcoin often miss the fact that currency competition is like running from a bear—you only have to outlast your slowest friend. Bitcoin, in its current immature form, competes with the weakest of fiat currencies, not with the US dollar, Euro or JPY, and does so despite its price volatility.

Is Bitcoin's volatility a problem?

I'm often asked if bitcoin's price volatility will prevent adoption. Bitcoin is volatile for two reasons. First, bitcoin's supply is fixed and doesn't react in changes to demand. Second, as a young currency, it is mainly used for speculation today. Its price is a function of deferred expectations of growth (and expectations of other people's expectations, and so on), all of which get revised all the time. The best way to think about volatility is as a temporary transaction cost. As bitcoin's market capitalization grows, less of its value will be from speculation (as there is less future growth to bet on) and more from

fundamental usage. That will lower bitcoin's volatility and make it cheaper to use.

While it can be seen as a chicken-egg problem initially—bitcoin needs adoption to become price-stable, but many forms of adoption require price-stability—using bitcoin has a different value to different people. Bitcoin's success as money shouldn't be judged by its ability to perform consumer payments. Instead, bitcoin is first adopted by those who can tolerate the costs because it helps them better than existing alternatives— or because there are no alternatives. With every additional group of people bitcoin serves, it becomes less volatile and cheaper to use, making it more attractive for use cases which are slightly more price-sensitive. A positive feedback loop! The fact that anyone uses bitcoin today, despite its volatility and complexity, is amazing to me and should be seen as a ringing endorsement by the market.

Summary

Bitcoin is a new financial network with a token (also called bitcoin but with a lowercase 'b') that is currently in its monetization phase. During this phase, its price is largely determined by expectations of future growth—making it expectedly volatile. Despite the cost and complexity, people use bitcoin on the ground today in developing countries and to make unstoppable transactions online. The more people use it, the less volatile it will become, encouraging further adoption.

Since bitcoin's supply is fixed (and substitute goods hard to make), the price is largely a function of demand to hold it. We identified three major trends in the world that could lead to significant demand down the road. Demand, that bitcoin is well positioned to serve— often as the only competitor— and that could create significant upside for existing holders.

Privacy and Cryptocurrency, Part I: How Private is Bitcoin?

Eric Wall

March 7, 2019

This is part 1 of a series

- Privacy and Cryptocurrency, Part I: How Private is Bitcoin?
- Future post will go here

Foreword

The Human Rights Foundation cares deeply about protecting our civil liberties and privacy in our increasingly digital age, especially in places where people live under authoritarian governments. Without a free press, without local watchdog organizations, and without effective ways to hold governments accountable, the 4 billion people who live under authoritarianism need our help, and technology is one way we can reach out. As we've seen with the evolution of encrypted messaging, virtual private networks, and free knowledge initiatives like the Tor Project, Wikipedia, and Signal, technology can be a liberation tool, if built with the right values in mind. But as we've seen with centralized platforms ranging from Facebook to WeChat, technology will also be a tool of surveillance and even social engineering.

Unless we take a stand now, and help make platforms and protocols with user privacy and decentralization in mind, mass surveillance and social credit may be the inevitable future. To help elevate this conversation, the Zcash Foundation has provided generous support for HRF to bring Eric Wall on as a Technology Privacy Fellow. Eric will be working with HRF for the next six months, writing five essays on privacy technology, with a special focus on cryptocurrency and how we can preserve privacy in the financial world. We look forward to sharing Eric's work with you, and seeing it inspire fresh conversations with policymakers, philanthropists, investors, students, and the builders of our current and future technology infrastructure.

— Alex Gladstein Chief Strategy Officer Human Rights Foundation —-

Key points:

- If you're an activist or a journalist, you may wonder how safe it is to use bitcoin to escape the prying eyes of a government or corporation
- Bitcoin is only semi-private; the protocol doesn't know your real name but transactions can still be linked to you in a myriad of ways
- Blockchain analytics firms specialize in deanonymizing bitcoin activity and sell this data to corporations and law enforcement agencies
- A grasp of how the system works and use of tools such as Tor, coin control, CoinJoin transactions and avoiding address reuse can make a crucial difference in protecting your identity and transactions from being unmasked
- This article aims to give the reader a primer on Bitcoin privacy—later articles in the series will look at different wallets, compare different cryptocurrencies and survey exchange platforms in regions with restricted economic and political freedom
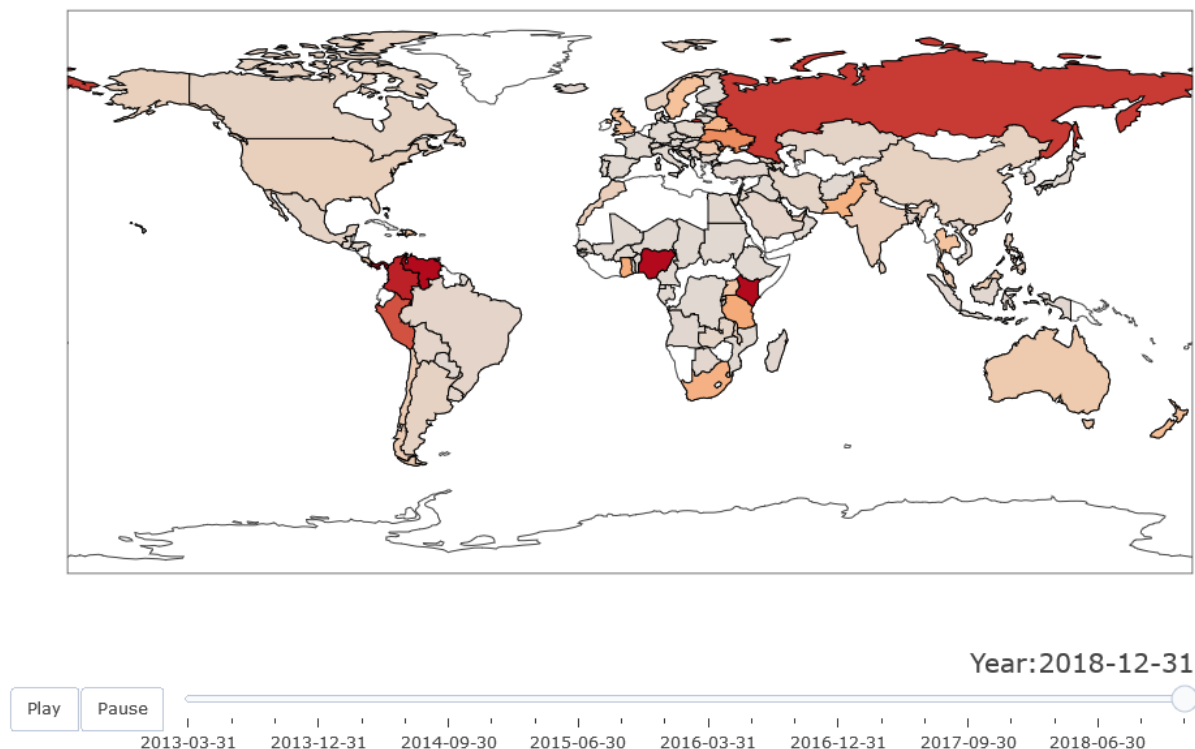
Why cryptocurrencies?

It's clear from the onset when observing cryptocurrencies at a protocol level that they are inherently more privacy-oriented than traditional digital payment systems. At the base layer of these protocols, there is typically no mapping between users' cryptographic key pairs and their real-world identities, yet they allow us to store and transfer wealth across the globe with an unprecedented degree of freedom.

The intention of the Human Rights Foundation is to examine these technologies and elucidate on their potential of bringing economic and political freedom to the individual. While there are many angles in the context of money that are within the scope of such an endeavor, we've chosen to focus on the topic of privacy foremost. In that pursuit it's also clear that the degree to which cryptocurrencies enable privacy is not by any means trivial or binary—it varies greatly depending on the user's particular choice of core and ancillary technologies and usage patterns, as well as the capabilities and sophistication of the attacker.

Regardless of that, we can observe that the adoption rate of cryptocurrencies—in particular, bitcoin—is increasing in countries where the economic freedom of the population is limited. While the liberating and democratic aspects of cryptocurrencies are apparent, especially the extent to which they enable censorship-resistant transaction networks and monetary policies impervious to various forms of government sabotage, none of these benefits are particularly helpful as long as authoritarian regimes can deanonymize and prosecute the users of these currencies at will.

LocalBitcoins Volume per Internet-Connected Economically Active Person by Country

Year: 2018-12-31

| Play | Pause |

2013-03-31   2013-12-31   2014-09-30   2015-06-30   2016-03-31   2016-12-31   2017-09-30   2018-06-30

Many thanks to Matt Ahlborg for lending us this visualization from his great piece "Nuanced Analysis of LocalBitcoins Data Suggests Bitcoin is Working as Satoshi Intended " which explains the exact methods used to generate it.

The ambition of this initiative is to cut through the complexity of the cryptocurrency privacy subject by sourcing subject matter expertise from the industry. When we approach this subject, we recognize that we enter into a complex field, and as in any complex field, experts disagree. We will strive to strip this initiative from personal biases and condense opinions and research into simple practical guidelines.

The product of this research will be an article series of which this is the first piece.

A primer on Bitcoin privacy

Bitcoin is neither completely anonymous nor completely transparent. The Bitcoin privacy conundrum exists in a grey area where the unmasking of a user's financial activity ultimately depends on the capabilities of the adversary and the sophistication of the user and their choice of tools. There is no perfect privacy solution for any activity on the Internet, and in many cases, privacy-conscious choices come with tradeoffs to both cost and ease-of-use where no one-size-fits-all

solution exists. Moreover, privacy is never a static thing but evolves continuously and in response to the battle between those who build tools to protect privacy and those who build tools to destroy it.

The Bitcoin protocol itself evolves over time, which can lead to dramatic changes in its privacy properties. Changes to the core protocol are seldom simple choices between privacy and transparency alone, but more often come packed with changes to the security, scalability, and backward-compatibility of the software as well. Historically, the trend and ethos within the Bitcoin community has always favored privacy over transparency, but more conservatively so compared to other cryptocurrencies where privacy is the primary focus.

As a result, activists or journalists who are considering using bitcoin to escape the prying eyes of an authoritarian government or a corporation need to understand what type of traces they leave when they're using it and whether the privacy nature of bitcoin is sufficient for their needs. However, achieving this understanding requires some amount of effort.

Tracing transactions

When you transact on the Bitcoin network you leave two types of traces. These can be categorized into "what's on the blockchain" and "what's not on the blockchain". The information that is on the blockchain reveals no direct link between your identity and your transactions, but it does reveal information that can link your transactions to each other. What *does* link your identity to your transactions are the things in the second category: "what's not on the blockchain".

What's not on the blockchain

When you transact on the Bitcoin network, you are sometimes sending or receiving money to/from some entity that knows who you are. That entity will then have outside-of-the-blockchain-knowledge that links your identity to a transaction.

When you combine this fact with the other fact that your transactions can be linked to each other, the result is that motivated entities can sometimes figure out how you're using your bitcoins, how much you have and who you've been transacting with.

There are also countless ways you could be linked to a transaction even *without* having transacted with an entity that knows who you are, since Bitcoin transactions are typically sent in unencrypted packets over the Internet and the source IP address can be pinpointed through various means. Bitcoin transactions sent via full nodes such as Bitcoin Core require some triangulation or targeted traffic sniffing in

order for the source IP address to be estimated, whereas other "light" wallets such as mobile wallets (Mycelium, Blockchain Wallet, Coinbase Wallet) will often broadcast transactions through company-run servers that can see your IP address directly and your full transaction history. The same is true for most hardware wallets (Ledger, Trezor) in their out-of-the-box setups.

Geolocation IP databases can often roughly approximate your physical location using your IP address. You can test it out yourself using this link, then enter the coordinates you get into an interface like Google Maps. More importantly, your IP address reveals your Internet Service Provider (ISP), which in turn knows the real-world identity of the owner of your IP address and often has a legal obligation to store this information for several months.

Even if you are using a public WiFi network to transmit your transactions, you could still accidentally associate your real identity with that IP address from the websites you visit and the background services your device connects to. Your Dropbox application will gladly connect to Dropbox's company servers when you start your laptop which will associate that IP address with your Dropbox account in Dropbox's server logs. The same thing will happen when you browse to a personal account on any website. Even if you don't visit any personal web accounts, cookies stored on your laptop can reveal who you are to the website you browse to through your cookie's association to your previous browsing history. Many websites allow third parties to track users like this for analytics purposes—Google alone is estimated to track users across 80% of the sites of the entire web.

Even if you clear your cookies, website operators can track you across their different sites as long as your browser fingerprint is unique and associate your IP address to your identity that way. And even if you have no services running and avoid browsing altogether, your device's MAC address could get exposed to the network provider which could be linked to your identity using sophisticated methods. So, even if your IP address doesn't lead back to you via an ISP record, you might still leave other traces that do when you're using your personal devices.
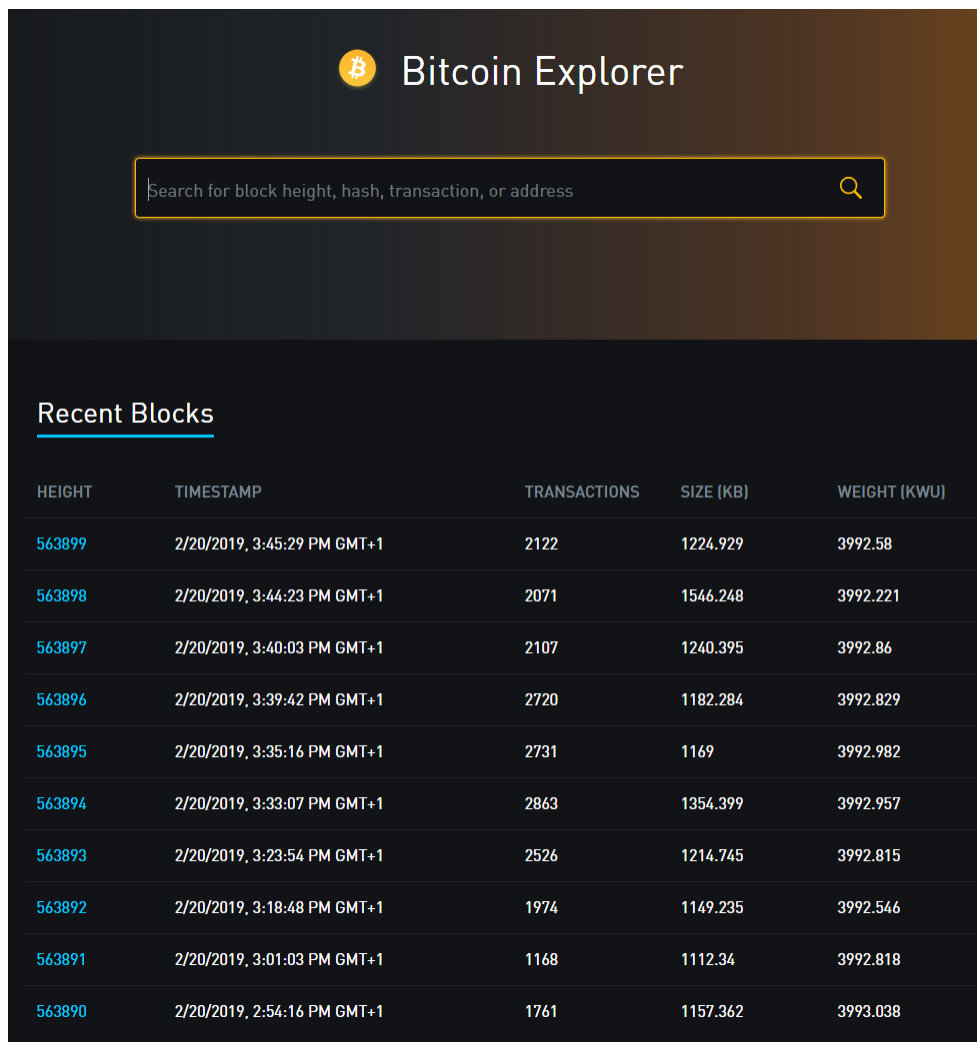
The worst category for privacy is of course when using third-party services that implement know your customer (KYC) practices as your Bitcoin wallet, as these services will keep logs of all your transactions and your real-world identity.

You could also be linked to a Bitcoin address or transaction just by searching for it using web-based tools since there usually aren't that many people other than you who are going to be looking up your transactions on the web for no good reason. Keep this in mind as we move to the next segment. Other data that isn't on the blockchain but can easily be logged about your transaction is the approximate time it was broadcast to the network.

The current known best method to hide your source device and IP address when retrieving information about transactions or when transmitting transactions is to leverage Tor hidden services. Many wallets including Bitcoin Core will provide this as a configurable option while others have it built-in. The Tor browser can similarly be a useful tool for your web-based Bitcoin-related activity as it, in addition to hiding your IP address, clears cookies upon each exit, prevents third-party cookies and is immune to most browser fingerprinting techniques.

What's on the blockchain

A simple way to begin understanding what type of information is revealed by the Bitcoin blockchain is to use a block explorer. For this exercise, we'll use the open-source explorer blockstream.info.

Bitcoin Explorer

Search for block height, hash, transaction, or address

Recent Blocks

HEIGHT	TIMESTAMP	TRANSACTIONS	SIZE (KB)	WEIGHT (KWU)
563899	2/20/2019, 3:45:29 PM GMT+1	2122	1224.929	3992.58
563898	2/20/2019, 3:44:23 PM GMT+1	2071	1546.248	3992.221
563897	2/20/2019, 3:40:03 PM GMT+1	2107	1240.395	3992.86
563896	2/20/2019, 3:39:42 PM GMT+1	2720	1182.284	3992.829
563895	2/20/2019, 3:35:16 PM GMT+1	2731	1169	3992.982
563894	2/20/2019, 3:33:07 PM GMT+1	2863	1354.399	3992.957
563893	2/20/2019, 3:23:54 PM GMT+1	2526	1214.745	3992.815
563892	2/20/2019, 3:18:48 PM GMT+1	1974	1149.235	3992.546
563891	2/20/2019, 3:01:03 PM GMT+1	1168	1112.34	3992.818
563890	2/20/2019, 2:54:16 PM GMT+1	1761	1157.362	3993.038

The most recent block at the time of writing (#563899) in the Bitcoin blockchain contains 2122 transactions. Let's look at what a randomly chosen transaction reveals.
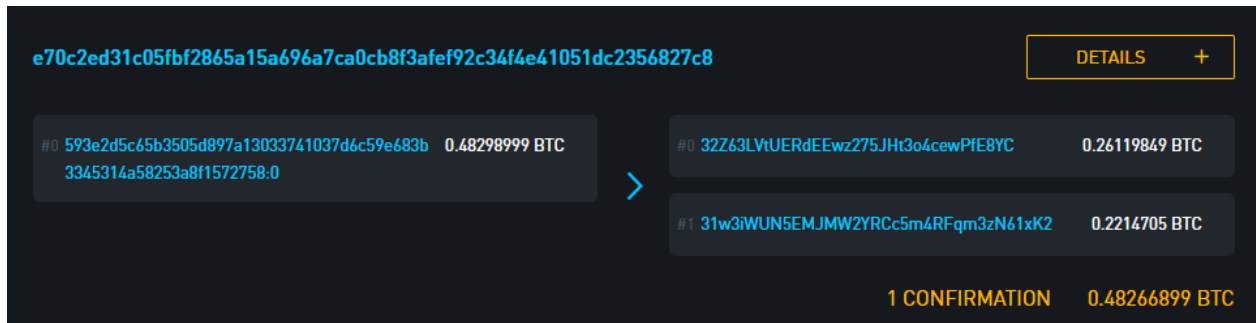
Transactions contain inputs and outputs and are identified by transaction IDs (seen at the top in the image above). If your Bitcoin wallet has sent a transaction, each transaction will be associated with one such identifier.

From a high-level view, what is revealed about this transaction is the following:

- The approximate time the transaction was mined (from the block header)
- The addresses bitcoins were sent to and the amounts sent (i.e. the "transaction outputs")
- The source of the funds for the transaction (i.e. the inputs)

Let's look at each of these items individually for the transaction shown above, e70c2ed31c05fbf2865a15a696a7ca0cb8f3afef92c34f4e41051dc2356827c8

Time

Transactions are not timestamped, but blocks are. Block timestamps are not necessarily precisely accurate, but assuming a majority of miners are reporting time honestly, all blocks are bound to be reasonably accurate within a few hours range. For the blocks mined by the honest miners, they'll be precisely accurate. This doesn't mean that the block timestamp is necessarily accurate within a few hours range to *its transactions' broadcast times* however, since it can sometimes take a lot longer for a transaction to be included in a block. Some block explorers complement data this by displaying the time they first saw a transaction on the network to give a more accurate view of transactions' broadcast times.

The approximate time when the transaction above was included in a block can be derived by looking at the block header (in our case it's block #563899 with the timestamp 2019–02–20, 14:45 UTC).

The addresses bitcoins were sent to and the amounts sent

The receiving addresses in this transaction are:

```
1: 32Z63LVtUERdEEwz275JHt3o4cewPfE8YC 0.26119849 BTC
2: 31w3iWUN5EMJMW2YRCc5m4RFqm3zN61xK2 0.2214705 BTC
```

There is more to an address than what meets the eye. It's easy to think of Bitcoin addresses as "hard-to-read email addresses but for bitcoins", but an address isn't always a simple pointer to a certain user's cryptographic key-pair. What addresses are in reality, are cryptographic descriptors of the *spending rules* for the next time someone wants to move those bitcoins.

For example, if you send bitcoins to:

```
37k7toV1Nv4DfmQbmZ8KuZDQCYK9x5KpzP
```

the configuration of this address is such that you're not sending bitcoins to an owner of a particular private key, but rather to a spending rule that releases the coins to anyone who can provide two different strings that have the same SHA-1 hash (this would mean that the SHA-1 hash function is broken, which it was in 2017— so don't send anything to that address!). What's good to note is that since many address formats used today are hashed when we send bitcoins to them, we t ypically can't tell what those spending rules are until someone spends bitcoin from that address, as they need to reveal what was hashed in order to do so.

In our example transaction, the blockchain reveals that bitcoins have been spent from both addresses, so the spending rules for those addresses are known.

```
32Z63LVtUERdEEwz275JHt3o4cewPfE8YC
```

was revealed to be a 2-of-2 multisignature address when it was spent from in the transaction

```
f491dfe9867c36e85950116a90a6128060d6070866ad0f3598d70d146750162f
```

We'll look at exactly how that information is revealed in the next section.

Similarly, it was revealed of

```
[31w3iWUN5EMJMW2YRCc5m4RFqm3zN61xK2](https://blockstream.info/address/31w3iWU
N5EMJMW2YRCc5m4RFqm3zN61xK2)
```

that it is a frequently used 2-of-3 multisignature address and at the time of writing holds roughly 2,700 bitcoin (US$10.6m). More advanced blockchain tools such as oxt.me will even plot the wallet balance over time and display with approximate accuracy which hours of the day it has seen the most activity.

Historical balance and activity relating to the address
31w3iWUN5EMJMW2YRCc5m4RFqm3zN61xK2 (oxt.me).

Seeing as 18:00-22:00 UTC are the hours with the least activity for this address, it wouldn't be unreasonable to assume that these hours represent the night-times 01:00-05:00 or 02:00-06:00 in the region where the address is controlled. Given the hours of activity, the volumes and the multisignature setup of this address, one could guess that this address belongs to a cryptocurrency exchange in the GMT+7/8 time zones.
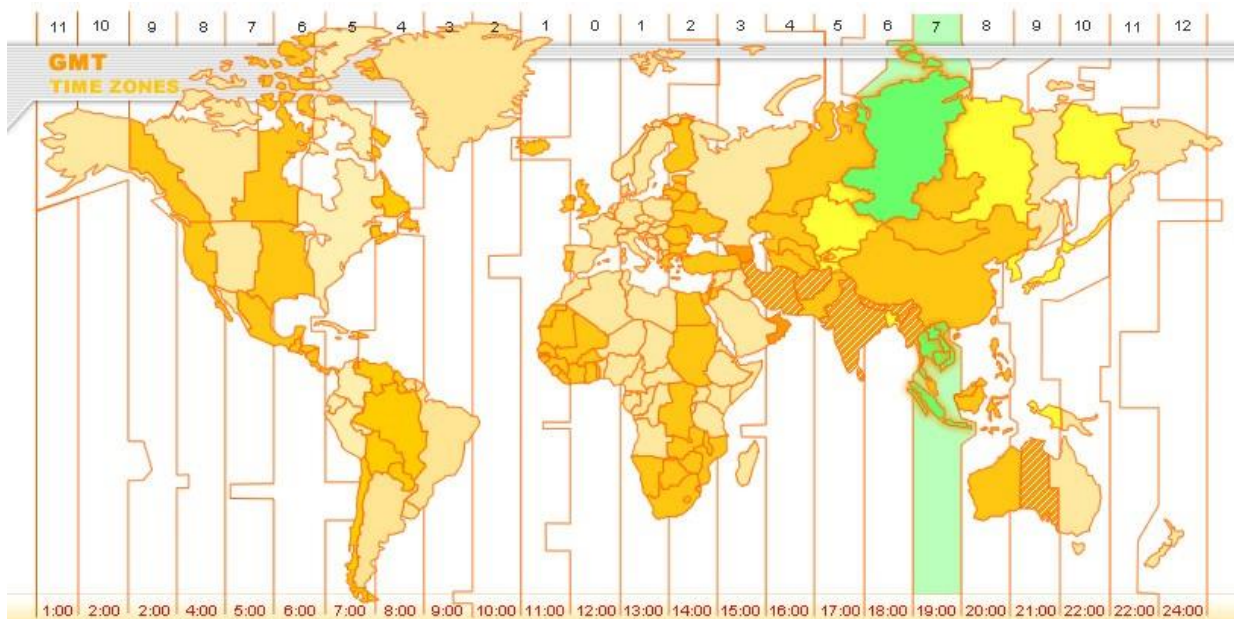
It's considered good privacy hygiene to never reuse a Bitcoin address because it helps to break transaction linkage. That's also a good idea for all users of P2SH addresses (all addresses starting with a "3" and 62-character addresses starting with "bc") because by the time you reveal what the spending rules are for that address, you've already sent the bitcoins to a new, hashed address for which the spending rules are yet unknown.

Wallets known as HD wallets can generate many addresses but only require a single back-up seed in order to access the funds. These wallets will also automatically generate a fresh address for you every time you've received a transaction.

Now let's look at the transaction again to see what else we can reveal about the sent coins.
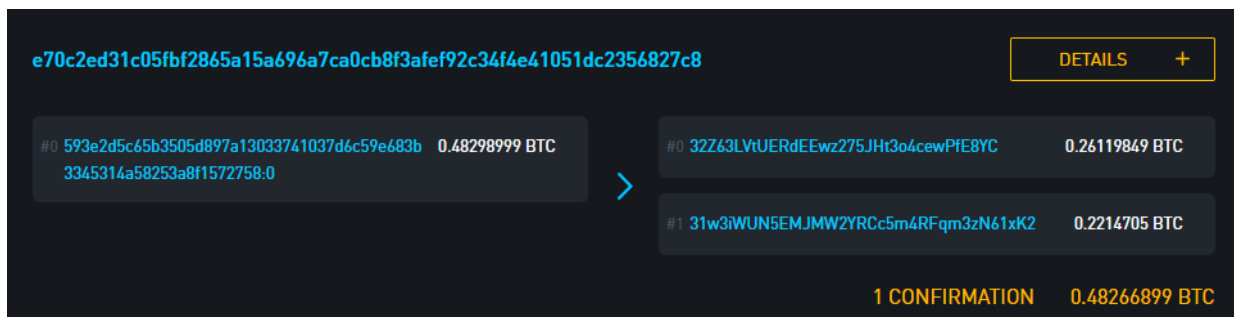
Bitcoin transactions are regularly directed towards *two* addresses where one of the transaction outputs is the actual payment and the other is what is known as a "change output" going back to the sender. It's similar to when you pay for a $3 item

with a $5 bill, it creates two payments; one of $3 to the merchant and one with the
change of $2 going back to the one paying.

Identifying a transaction output as a change output requires the use of _heuristics_
.Examples of heuristics that can be used to discern a change output from the other
payment are; the usage of round numbers (in the bitcoin amount or in the fiat
currency value of the amount at the time of the transaction), the order of the outputs
in the transaction body and so on. In our chosen transaction, it's easy to detect the
change output because it's going back to the same address that was used to
receive the bitcoins that were spent, as we'll see below.

In principle, Bitcoin wallets behave somewhat differently from each other and leave
different traces on the blockchain — similar to how browsers reveal pieces of
information about themselves when they browse the web. Because of this, it is
sometimes possible to identify certain transactions as originating from a certain kind
of Bitcoin wallet application.

If your adversary knows which wallet application you're using then that knowledge
can contribute to mapping your identity to one of your transactions, which would
weaken your privacy. Every little piece of information helps an adversary paint a
picture of who you are and what you are doing.

The source of funds for the transaction

In Bitcoin transactions, the "source of funds" is always other "unspent" transactions,
or to be precise, unspent transaction outputs (known as UTXOs). It's good to keep in
mind that what is seen in a block explorer is a combination of decoded raw
blockchain data and _derived_ data. One block explorer might choose to display the
transaction like this:

e70c2ed31c05fbf2865a15a696a7ca0cb8f3afef92c34f4e41051dc2356827c8

31w3iWUN5EMJMW2YRCc5m4RFqm3zN61xK2 (0.48298999 BTC - Output)	➡ 32Z63LVtUERdEEwz275JHt3o4cewPfE8YC - (Spent)	0.26119849 BTC
	31w3iWUN5EMJMW2YRCc5m4RFqm3zN61xK2 - (Spent)	0.2214705 BTC
		0.48266899 BTC

From blockchain.com.

Here the "source of funds" is displayed as an address. Blockstream's explorer
chooses to display it like this, where the source of funds is displayed as a
transaction:

The reason why Blockstream's explorer doesn't show an address as the source of funds is that addresses aren't technically a part of the inputs to a transaction and it isn't always possible to infer the notion of an originating address (example). Moreover, since address reuse is discouraged, it's good to break inherited mental models from traditional payment systems and not further cement the idea that money could or should be sent back to the recipient at the same address by showing addresses as senders.

Let's get more technical for a moment and look at the decoded raw data of the transaction, which you can fetch from your own local copy of the Bitcoin blockchain if you run a full node (or by using a trusted web-based interface). Here's what it looks like:

```
1   $ bitcoin-cli getrawtransaction e70c2ed31c05fbf2865a15a696a7ca0cb8f3afef92c34f4e41051dc2356827c8
2   {
3       "version": 2,
4       "locktime": 0,
5       "vin": [
6           {
7               "txid": "593e2d5c65b3505d897a13033741037d6c59e683b3345314a58253a8f1572758",
8               "vout": 0,
9               "scriptSig": "0020fa28dc1e5eb222055e90f8cade9bcd13ca9ddab7a5ed029e27d41a736f7455ce",
10              "txinwitness": [
11                  "",
12                  "304402204d969f7102fd24009c21533e65c506f2083e0c372994a5e724c2ba831ce42f1
13                  10220623958a13694d19b7c3a65553d862d04d67decb565969594c1a2cd26afb8de9801",
14                  "30440220235ec716247a2a2dfae4aeaee6c16bac3be4055b70c7585f4cf25a77b30775d
15                  5022011771761f11dd8f040c9a2dcd15e1e0ef88f0cfb7b4b1f7037d384622e4bef7501",
16                  "5221027111c0d6cbc3a40c6e6197ed234bd6e59f277c88094fd33297b1e0a3787a5b7d2
17                  102e71711c9840d68e6401d4bd5df78f1850e25ae41f082f4b38ceec37d60cab5442103
18                  eeae18900c0d12046f644b960a1ef84589f7f4f71d07914006d550bf85c576e153ae"
19              ],
20              "sequence": 4294967294
21          }
22      ],
23      "vout": [
24          {
25              "value": 0.26119849,
26              "scriptPubKey": "OP_HASH160 09783c21e42b639f4f91819706aa42949361762c OP_EQUAL",
27          }
28      },
29      {
30          "value": 0.22147050,
31          "scriptPubKey": "OP_HASH160 02a751dc8c10e35fed2c6eddc2575c9af2c71d23 OP_EQUAL",
32      }
33      }
34  ],
35  }
```

e70c2ed31c05fbf2865a15a696a7ca0cb8f3afef92c34f4e41051dc2356827c8 decoded (manually trimmed).

The source of funds is described by the `vin`-array. It doesn't refer to an address specifically. Instead, it refers to the output of a previous transaction;

`593e2d5c65b3505d897a13033741037d6c59e683b3345314a58253a8f1572758`
, where `vout: 0` refers to that transaction's *first* output (`vout: 1` would mean its second output, and so on). This unspent transaction output (UTXO) is the *source of funds*.

To clarify what this means, the source of funds for a transaction is not an address, nor is it a transaction. The source of funds is a specific *output* of a specific previous transaction. Knowing this will help you protect your privacy when using bitcoin, as we'll see in later sections.

The source of funds for
e70c2ed31c05fbf2865a15a696a7ca0cb8f3afef92c34f4e41051dc2356827c8.

We can further decode parts of this transaction from the decoded raw data such as what's in `txinwitness` to find out more about the source of funds. The last hexadecimal string in `txinwitness` reveals the 2-of-3 multisiginature script, which allowed us to deduce that it's likely to be an exchange wallet.

```
1    $ bitcoin-cli decodescript
2    5221027111c0d6cbc3a40c6e6197ed234bd6e59f277c88094fd33297b1e0a3787a5b7d
3    2102e71711c9840d68e6401d4bd5df78f1850e25ae41f082f4b38ceec37d60cab54421
4    03eeae18900c0d12046f644b960a1ef84589f7f4f71d07914006d550bf85c576e153ae
5
6    {
7        "result": {
8            "asm": "2 027111c0d6cbc3a40c6e6197ed234bd6e59f277c88094fd33297b1e0a3787a5b7d
9                    02e71711c9840d68e6401d4bd5df78f1850e25ae41f082f4b38ceec37d60cab544
10                   03eeae18900c0d12046f644b960a1ef84589f7f4f71d07914006d550bf85c576e1
11                   3 OP_CHECKMULTISIG",
12           "reqSigs": 2,
13           "type": "multisig",
14           "addresses": [
15               "164GApvfW9FkteXYS2J6RsSp262dEBxF6H",
16               "1A4PaXs5CJRy2BLN5wXxqYKPjvia9T8v8c",
17               "1Q55L1VQ616mCdrQD9jwUSqZGeiSDhRBs9"
18           ],
19       },
20   }
```

The two other hexadecimal strings we saw in the txinwitness are just the signatures fulfilling this 2-of-3 multisignature condition.

Now that we've identified the source of funds, we can see in this example that it's a 0.48298999 bitcoin output (~US$1850), even though the sent payment was just one of ~US$1000. This has an undesirable consequence: imagine a situation in which a friend pays you $10 but the transaction reveals that he's the owner of a million dollars and has immediate access to send the full amount— obviously not very good for privacy. If you are worried about disclosing information about your bitcoin wealth when you are sending a payment to someone, you need to be aware of which inputs are used in your transactions (more on this below).

Combining the knowledge

Because transactions always need to provide the source of funds, transactions become linked together, producing what's known as a transaction graph. If you pay a friend in bitcoin, not only will your friend see the inputs you used in the transaction, but you will also be able to see when your friend spends those coins and to which addresses the coins are sent.

Some addresses are known in the Bitcoin space, such as the Bitfinex cold wallet or the seized Silk Road coins. An address can become known because an entity—for example, a business or a charity—advertently exposes their deposit or donation addresses on their website, or inadvertently because a forum post or a law enforcement record publicly reveals the connection. Blockchain analytics firms will scrape the web regularly to find such information.

Other addresses become exposed via association through a technique called clustering.

Clustering

Let's go back to our example transaction from the previous examples, e70c2ed31c05fbf2865a15a696a7ca0cb8f3afef92c34f4e41051dc2356827c8. Here, we can immediately see that both the source of funds of our transaction and our transaction (red dots) have been used to jointly fund a third transaction (big blue dot).
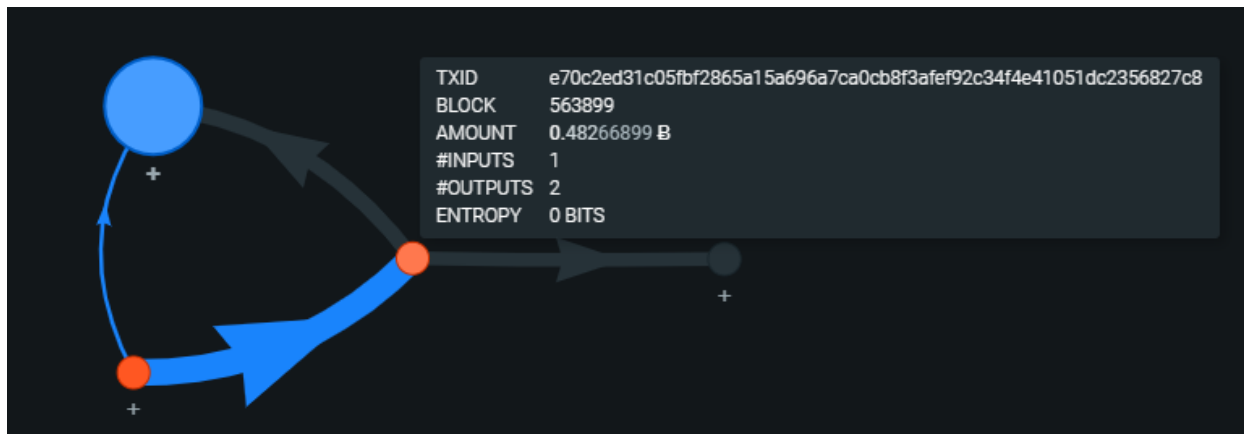
Transaction graph for
e70c2ed31c05fbf2865a15a696a7ca0cb8f3afef92c34f4e41051dc2356827c8 (oxt.me).

Particularly, it's the second output of the funding transaction and the first output of our transaction that are involved in funding this transaction. They were previously sent to the addresses:

```
3Qt1YaJwQwtHMb4mjJ41DZVawWXih9LGMq
32Z63LVtUERdEEwz275JHt3o4cewPfE8YC
```

On the surface, these appear to be two separate addresses with just one innocuous-looking incoming and outgoing transaction each. But because their private keys have both been used to sign the big blue dot transaction, these addresses now all belong to the same *cluster* (along with 407 other addresses involved in the inputs to the transaction), which we can make assumptions about having the same owner. This heuristic has gone under a couple of different names in the past, the most recent one being the common-input-ownership-heuristic.

Transaction graph for "the big blue dot" transaction
f491dfe9867c36e85950116a90a6128060d6070866ad0f3598d70d146750162f (oxt.me).

Blockchain analytics firms will use such heuristics to create giant clusters. The blockchain explorer WalletExplorer has pinned the two addresses to belong to a cluster of 162787 addresses in total. Analytics firms label such clusters with all identities (IP addresses, user accounts, organizations, real names) they're able to pin to the cluster in order to map out the Bitcoin transaction ecosystem. They then sell access to these data sets to law enforcement agencies and other companies.
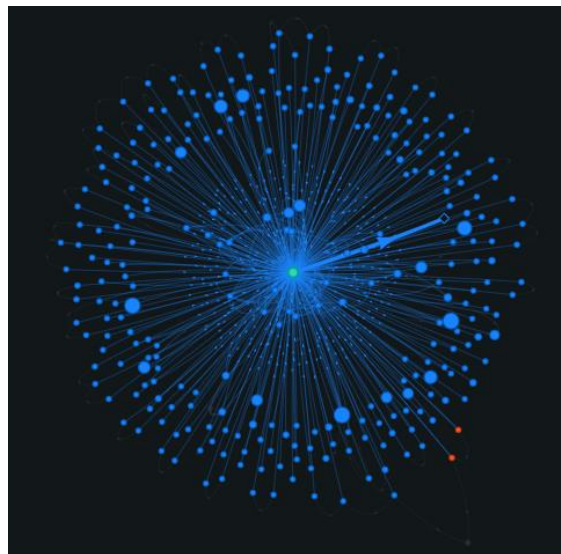
Many blockchain analytics firms receive information about transactions directly from their own customers, such as cryptocurrency exchanges. However, two of the largest analytics firms, Chainalysis and Elliptic, have stated that they do not trace back transactions to specific individuals in the data they receive, but only to the exchanges or other business entities (1, 2).

It only takes the deanonymization of one address in a cluster to deanonymize an entire cluster.

Breaking the heuristics

We've seen now that there are a multitude of ways your identity can be linked to a certain Bitcoin address or transaction and yet another multitude of ways your Bitcoin transactions can be linked to each other. When put together, these information leaks in combination can unmask our entire financial privacy.

Some Bitcoin users intentionally try to make this kind of analysis difficult by using tools and techniques to break the heuristics analytics companies employ. Some techniques decrease the effectiveness of the heuristics through distortive methods while others attempt to avoid the heuristics altogether. Bitcoin wallets can assist users by automating some of these techniques or make them available through a user interface.

Here's a non-exhaustive list of some examples:

- Randomizing the order of outputs when creating transactions to decrease change output detection accuracy (example).
- Avoiding address reuse via HD wallets.
- A PayNym is a publicly sharable ID which allows you to receive payments at different unassociated addresses you control that only become known to you

and the sender. The PayNym allows a new address to be derived for each payment without you having to manually present a new address each time, which is great if you want to conveniently receive, say, donations online using bitcoin.

- Coin selection/coin control—wallets can be designed to prioritize clustering fewer addresses together when possible by selecting inputs for transactions more carefully (example), or allow users to select inputs for transactions manually to avoid revealing ownership of certain coins (example).
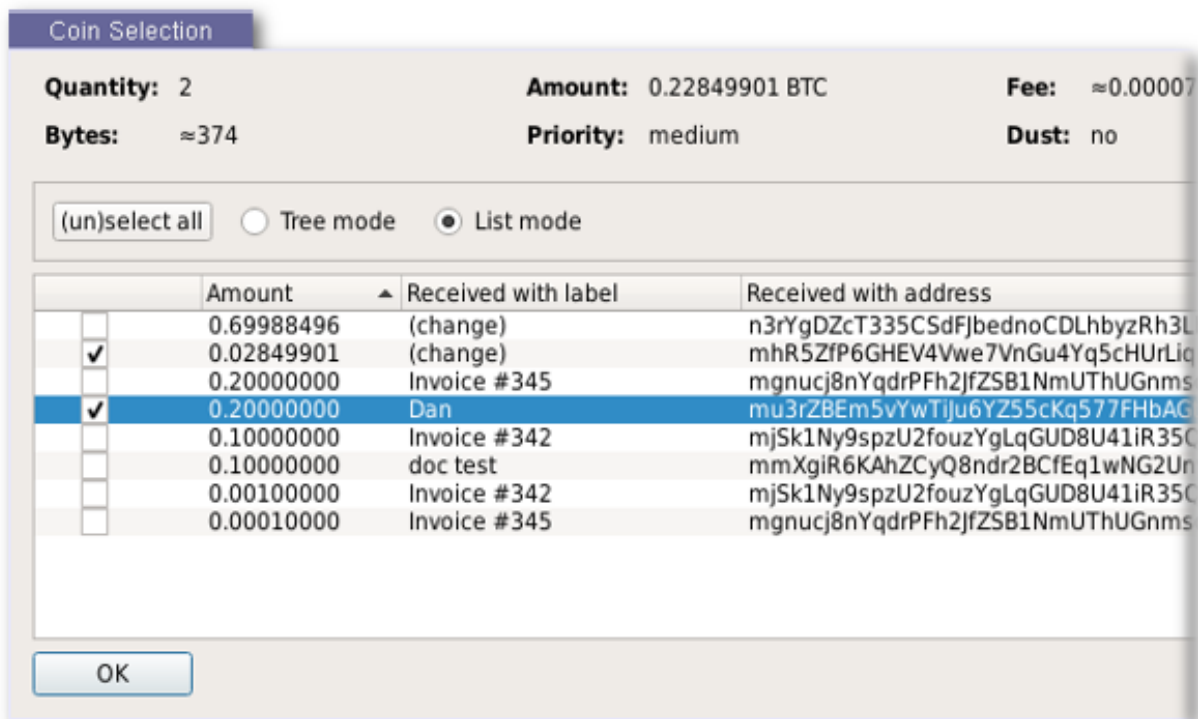
Coin control in Bitcoin Core—user can manually choose the source of funds for a transaction.

A more advanced example of a privacy-enhancement technique is **CoinJoin**transactions. CoinJoins are a scheme which adds many inputs from many different users into a joint transaction before the transaction is broadcast.

In our example, we saw how the input of a transaction always references a *specific* output of a previous transaction, rather than the whole transaction:

The source of funds for
e70c2ed31c05fbf2865a15a696a7ca0cb8f3afef92c34f4e41051dc2356827c8.

But the inputs and the outputs *within* each individual transaction don't reference each other in any way; transactions are valid as long as there's enough bitcoin in the inputs to cover all the outputs.

A CoinJoin transaction (72046c65fa25724f11c91f35799f69b66072bc07b2b4e3fc363852c2506b2b90) created by the Wasabi Wallet.

Here, the outputs are chopped up into many equal-amount chunks, so you can't be sure which input funds which payment. The result is that a payment can have a plethora of possible "source of funds" indiscernible from one another, as well as a plethora of possible destinations. This technically doesn't *hide* the source of funds or the destination, but it mixes it so that it becomes difficult to prove what actually funded a particular payment and who's bitcoins went where.

What's also interesting about these kinds of transactions is that they complicate the idea of the common-input-ownership-heuristic. These inputs would all get flagged as belonging to the same owner, which in this transaction they aren't. The images

below show false clusters of independent payments as a result of CoinJoin transactions.

CoinJoin transactions created by the Wasabi Wallet. Transaction IDs from left to right: 72046c65fa25724f11c91f35799f69b66072bc07b2b4e3fc363852c2506b2b90, d7a428a8e3d69f236519cb999dbcb47b3b283548875371da567259be806e35ea, 20cf4fa2f685167f46682dd30c7720a06618656939fadbd1f20e3d471d08dfbb (oxt.me).

But because these transactions all have the odd look of equal-amount outputs, they're rather easy to spot and can be eliminated from the clustering analytics tools. Equal-amount CoinJoin transactions are best understood as *mixers* to be used when one wishes to obfuscate the source of funds for a payment and the destination to which a payment is sent.

However, the same principle is used to create transactions that are indistinguishable from normal transactions in a recent invention called a **PayJoin** or **Pay-to-EndPoint (P2EP)**. This emerging transaction type mixes inputs from the payer and the recipient and pays the recipient by shifting over the payment amount from the sender's output and to the recipient's output during a real payment for something.
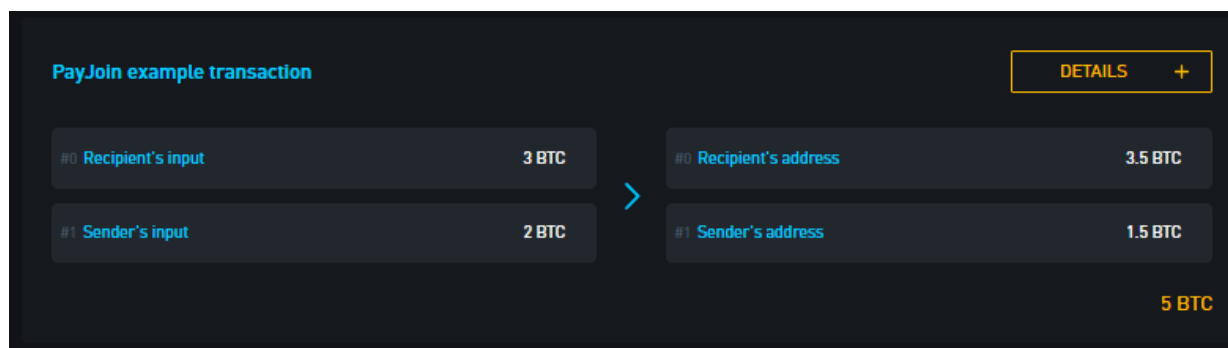
A PayJoin transaction template where the sender pays 0.5 bitcoin to the recipient, mixing inputs with each other in the process.

This transaction doesn't do a lot of mixing—but it does trigger the common-input-ownership heuristic erroneously. More importantly, it triggers the heuristic without leaving any clues for the analytics firms to *not* cluster the inputs together, which they would need to in order to avoid giving false positives. If the usage of PayJoins becomes widespread, the portion of false common-input-ownership positives could become so great that the heuristic itself becomes unreliable, which would be a massive setback for the blockchain analytics tools.

The Lightning Network

The Lightning Network is a beta technology that is being developed on top of the Bitcoin protocol to facilitate low-cost, instant payments. The Lightning Network is accessible to users of Lightning wallets. Lightning transactions differ from base-layer transactions in many ways which make them advantageous from a privacy perspective:

- Lightning transactions are not stored on a public ledger.
- Lightning transactions use onion routing which doesn't disclose who the final recipient is to the rest of the network.
- Lightning transactions don't mix inputs and can't be clustered together.

The Lightning Network is a system of channels which require liquidity; the current set of merchants and users that accept Lightning payments today are a small subset of the total set of Bitcoin users in the system, and not all payments (especially larger ones) can propagate through the channel system, although that is expected to improve over time. This also means that while Lightning can provide improved privacy for the transactions in its channel system, those channels still need to be funded by regular Bitcoin transactions, which are subject to the privacy concerns in this post.

Another problem is that unlike base-layer Bitcoin payment recipients, recipients of Lightning payments are required to have a Lightning node running. Your node communicates with other Lightning nodes using TCP/IP. Whenever your node interacts with the network (sending, receiving or routing other payments) someone will learn about the existence of your node, its public key and its IP address. From your public key, it's trivial to find out which channels are open between you and other nodes, and how many bitcoins you each have committed to those channels upon opening them. For private channels, the IP address is only revealed to the ones you have an open channel with, but for public channels, it's revealed to the entire network and it's even possible for someone to probe the channels' current balances to figure out if you're a target worth attacking.

When you run a Lightning node, you should assume that your channel balances are known and that they can be linked to your IP address. For this reason, running your Lightning node over Tor is a good option to protect your privacy.

The Lightning Network is currently under quite rapid development and many of its properties might be subject to change in the near future.

Protocol changes

There are several privacy-enhancing technologies that are in development for the base-layer Bitcoin protocol. Here are a few examples:

- Schnorr signatures—a signature scheme which, among other improvements, makes multisignature addresses indistinguishable from single-signature addresses
- Scriptless scripts—a method by which to use scripts without disclosing the actual spending rules
- Taproot—a technique with the potential of making transactions of all types of spending rules indistinguishable from each other

Conclusion

This article aims to give a primer to how privacy works in Bitcoin. The pseudonymous but transparent nature of the Bitcoin blockchain creates an environment where the privacy of the system ultimately hinges on the tools employed by the user and the spying entity. Users who take few precautions for protecting their privacy will most likely leak enough financial information in order for it to be dangerous, assuming that the spying entity is analyzing the blockchain.

The next step is to get acquainted with how different Bitcoin wallet applications can help with privacy, and what to expect when using them. This will be covered in the next article in this series. In later articles, we will look at different cryptocurrencies

and survey available exchange platforms in regions with restricted economic and political freedom.

Further reading

To completely understand what is going on under the hood of Bitcoin, Andreas Antonopoulos' Mastering Bitcoin is an excellent resource which is translated into several languages.

More specifically, the Privacy page on the Bitcoin Wiki goes into much more depth on several of these topics and was very recently updated by Chris Belcher. The Blockstream block explorer was also patched recently to show "privacy ratings" for transactions and is now a good resource to learn more about what conclusions can be derived from transactions' information.

Special thanks to Adam Gibson, Tomislav Dugandzic and Simon Bohlin for their thoughts and feedback to this article.

The essays in this series will form the basis for a report to be published by Coin Center, the leading cryptocurrency policy research and advocacy group based in Washington, DC.

The Zcash Foundation contributed funding for the project. The Zcash Foundation exists to build and support tools that enable privacy and autonomy, particularly with respect to people's transactions and financial information. Privacy is important for numerous reasons—personal, medical, political, and more. For this reason, Zcash pioneers the use of zk-SNARKs, a novel form of zero-knowledge cryptography with strong privacy guarantees. Ultimately, the Zcash Foundation's impact will come from serving the needs and workflows of real people, including those from many backgrounds and locations.

The views and opinions expressed by Eric Wall does not necessarily reflect the views of his employer or any affiliated entity.

The Lightning Network Reference Rate
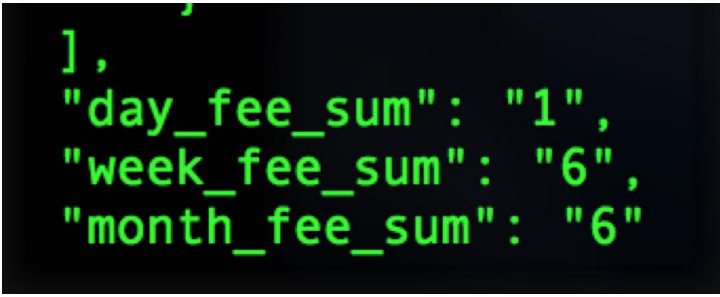
Nik Bhatia

Posted March 11, 2019

The Lightning Network Reference Rate, Part 4 of 4

Abstract

I present a three part proposal for Lightning Network node operators. The first and most crucial part of the proposal is a node-level calculation standard for the accrual of satoshis. The Node Accrual Rate (NAR) is offered as a formula to calculate the profitability of an individual Lightning node, expressed as an annualized interest rate.

The second part of the proposal is to convince Lightning node operators to disclose their NARs to each other. Transparency and financial disclosure are core tenants of capital markets, and the disclosure of NARs could correspondingly push bitcoin forward on its path to becoming a more robust asset class.

The third and final part of the proposal is to advocate a framework in which NARs across the network can be aggregated, averaged, and reported as one rate called the Lightning Network Reference Rate (LNRR). LNRR can pave the way for a world of relative value calculations and be instrumental in the pricing of off-chain bitcoin lending.

This is not a proposal for any changes to Lightning Network itself, nor a call for all nodes to share fee accrual data. Nodes will elect for themselves whether or not to share data, and most will likely choose not to do so. The formula is merely a suggestion for developers trying to capture the economics of payment routing.

The Time Value Layer

The Lightning Network sets up a framework from which we can calculate the time value of bitcoin. Interest rate calculations must have three known inputs: principal, income, and time. In Lightning terms, a node opens channels with other nodes and broadcasts the channel opening, essentially locking up principal for a predetermined amount of time. Assuming incoming channels are also opened to the node, the node is now positioned to route payments and charge fees for doing so.

These routing fees can be considered income. The ending calculation can be expressed in many ways, but through time node participants will elect standards around which to coalesce. This proposal is a starting place for the discussion around these standards. If multiple standards emerge, I would view this as a positive development because competing calculation standards would foster deeper study of Lightning Network routing economics.

Lightning Network is also an optionality layer. Optionality is relevant to Lightning because it serves to offset one of the primary risks undertaken by Lightning node operators: malicious counterparty risk. Nodes carry the risk of their channel counterparts broadcasting a previous channel state, but this risk is theoretically negated by embedded call options which become executable upon malicious activity. The settlement optionality simultaneously serves as a security enforcement mechanism and a velocity accelerant.

Proposal #1: Node Accrual Rate

I propose the idea of a Node Accrual Rate (NAR) for individual Lightning nodes that desire a standardized method for calculating their realized interest rates. Nodes should be able to automatically calculate their rate of return on capital allocated to facilitate Lightning Network payment routing. Rates can be calculated by querying observable data available in their lnd, c-lightning, or Eclair clients. The following is a proposal for one way to calculate the rate using a generic formula for compounding interest and adapting for block time. The node data can be sliced and diced dozens of logical ways, and I look forward to many counterproposals that are sure to include innovative ways to capture return data.

NAR = [(p+f)/p]^(52,560/n)-1

Let *n* = the measurement period, expressed in number of blocks, suggested minimum value of 100

Let *p* = node's average balance held in channels over the measurement period, expressed in satoshis

Let *f* = total routing fees earned by the node over the measurement period, expressed in satoshis

52,560 is the approximate number of blocks per year to normalize NAR as an annualized rate

n:

The suggested 100 block minimum measurement period is arbitrary but matches the minimum block time before mining rewards become spendable. Said another way, your Lightning node should be active a certain number of blocks in order to reasonably measure an annualized rate of return. I believe this minimum can be

increased to cover at least one full difficulty adjustment period of 2,016 blocks once routing activity becomes more commonplace. A longer minimum measurement period would make for higher quality and less noisy data.

p:

The average balance of a node throughout time can be measured a multitude of ways. Striking channel balances upon each new block confirmation and then averaging these amounts over the measurement period could be a clean and impartial way to determine *p*.

f:

Lightning Network node operators are already sharing *f* with each other. I've seen numerous " *day_fee_sum"_screenshots on Twitter with positive integers next to them. Accelerated adoption of the Lightning Network over the past few months brought time value to bitcoin in a trustless way, and nodes are earning sats as a result. Node operators already sharing _f* with each other will soon be calculating and sharing their NARs as well.

Proposal #2: Disclosure of NARs

Lightning node operators currently volunteer information about collecting routing fees, managing payment channels, and other emergent routing techniques. In a similar way, I anticipate and strongly encourage nodes to volunteer their NARs. Sharing NAR data is an easy way to display profitability to other capital market participants. The exchange of profitability information is a foundational tenant of capital markets; the widespread exchange of NAR data between nodes would accordingly bring long term health to bitcoin's capital market. Node operators are already disclosing the small amount of sats they've earned by routing payments through the Lightning Network, leading me to believe that such NAR exchanges will be commonplace for nodes motivated by profit or by transparency. Some nodes will look to attract capital in order to leverage their newfound skill set, even though most nodes will not be motivated to share data. Some nodes will be dishonest about their NAR, and the market will have to identify fraudulent disclosures just as forensic accountants dissect every disclosure from publicly traded corporations.

Advertising profitability, even if unaudited, will attract capital looking for return. Example: a Lightning node with sufficient capital and well positioned inbound and outbound payment channels earns a NAR (annualized return) of 0.25%. Funded with 10 million sats (0.1 bitcoin/ ~ $400), the node earns about 957 sats (~ $0.04) in one difficulty adjustment period (2,016 blocks/ ~ 2 weeks). The implications of being able to earn sats without relinquishing control of private keys is truly a monumental arrival for bitcoin in capital market terms, no matter how tiny the amount of interest may seem.

The node operator can choose to leverage its profitability by advertising a historical rate of return. The node from the example promises depositors a rate of return of 0.15% because a 0.25% return on routing would ensure a positive profit margin. The investor takes counterparty risk because the node could instantaneously exit scam with the depositor's money or simply fail to deliver on its promise to pay a rate of 0.15% on invested capital. The node, however, is instead motivated by creating a strong reputation as a counterparty and repays all depositors the promised rate to establish creditworthiness and increase the potential for additional deposits. The routing income accrues to the node in a trustless way, but the depository relationships occur entirely off-chain in trusted counterparty situations. The bitcoin era Lightning Network bank, without barrier to entry, available to anybody with the appropriate hardware and software, has arrived. Many will route, profit, succeed, raise deposits, fail, mislead, overpromise, and default, all essential components to a healthy and functioning capital market.

Proposal #3: Lightning Network Reference Rate

Lightning Network transitions bitcoin to a more capital market oriented asset. Hashed Timelock Contracts (HTLCs) combine some of the protocol's most powerful features into a standardized financial agreement with defined optionality and expiry, allowing participants in the Lightning Network confidence to transact bitcoin without the burden of continuously auditing individual clauses. In theory, the HTLCs in Lightning Network provide bitcoin with its own native risk-free asset, which is a theoretical term in traditional finance used to describe the asset bearing the lowest possible risk within an investment universe. The US Treasury's obligations carry this label in US Dollar capital markets, and like bitcoin held in Lightning payment channels, have materially less risk than other counterparties. Bitcoin held in Lightning payment channels should serve as a low-risk alternative to off-chain lending and can be used as a reference transaction by which to measure risk premium.

If Lightning node operators around the world disclosed enough NAR data to establish a statistically significant average, this average rate could serve the purpose of offering the bitcoin capital market an accurate measure of low-risk time value. Example: hundreds of nodes disclose NARs, and a cluster of rates is observed around 0.18%. The rate can be a cluster, average, or median of publicly disclosed NARs taken each block or daily, and the end result would be a reference rate widely disseminated to all Lightning Network participants. The Lightning Network Reference Rate (LNRR) can be a very powerful signal that bitcoin has a native time value, a rate that risky off-chain lending should theoretically exceed. If LNRR is equal to 0.18%, an exchange offering 6% on deposits is actually offering a rate of LNRR+5.82%. LNRR represents the time value of the transaction and 5.82% represents its risk premium.

Investors can lend money to the US Treasury at 2.5%, or they can lend to investment grade (IG) corporations at Treasuries plus 1% or junk grade (HY) corporations at Treasuries plus 4%. Investors don't look at the IG and HY companies as investment opportunities yielding 3.5% and 6.5%; they strip away the Treasury component (time value of the US Dollar) to determine relative value between credit spreads. The Lightning Network Reference Rate can and should serve a similar function in bitcoin capital markets. Exchanges wouldn't be offering deposit rates at 6% or 8.5% but instead at LNRR+5.82% or LNRR+8.32%.

Reserve Currencies

Reserve currencies need deep and liquid capital markets. Investments denominated in bitcoin exist only on a small scale, largely because bitcoin is still mostly a commodity and costs resources to store and use as opposed to other assets that accrue positive time value. Lightning Network officially switches the equation for bitcoin but is still a nascent technology. For bitcoin to continue its journey toward becoming a world reserve currency, theoretical financial frameworks such as time value, risk premium, and optionality have to evolve but without relying too heavily on legacy ideas and ideals. The primary reason for this proposal is to offer an opportunity for bitcoin to capture relevant characteristics from traditional capital markets and transform them into native and emergent bitcoin financial theory.

Further Reading

This is the fourth and final article in the series titled The Lightning Network Reference Rate. Please check out Part 1, "The Bitcoin Second Layer," Part 2, "The Time Value of Bitcoin," and Part 3, "The Bitcoin Risk Spectrum."

Follow me on Twitter at https://twitter.com/timevalueofbtc

Bitcoin Mining Explained in 15 Tweets

By Yan Pritzker

Posted March 14, 2019

A Tweetstorm Series featuring Yan Pritzker

Bitcoin Mining Explained. There is lots not covered here, but shooting for an intro rather than deep dive.

1/ Bitcoin is a ledger of accounts where thousands of people have a copy. In order to ensure consistency of the ledger, only one person can write to the ledger at a time.

2/ To ensure only one write, we implement a lottery system. The lottery will allow the winner to write to the ledger. It will also reward the winner with newly created Bitcoin. This is how we make Bitcoin distribution "fair".

3/ A lottery system needs tickets, but we can't trust anyone to sell tickets. Instead, players must burn energy to buy the tickets. Each ticket costs a certain amount of electricity. Electricity costs money because of 1st law of thermodynamics.

4/ Each ticket consists of a run of a "hashing algorithm." This is a piece of code that takes data and creates a fingerprint of that data. The number of possible fingerprints is roughly 2^{256}, or about the number of atoms in the universe. We can visualize it as a number line.
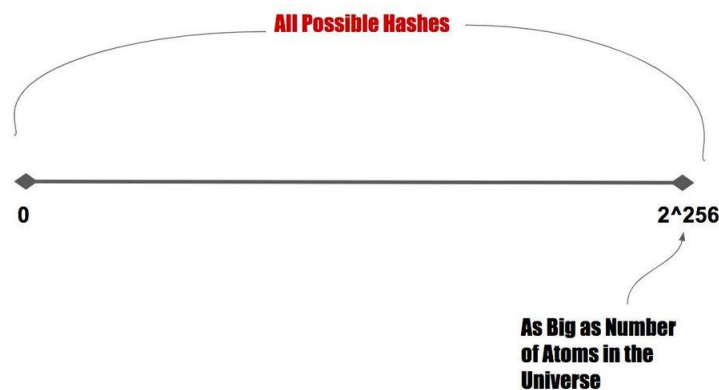
5/ To generate a ticket, you take the payments that everyone wants to make (the transactions), you add a random number, and you produce this "hash". The hash is a number between 0 and the number of atoms in the universe and lands somewhere on this number line.

6/ Ahead of time, everyone has agreed that in order to win, you have to find a hash that's under a specific Target Number. Let's say that number is 100,000,000,000.

That means every time you roll your random generator, you have to land in a tiny space on this number line to win.

All Possible Hashes

Winning Hashes

0   2^256

Target Number 100,000,000,000

As Big as Number of Atoms in the Universe
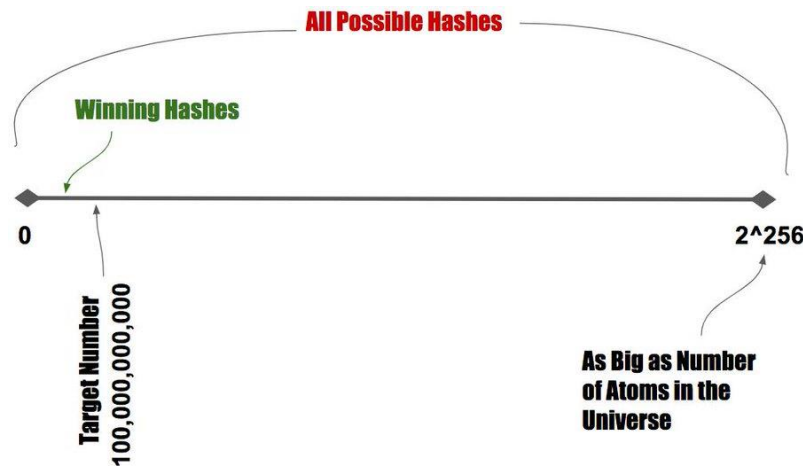
7/Most of the time, you miss. Roughly once every 10 minutes somewhere in the world, someone hits a number that's lower than the Target Number and wins the Block Reward of newly minted Bitcoin. In order to win, they present to the network all the data they used to get the hash.

8/ Since the chances of hitting that tiny space are very very small, by proving that they generated such a number, they are proving that they've done the work of burning a certain amount of energy.

9/But if more people start mining, doesn't that increase the chances that we'd find a winning number more frequently? Yes! So, every 2016 blocks, every node checks for how often blocks have been coming and adjust the Target Number proportionally.

10/ If blocks came too fast, the Target is decreased, making it less likely to hit the Target, meaning you have to spend more energy to find a winning combination.

All Possible Hashes

Less Winning Hashes Harder To Mine

0   2^256

Target Number 100,000

As Big as Number of Atoms in the Universe
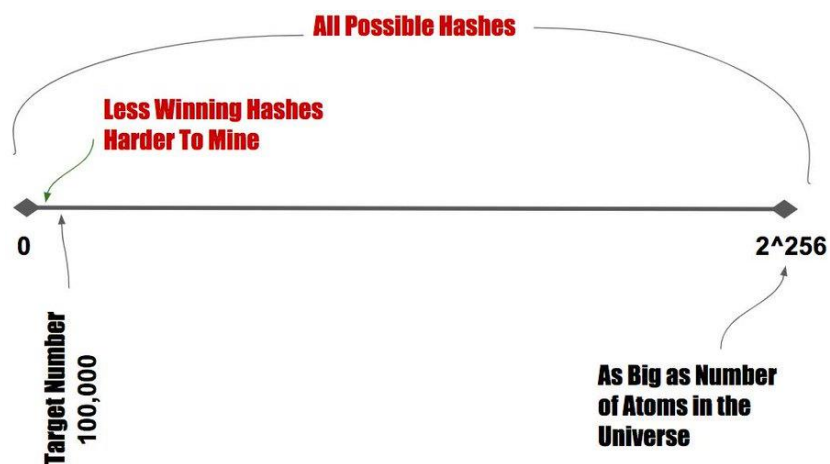
11/ And if blocks are coming too slowly, because too few miners are active, then we can increase the Target, making it more likely that you'd hit the Target with fewer rolls of the die, and thus more profitable. This will attract more miners.
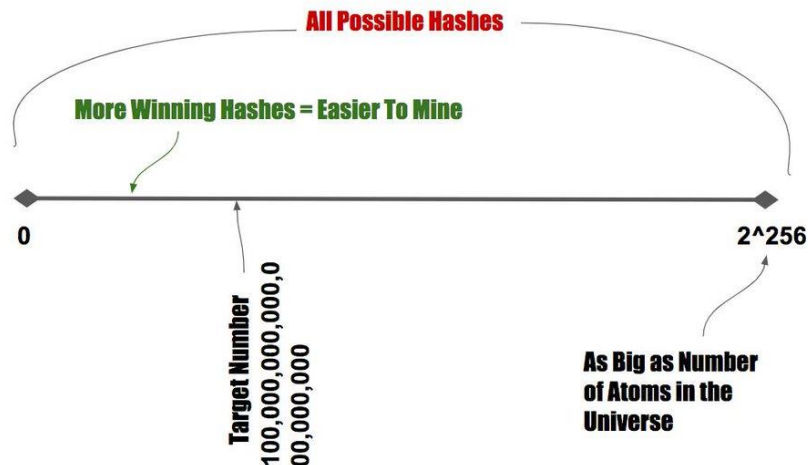
12/ The data that produces the hash consists basically of the transactions we want to write to the ledger, the hash of the prior block, and a random number. This connects every found block to the prior block, ensuring a consistent chain of history.

13/ A large amount of energy goes into mining each block, and the block's hash acts as a fingerprint on the data that's in the block. If someone wants to modify an old record in the Bitcoin ledger, they have to re-mine that block by producing a new hash. This is very expensive!

14/ If they try to tamper with an old block, that block's hash will change. But because every subsequent block used that block's hash as part of its hash, then every subsequent block will change too. That means you have to re-mine the entire chain from the point of tampering.

15/ This makes it extremely expensive to change the Bitcoin ledger. You would have to spend as much energy as the entire honest mining network.

Fin. If you found this insightful, I would appreciate a retweet of the first tweet in this thread.

Could Bitcoin fix the stagnant political and economic landscape?

By <u>Genesis Node</u>

Posted February 15, 2019

Photo by <u>André François McKenzie</u> on <u>Unsplash</u>

This article presents a view that modern politics is ineffective and largely hamstrung due to the underpinning economic system that a political party inherits when they take office. Capitalism is not the issue, it is the form of capitalism employed today and for over 100 years that has led us to a political and economic precipice. A return to a sound monetary system based on Gold or Bitcoin could redress the balance as it did for Britain post the Napoleonic wars when the nation was saddled with debt but transformed into the great economic powerhouse many still think of it as today…times may have changed, the rules of sound money and economic growth have not.

Part 1: Bitcoin is changing the world

Part 2: Politics isn't working

Part 3: Economics is broken…long live economics

Part 4: Can Bitcoin fix Politics and economics?

Part 1: Bitcoin is changing the world…

Bitcoin is the single greatest disruptive innovation the world has seen since the internet and could transform the lives of individuals and nations that adopt it for use as their primary means of value exchange. Bitcoin can most easily be thought of as 'digital gold' and to a growing chorus around the world, is seen as the first truly digital currency that satisfies the key components of money: a medium of exchange, store of value and unit of account. Some would argue that it is too young (only 10 years old) and too volatile ($1k in Dec 2016, $19k in Dec 2017, $3k in Jan 2019) to fulfil the 'store of value' and unit of account narrative. However these detractors are

missing the point, Bitcoin is an emergent form of money which at the extreme end of the scale could very well consume the entire monetary supply of the world extending across all existing currencies, monetary metals such as Gold, Silver and Copper and other more obscure forms of wealth storage such as real estate, art and even classic cars.

Photo by [Dmitry Moraine](#) on [Unsplash](#)

Bitcoin is young and needs time to mature, time to grow and time for the world to catch up and understand its real value, it is far too early to judge this crawling toddler on its ability to sprint at the Olympic final. Over time the open source Bitcoin software code will be improved by developers and computer scientists to solve some of its current perceived challenges (not all involved agree there are challenges that need to be overcome) such as the fact that it is not suited for micro-transactions like coffee and sandwich purchases and that it is the most transparent form of value transfer in the world. It is possible to 'hide' your identity using Bitcoin but the transaction can be traced with ease and Danish prosecutors successfully deployed blockchain forensic capabilities to arrest criminals in 2017 based on their use of the digital currency in illegal activities. So as we see the Bitcoin software add new features such as privacy to protect the information, account balance and activity of a user, ensure transactions cannot be traced, and increase the scalability to make it better suited for micro-purchases to fulfil the role that legacy networks such as Visa and MasterCard play today we will see it gain greater perceived value and utility.

Photo by [Rodion Kutsaev](#) on [Unsplash](#)

The user experience and 'on-boarding' of individuals is still a challenge and is one akin to the switch from paper money and cheques to using plastic cards, chip and pin systems and online banking. When onboarding issues are addressed and customer experiences become as seamless as tap and pay and 1-click eCommerce buying we will gradually see the world shift to using Bitcoin instead of paper money (tap and pay and PayPal are simply digital versions of paper money) and eventually institutional and government adoption will arrive—for context the Bitcoin and distributed ledger technology sector is probably where the internet and eCommerce was in the early 1990s. Some people argue that currency is already 'digital' so there's no need for Bitcoin. They are half right, systems like PayPal, online banking and tap and pay are all integrated into the existing banking infrastructure which is controlled by centralised authorities such as banks and governments with the power to stop or limit transactions and/or inflate the currency supply. The fact that governments and central banks effectively impose the use of their printed paper (and digital forms of it) money does not mean that the currency actually has any value—the link of paper money having real value ended when the gold standard finally ended in 1971 and the world moved to adopt a government issued paper money (fiat currency) that is still in place today. Bitcoin represents a break from this system as it is not owned or created by a central authority, it is an open source, permissionless, peer to peer software protocol that is backed by the laws of mathematics. There is no longer a need to trust a government to undertake responsible economic behaviour that erodes the wealth of savers, risks hyperinflation and as Bitcoin matures to become a less volatile and more reliable store of value the final stage for it to become a universally recognised and accepted unit of account will be challenged by all governments in the world as it reduces their power and ability to control the people.

Why is this important?

Photo by [Kristina V](#) on [Unsplash](#)

Bitcoin offers the world an opportunity to move to a more sound monetary basis, one that is not controlled and dictated by Central Banks and Governments and one which more closely fits the principles of Austrian Economics and is closer to a gold standard model that will allow growth and economic prosperity where there is genuine competition and international trade rather than the existing world of artificial credit creation and money printing which is heading towards an economic disaster as we approach the event horizon. As soon as the mainstream media starts writing about the benefits of 'helicopter money' and negative interest rates and how they will stimulate the economy and bring back growth and prosperity then that is the signal that the end is near…time to stockpile tinned food and hide in the woods. As for banks such as JP Morgan deploying their own 'cryptocurrency'…the media analysis, understanding and reporting on the entire crypto and distributed ledger technology space is spectacularly appalling and ill-informed.

Bitcoin is economic sovereignty, the world needs it now more than ever and there really is no competition.

Part 2: Politics isn't working…

Photo by [Eva Dang](...) on [Unsplash](...)

The effectiveness of policymakers to effect change is growing increasingly stagnant and all across the political spectrum there seems to be a general sense of dissatisfaction and an emergent notion that we have arrived at a stalemate in the current political context. Left, Right, Centre....none of it seems to have the impact it once did and the feeling is one of foreboding dread that we are simply rearranging the deckchairs on a sinking ship. One of the root causes could very well be the fact that all policies are affected by, and implemented using the same broken underlying economic principles that will at some point come crashing down around us...and our politicians are not talking about it anywhere near enough because to engage in the discourse is complex, arduous and unlikely to win any votes. This is not a challenge to the notion of capitalism, rather it is the fact that our current form of capitalism isn't working and has left us trapped in a period of low interest rates, anaemic growth and high debt.

Photo by Ruth Enyedi on Unsplash

Whether a particular political party promising *'free healthcare for all'* and an *'increase to the social welfare budget'* or another proposing *'huge capital infrastructure investments to spread wealth around the country'* and an *'increase to the basic living wage allowance'* the net effect is the same—greater debt funded by unconstrained monetary policies which erode the purchasing power of the individual and increase the national debt burden on a massive scale. Whichever political party may be in power is now irrelevant and any changes pushed through are likely to be superficial and short lived in benefit as the incumbent party will simply be contributing to the increasing debt pile and doing nowhere near enough to change the underlying issues of a flawed and broken socio-economic system. Unless there is a total global reset where all public debt is wiped out then it simply must be repaid and it is folly to assume that expansionary monetary policies could continue to provide a solution without creating other indirect issues in society. These issues eventually bubble up via political divisions and rivalries with one faction blaming the other for perceived inequalities and mistreatment at the expense of the other whilst the one common cause of global disparity in living standards, growing rich/poor divides and overall instability sits back, watches, creates a narrative to apportion blame to a particular sector(s) within society and enjoys the inevitable state aid funded via the monetary

printing presses to temporarily fix the symptoms rather than the root cause at the expense of long term damage to everyone else.
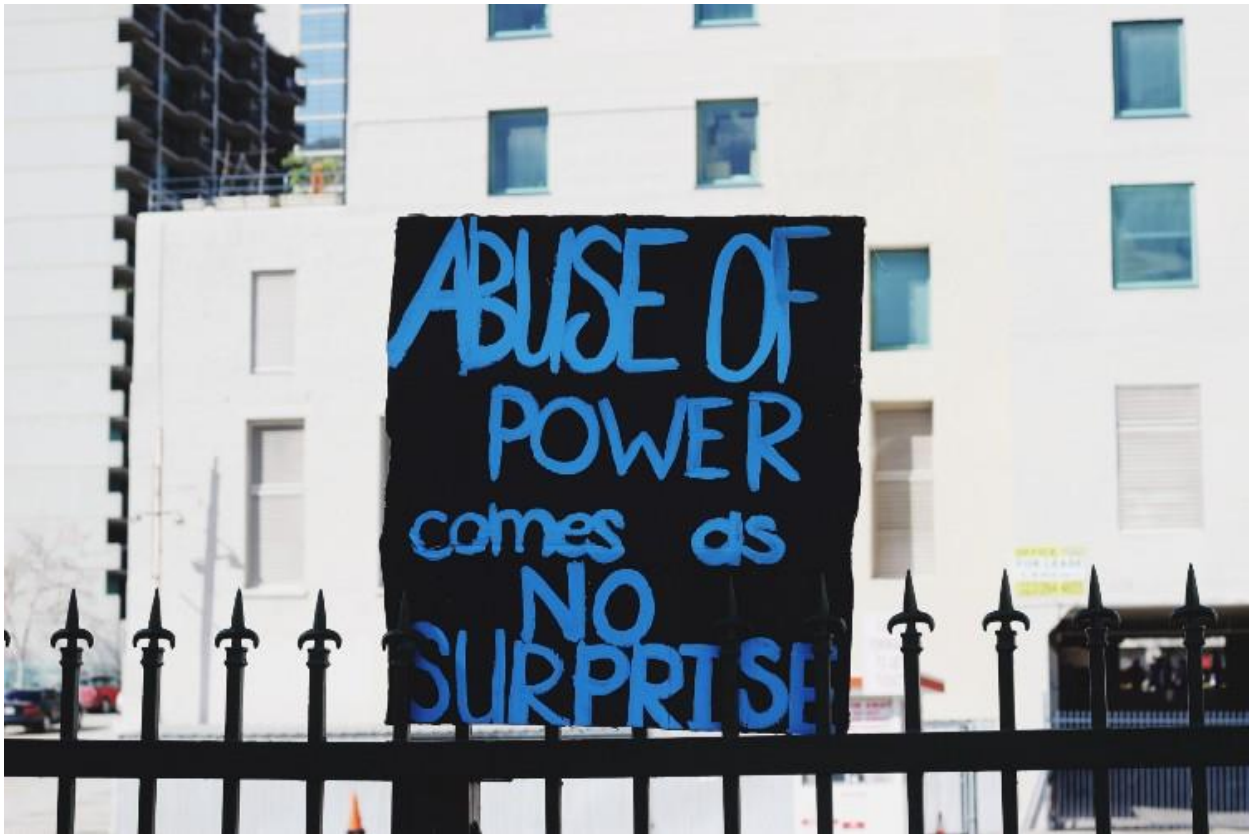
Photo by [Samantha Sophia](#) on [Unsplash](#)

Are the politicians themselves to blame? Maybe, but the sad fact is that they are probably well meaning idealists that are either unaware of the root causes of the political and economic malaise the world is in or they are so entrenched in the nature of their current reality that they are afraid of asking deep, difficult and complex questions about the effectiveness of their own policies and the foundation upon which they sit. For them it is probably better to use catchphrases and capture popular sentiment to win votes than to tell a difficult truth and expose peers, sponsors and face private sector funding cuts. In a short term cycle of government power (every 4 years in the UK) it is more effective to accuse the other of financial mismanagement and point the finger of blame whilst promising 'real change for the people' rather than working collaboratively across parties to correct the course of a ship that has sailed far off course over the last 100 years since the first break with the gold standard and the era of government money began.

Part 3: Economics is broken...long live economics...

Photo by [Randy Colas](#) on [Unsplash](#)

At the root of these issues is the basic belief that Keynesian economic policies, government spending and central planning are the most effective mechanisms of economic management. If implemented with trust and discipline, these doctrines could possibly have led the world to a more sustainable position than we find it in today however the temptation for governments and central banks to print money and expand the economy without a sound basis such as a gold standard has proven too tempting and with long lasting negative impacts for the world. Central banks and central planning authorities such as the International Monetary Fund, European Central Bank, Bank for International Settlements, Federal Reserve, Bank of England, Bank of Japan and the Peoples Bank of China (amongst others) seek to balance the trade and economies of the world through complex statistical models that have created an enormous drain of capital, brain power and research that could have gone to better use and arguably they have done little to improve society aside from adding mountains of debt and complexity.

Since the start of World War One we have seen a succession of governments around the world realise that if they move away from sound monetary principles such as was in place under the gold standard and implement a 'fiat' (government dictated money) currency that they fully control then they award themselves almost

limitless power and resources—but in return they promise to the citizens not to print too much money to avoid an inflationary crisis. If they manage that with central planning authorities in place then in effect they can continue the illusion that a growing economy requires 'expansionary monetary policy' to accommodate it and that they are engaging in policies that support economic growth and an improvement in living standards. The trouble there however is that the level of debt we now find ourselves in the world over is at an almost unsustainable level.

The previous levers that were used to inject momentum into failing economies no longer work as effectively as they once did because:

1. **Interest rates are near zero** and can't be cut much further to stimulate growth
2. **Government bond purchases**by central banks **exacerbate the debt problem**
3. **Devaluation of a currency can spark a trade war** and an escalation in international political tension

In summary, the global financial armoury is severely depleted.

Photo by Imelda on Unsplash

The recent social media fad of a *#10yearchallenge* doesn't look too good for the UK with a Debt to GDP ratio in 2008 of 49% and a 2018 ratio of 89% , the USA moving over the same period from 68% to 105%, Greece from 105% to 180% and Japan in 2019 at over 250% one could ask where this all ends and how it could possibly be sustainable. The current disillusion and unrest across the Eurozone area is an interesting analysis here and is not something that should be ignored because it can, to a large extent be laid at the feet of the failed Euro currency experiment and central planners attempting to control the fiscal policies of nation states that are simply too distinct and too different to operate under a centralised model.

Photo by NeONBRAND on Unsplash

In his recent book, 'Euro Tragedy: A drama in nine acts' Ashoka Mody, ex-Assistant Director at the IMF outlines the core principle behind the flaw of the Euro currency, *"the core flaw is very simple. That a single currency means a single monetary policy. The very diverse economies that are sharing a single currency, they have the same monetary policy. That monetary policy is likely to be too tight for the countries that are economically weak. That monetary policy is likely to be too loose for countries that are strong. And so, the weak country will be further handicapped by a tight monetary policy, the strong country will benefit". Mr Mody goes on further to state that, "there's no question that the euro was a bad idea in every way. It was bad economics, it was bad politics. And the only thing we can say for it today is that perhaps the cost of breaking it up would be so great that we need to try to hold it together. There will always be an inherent tendency in the euro system to pretend that a crisis does not exist, so to first deny it, then delay the response, and the denials and delays will cause the crisis to fester, and become worse. The original economic wound will leave scars. Over time, these scars, through successive crisis, will continue to build, the social and political fabric of Europe will continue to be undermined. And that, I think, will eventually end in a way that could make everybody very unhappy."*

So what can be done to fix all of these issues?

Photo by Cole Keister on Unsplash

For starters the mainstream and commonly accepted view that Keynesian economics and the belief that government spending stimulates an economy needs to be challenged and a more moderate discourse needs to be evaluated and given prominence in Universities, governments, institutions and central banks around the world—whether there is merit in continuing to pursue a centrally planned, Keynesian economic doctrine is to be determined. The Austrian model of economics purports that a free market system based on sound monetary principles would present a truer and more responsible approach to money, finance and economics. Perhaps a new blend of Austrian and Keynesian principles could emerge so that fractional reserve banking (banks lending out more money than they have in deposits) either stops or is severely reigned in, government spending is limited, debt levels are reduced and the easy money principles that cause debt mountains, encourage high risk investments and moral hazard dilemmas that are facilitated by central banks are put to an end.

Photo by Rick Tap on Unsplash

Nomi Prins, ex-Wall Street Executive turned author discusses the impact of global central banking and easy money policies in her book 'Collusion: How Central Bankers rigged the world' and writing for ' *Le Monde diplomatique*' in December 2018 she concluded that, *"The financial crisis of 2008 initially fostered a policy of bailing out banks with cheap money that went not into Main Street economies but into markets enriching the few. As a result, large numbers of people increasingly felt that they were being left behind and so turned against their leaders and sometimes each other as well. This situation was then exploited by a set of self-appointed politicians of the people, including a billionaire TV personality who capitalized on an increasingly widespread fear of a future at risk. Their promises of economic prosperity were wrapped in populist platitudes, normally (but not always) of a right-wing sort. Lost in this shift away from previously dominant political parties and the systems that went with them was a true form of populism, which would genuinely put the needs of the majority of people over the elite few, build real things including infrastructure, foster organic wealth distribution, and stabilize economies above financial markets. In the meantime, what we have is, of course, a recipe for an increasingly unstable and vicious world."*

Part 4: Can Bitcoin fix Politics and economics?

Photo by Marvin Meyer on Unsplash

How then could Bitcoin possibly fit into all of this and make a difference? For most people, Bitcoin is a magic internet money that should be dismissed as a result of its

alleged links to organised crime, money laundering and drugs. The sad truth is that the media coverage and the global understanding of what Bitcoin represents is woeful and the international currency of choice for any kind of criminal activity is the US Dollar with most major banks in the world being accused of some form of fraud, money laundering and criminal activity over the last 10 years—just last year there was an estimated $3 Trillion of money laundered through the existing banking system.

Photo by [Dmitry Moraine](#) on [Unsplash](#)

In a nutshell Bitcoin is the most effective form of money the world has ever seen and will change the world of money and finance as we know it as the possibility of circumventing the existing system and authorities to store, transact and transfer value globally now exists. Bitcoin is verifiable, portable, fungible, durable, divisible, scarce, censorship resistant and has an unforgeable costliness to produce and create as a result of the complex 'mining' required to produce new supply, verify transactions and secure the network — it cannot simply be created by a central authority unlike paper money today. After 10 years of life Bitcoin has never been hacked and the 'Lindy effect' outlines that every moment that goes by when Bitcoin exists further reinforces its value and implies a longer remaining life expectancy — the energy and computing power required to compromise the Bitcoin network would require a number of nation states to cooperate with little potential benefit at the end as the network would simply 'fork' away from the compromised chain of transaction records, rendering the hack costly and of little value to the agitator. Critics of Bitcoin, including the BIS in a recent publication, argue that it is too energy intensive to be useful however again, they are missing the point, the 'unforgeable costliness' of mining and securing the network ensures the system is safe and that it cannot be hacked by malicious actors.

Only 21 million Bitcoins can ever exist, circa 17m currently exist and it will take until c2140 for the full supply to be released into society — this is true monetary 'hardness' and scarcity of supply as opposed to 'soft' fiat government money that can be either printed at will in whatever quantity is required or injected digitally at next to zero cost to 'stimulate economic growth' — but the basic rules of supply and demand dictate that the higher the supply the lower the price of a good. The ability to safely and securely use the Bitcoin network to send almost unlimited value around the world within hours is truly transformational and its uncensorable nature means that it can be used as a medium of exchange in countries where government money has failed such as Venezuela or Zimbabwe and with others such as Argentina, Pakistan and Turkey staring into the monetary abyss (Italy and Greece aren't far behind either) there may yet be more countries who wilfully adopt Bitcoin as their primary medium of exchange.

Photo by [Rod Long](#) on [Unsplash](#)

The exchange of 'money' for goods and services is an act that has been going on since the earliest days of humanity and for the first time, Bitcoin offers a near perfect solution. The open source software probably needs to be improved to accommodate micro-purchases and operate as a high speed transaction network at scale such as Visa and there is probably merit in implementing privacy as it is at present, the most traceable and most transparent payment mechanism the world has ever known—you don't really want the coffee shop owner to have the ability to check how much value is in the account you just paid them from and all the other transactions you have ever undertaken using that account which is the case with Bitcoin today. The best way to think of Bitcoin is as digital gold with the scale of wealth it can transfer being more akin to a huge container ship transporting goods across oceans rather than the final mile postman delivering packages and letters.

So could Bitcoin really fix the stagnant political and economic landscape?

Whilst it would be great to give a resounding 'yes' to this question the reality is much more opaque and complex. For Bitcoin to have a real impact on a mass scale it requires adoption, mass adoption could drive wholesale change at a national level and that in turn could lead to a nation state (possibly more than one) choosing to move towards a more sound version of money and economic principles with Bitcoin as the primary medium of exchange—it will not be an easy or painless journey but long term would help restore an order of capitalism, competition and market forces that is a true reflection of the value of labour outputs of a nation.

*Photo by [Randy Colas](#) on [Unsplash](#)*

Instead, the best question to ask yourself is what you know about the root cause of

endemic failures in the economic system that invisibly governs the whole world and causes so much division and divide—the recent Gilet Jaunes protests in France are a good indication of the deepening divisions and disillusions with the current system and ruling classes. Any political party that proposes a root and branch review and change of the economic systems that have been in place for almost 100 years and challenges the need for fiat currency will not however garner mass support or win enough votes to take office. So unless a government with potentially unlimited and unchecked power voluntarily cedes economic control back to the people and starts a slow and painful process of change to improve the lives of its citizens the charade will continue until the entire system collapses and a scapegoat is found. We may yet see both a bottom up approach where the people of a country in strife choose Bitcoin en-masse as their money and medium of exchange and force the hand of their government. We may also see a top down approach of a government that is facing some form of international sanctions and embargoes adopt a new, uncensorable money—Venezuela will be interesting to watch throughout 2019–2021 as the people there are already adopting Bitcoin on a massive scale and with the Bank of England rejecting the recent Venezuelan Government request to repatriate over $1 Billion of their own gold (and for good reason!) then even the government might choose to adopt Bitcoin and rebuild their society on a more sound, sovereign and independent footing.

It is possible that Gold and Bitcoin backed currencies, Austrian economics and a return to more traditional economic values and a free market approach presents a way out of the chaos. Real change in politics around the world needs cross party consensus and commitment that the one thing that unites us all is fixed before we can return to a conversation about Left vs Centre vs Right.

Fin
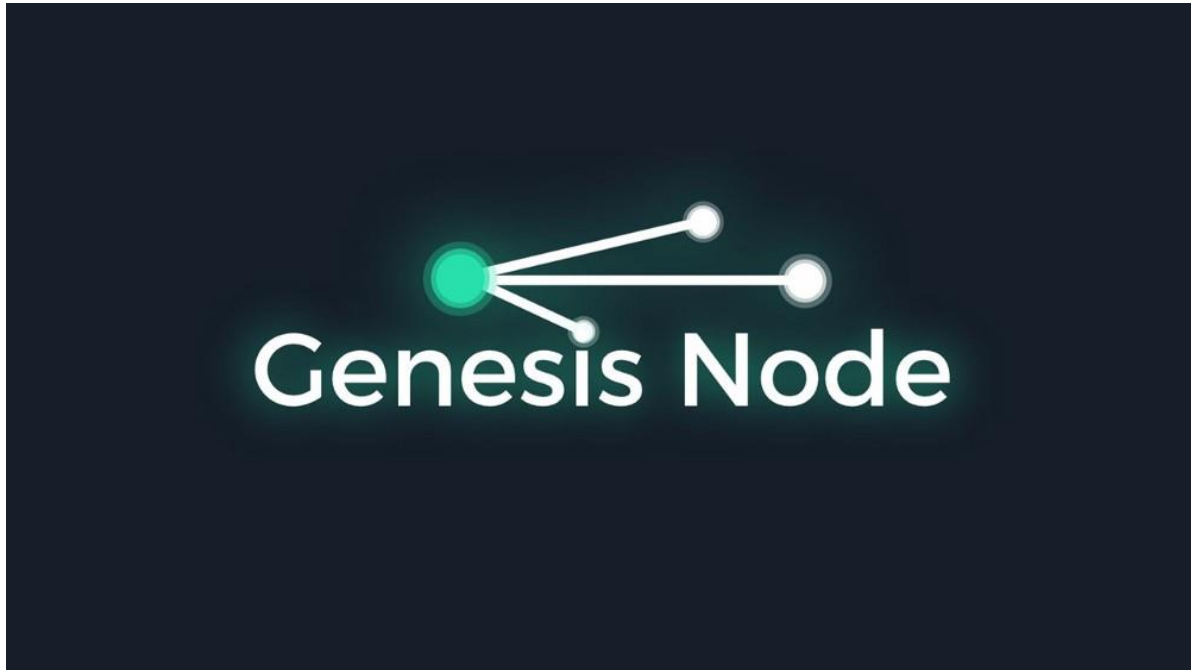
Copyright Genesis Node 2019

Genesis Node is a Bitcoin, cryptocurrency, distributed ledger and decentralised business model training and advisory company and can be found at www.genesis-node.com

References

Photo by [Thomas Kelley](#) on [Unsplash](#)

Referenced articles

Ashoka Mody: https://paw.princeton.edu/podcast/pawcast-ashoka-mody-euros-inherent-flaws

Dan Held : https://medium.com/@danhedl/planting-bitcoin-56bd1459cb23

Max Rangeley: https://www.montpelerin.org/wp-content/uploads/2018/07/Rangeley-Max-The-Emerging-Free-Market-in-Money.pdf

Misir Mahmudov: https://blog.goodaudience.com/bitcoin-winner-takes-most-or-winner-takes-all-c509aebaa19a

Murad Mahmudov: https://blog.usejournal.com/bitcoin-past-and-future-45d92b3180f1

Murad Mahmudov: https://hackernoon.com/the-many-faces-of-bitcoin-1c298570d191

Nic Carter: https://medium.com/@RainDogDance/bitcoin-as-a-novel-market-institution-nic-carter-talk-at-baltic-honeybadger-2018-e085f163b213

Nomi Prins: https://mondediplo.com/openpage/wall-street-banks-and-angry-citizens

Venezuela Gold: https://www.telegraph.co.uk/news/2019/01/28/venezuelas-interim-president-asks-bank-england-stop-nicolas/

Venezuela Bitcoin usage: https://bitcoinist.com/venezuela-bitcoin-trading-giant-high/

Books

Collusion—Nomi Prins

Euro Tragedy—Ashoka Mody

Human Action—Ludwig Von Mises

The Bitcoin Standard—Saifedean Ammous

Why Bitcoin Matters

It's more important than you might think

By Aleksandar Svetski

March 15, 2019

This is the article version of a talk I gave to kick 2019 off for a few Bitcoin meet-ups in and around Australia.

The video version of the article is here, but if you don't want to see my ugly head (nor Jeff's), please continue.

Why Bitcoin Matters...and yes — that's Bezos

Why Bitcoin Matters…and yes — that's Bezos

Thank you Jeff Bezos for the wonderful introduction.

There's a lot more than meets the eye when it comes to Bitcoin, and coming into 2019, I'm glad to see a broader push back toward the Bitcoin narrative, especially after a solid 2yrs of shit-coinery, ICOs, Bcashing, Wrighting, wronging, Verring, blockchaining for the sake of blockchain & whatever other stupidity we saw..

It could be the echo-chamber effect in that I've narrowed my focus; but I'm hopeful that it's something more, and shall err toward that as being the truth.

Either way; I hope this article helps to drive the narrative forward even further, and reinforce why this thing called Bitcoin is so important.

If we're to move toward a society & world that's more functional, where unfair asymmetries & rent seeking are made more difficult and where the labour we transform into some unit of value (that's able to be stored or exchanged) is impossible or at least impractically hard to manipulate or undermine, then we need to take Bitcoin a whole lot more seriously.

There's some further reading and a few reference articles I'll include at the bottom, which should help you get a better grasp of some of the concepts throughout.

Other than that, let's dive in.

The Societal Stack

I'm going to quote myself a few times throughout, because…well why not..

"Nothing great was ever built on shit foundations"

-Aleks Svetski

To understand money & Bitcoin, we need to go back in time and go down what I like to call "the societal stack" (as per my sophisticated diagram below).

It's only when you understand the foundations of what we see around us, that things start to make sense.

"The Societal Stack"

You'll note, we have communication as the lower foundation, or the basis for everything. I like to call it the "Societal Sub-Strata"

Communication is the prerequisite for cooperation, which in turn; is the predicate for society.

Money as a mechanism via which we can exchange, specialise, measure, collaborate, cooperate & organise sits

directly on top.

Everything else, I've called "society" then sits above it.

Let's take a moment to explore. If we look deeper into the "communication layer" we can split it into two, broad categories.

"The (broad) layers of communication"

1) The lower foundation.

This is the biological ability to communicate, and we share this ability with every other species on the planet (at least that we know of). All species communicate…somehow.

2) The upper layer.

This is Homo Sapiens ability to communicate on abstract concepts & ideas. This is *unique to us*, and it's this layer that allows for broad-based coordination.

Yuval Noah Harari, in his seminal book "Sapiens" termed
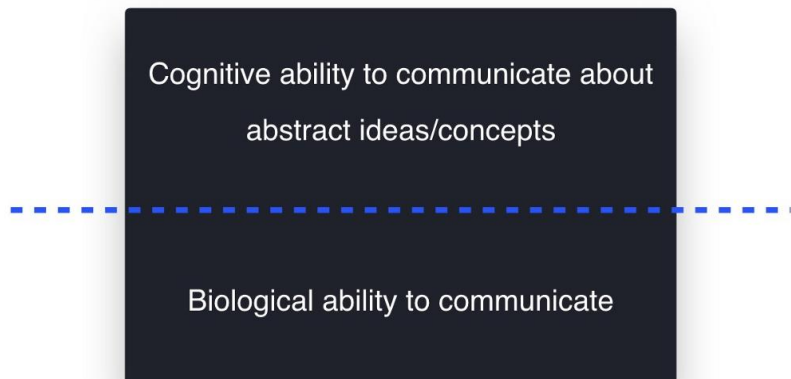
those abstract concepts & ideas; "Shared Fictions", and via that inspiration, I'll quote the following:

In communicating about fantasies/imaginary concepts & fictions, we are able to "hack" our biology & attain the trust required for us to cooperate in numbers that exceed our biological limits.

This is an important thing to understand. Homo sapiens "hacked" trust, and thus became the dominant species on planet earth.

We're the only species able to cooperate both flexibly & in large numbers, and this is all thanks to the stories we tell each other & choose to collectively believe.

This unique function has allowed us to build the complexity in society that we often take for granted today.

It's allowed us to cooperate in numbers that exceed what's called "Dunbar's number".
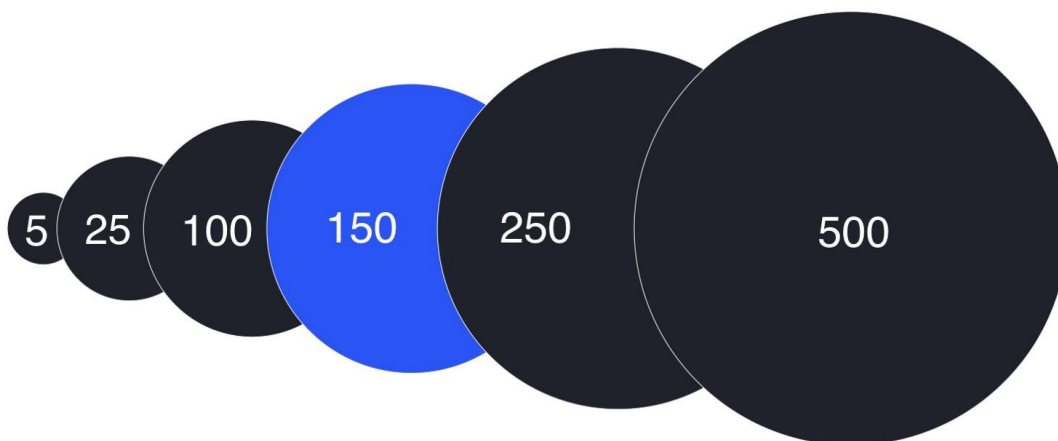
Dunbar's number is a suggested cognitive limit to the number of people with whom one can maintain stable social relationships.

And as a result, we've evolved from some insignificant ape, sitting somewhere in the middle of the food chain, to the apex species, at the top of the food chain, who rule the world & have created what scientists now call the "anthropo-sphere": The layer of the planet planetary ecosystem associated with **us**.

This is an extraordinary feat; made possible (at least as far as we understand) by our ability to hack trust via shared fictions & complex communication.

Now for those of you who think you might not be familiar with any of these so called "shared fictions", here's a few examples; that you've either heard of, buy into daily or live by:

- Gods
- Kings
- Religion
- Corporations
- Laws
- Nations
- Human Rights
- Race

They are all, by definition; fictions.

And what's the most important and long-standing story / shared fiction of all? That's right....

Money

But, before we move onto Money, let's just have a look at that stack again:
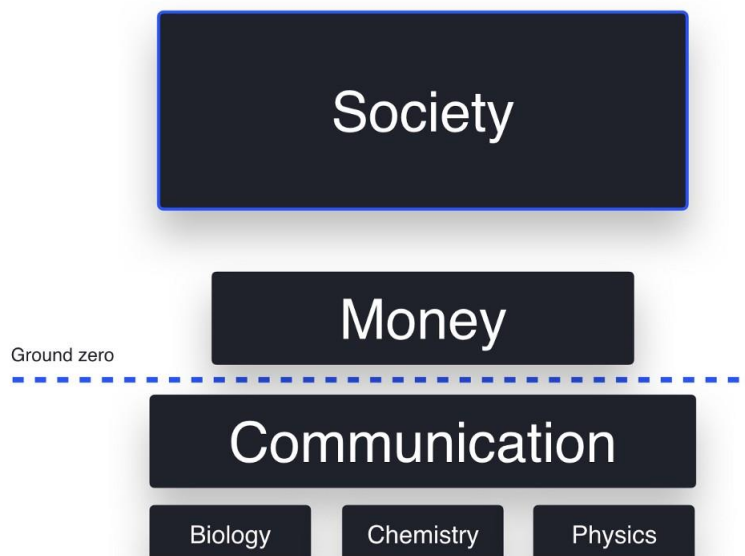
Notice how the further down the stack of society/humanity you go, the more robust it has to be?

Let's take a moment to explore language as a function of communication.

Language

Communication / Language is but a set of rules, that govern how we use our physiology & sounds to convey a message (however complex).

Language is a PROTOCOL (or set of protocols).

We have specific rules for language. Basic ones such as vowels & consonants, through to higher order rules such as grammar, register, punctuation, etc.

You'll note, these rules don't bend & they don't change, yet we are able to create however much complexity in our communication with those fundamental ingredients.

If you screw around with the base layer rules, you're not going to get a "cool variation" on your message, you're going to get a jumbled up line of shit nobody understands!

The more basic & fundamental the rule, the more rigid it must be, and it's this rigidity of ingredients & fundamental rules that gives language its power.

Its strength of foundation has allowed us to build a level of complexity in the world that far exceeds any other species.

Two more things to note:

a) If you go lower than communication, the rules get even stricter. You get into math & the sciences:

- Biology
- Chemistry
- Physics

b) One might say: "well, language does change". And whilst that's true, think about how it happens. Language evolves generationally and involves a form of social consensus driven by people's need to be understood & the adoption of similar language patters for the sake of better communication & exchange.

So yes—Language and it's rules change; but that change is not abrupt. The change is more like an evolution over time, involving broad based consensus amongst the participants involved in using that language.

Sound familiar??

Anyway. Back to Money…

Money

Money is very similar to communication in many ways. Being so fundamental to the stack, it must be sound. It must be rigid. It must be robust.

You can't build monuments on poor foundations.

To truly appreciate this, we'll need to go back to the beginning and explore money's journey & evolution through time.

So where where did Money start?

Money, ledgers & promises.

I also used to believe the earliest form of 'money' was something like Barter—but I'm now convinced I was wrong.

I don't believe barter was ever a functional form of money or value exchange, primarily because it has a combinatorial problem (also known as the lack of coincidence of wants—Saifedean Ammous).

What this means is that if Bob has an apple, and Jim has a shoe, they will be able to trade (albeit the amounts may be difficult to agree on), but what if Jim doesn't want an apple? What if he wants a banana?

Then Bob needs to go find Zoe who has a banana, that wants an apple, swap with Jim so he gets his shoe.

That's just 3 people, and I'm already confused. This gets exponentially more difficult, particularly with increased specialisation and a larger number of participants.

Barter :/

So if it wasn't barter, what did money start as?

Well, believe it or not; the concept of money has its root in "promises". Promises related to some form of labour, work, debt, item (product) or service that participants of a community would keep track to know who did what & who owed what.

And where were these promises kept? On a ledger.

This ledger was viewable, or able to be viewed by everyone, and the people who helped manage it were the first form of book-keepers.

Digging deeper here is outside of the scope of this article, but what's interesting to note is that here we are, tens of thousands of years later, with a digital version of a ledger, made up of 'promises' (txns), that's viewable by anyone, ie; Bitcoin.

LHS image is Satoshi's first iteration ;)

So back to early Money.

Promises & some writing on the wall were great, but we realised that we needed some form of more tangible, transportable, objective representation of money, so we could use it outside of our immediate community.

So naturally, we proceeded to use things of value such as cattle, salt, cotton, etc to represent money—this was commodity money.

As we got smarter, we started to abstract Money further, with objects that had better attributes, had a greater degree of scarcity & that more people could agree on / recognise as Money.

ANCIENT MONEY

>10,000 BCE	9000 BCE	5,000 BCE	2,500 BCE	1,500 BCE
Promises ↓ Ledger	Commodity Money (Cattle, Salt, Sugar, Tobacco, Cotton)	Stage 1 Abstractions (Shells, Rocks, Rai Stones)	Stage 2 Abstractions (Metals, Bronze, Gold, Silver; even knives)	Gold

@getamber.io   amber.app   amberexchange
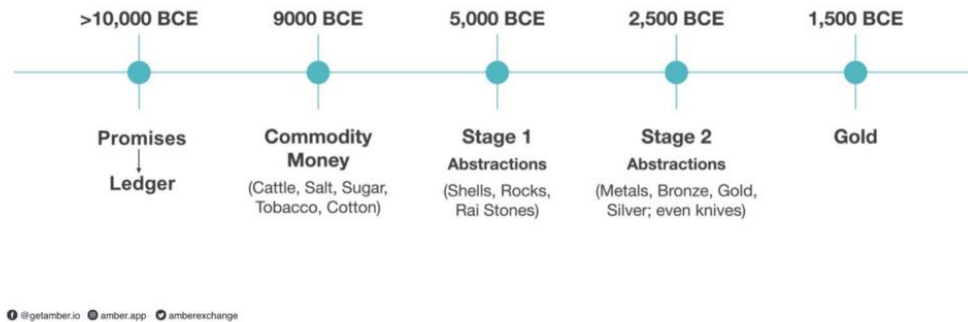
This right here is what fueled the acceleration of the development of society.

Money was the first & still is the most important collaborative technology homo sapiens have created.

Whilst the Ancient forms of money changed everything, they were clunky and difficult to build broad consensus with. So as the ingenious creatures we are, we found ways to abstract it further and thereby create more complexity and specialisation with less friction, all via the creation of "Modern money".

MODERN MONEY

1000 BCE	1500's	1950's	1990's	2000
Coins Ancient > Roman > Medieval	Gold Backed Paper Money	Fiat Paper Money	Plastic Money (Starts with Diners Club, then AMEX)	Digital Money

@getamber.io   amber.app   amberexchange
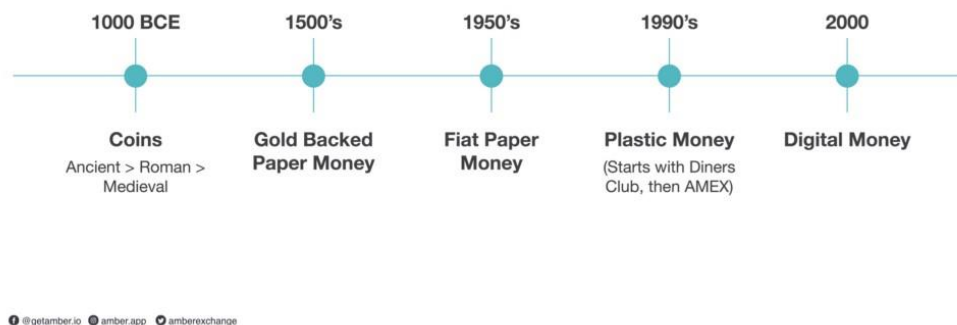
Modern Money = The introduction of "trust" in an intermediary

In broad terms, the element of trust in a third party became an important feature of making Money more physically useful—but somewhere along the line, the core

tenets of Money were either forgotten or conveniently swept under the rug—*and it's this that we need to get back to.*

So let's define it.

What is Money

A friend (Sven) calls it "crystallised energy" or "crystallised life force". And without wanting to sound woo-woo about it; that's exactly what it is!

Money is your labor in a measurable form.

When people tell me something like "Money is the root of all evil", it just shows how little they understand about it. In fact, if you think about it; they're saying that their work, their labour & their effort is evil. Seriously?

It's madness.

I have a saying:

Money is *not* the root of all evil.

Money is the root of all complex cooperation.

So it's time we stop shitting on it & start realising that money as a concept is fundamental to humanity & critical for us as a whole.

We must recognise that the **fiat** form of money we've been sold for the last century is the steaming pile of **shiat** that needs to be transformed.

Defining Money

A definition of Money I like to use is:

Money = A representation/abstraction of "Value"

If we take this definition, we can then extend the functions it should perform, and the attributes a form of Money must have in order to best perform those functions. See below:

MONEY

Definition: Abstraction / Representation of Value

Functions		Attributes	
Store of value		Fungibility	Cognizability
Means of exchange	$	Portability	Divisibility
Unit of Account		Durability	*Scarcity*

@getamber.io amber.app amberexchange   28

The core tenets of Money.

You've probably seen the above in one form or another, but what you may not have seen on the list is the term "Scarcity".

It's the attribute that not enough people talk about, because they don't understand the fundamental predicates for value.

We'll explore scarcity below, but the important take away here is that *these are the core tenets of Money.*

This is what Money must be & do in order to allow us to best collaborate & build complexity without having the entire shared fiction / story fall apart (as it has every time we've strayed away from it).

Scarcity

Why is Scarcity important? In short:

Scarcity is inherently tied to our notion of value.

Furthermore, something that remains scarce, will ensure value is maintained, *across time.*

A few examples will help:

Why does one care about (value) their friends & family so much?

Have you ever heard of the saying:

"You only have one mother / father / brother / sister" ?

Your family members & friends are verifiably scarce, or in other words unique to you. If something happens to one of them and they're gone; you can't get them back and you can't create a duplicate.

We value our loved ones because they're truly unique, and inherently *scarce.*

The same goes for a special trinket handed down to you by your great grandmother. It's rare / scarce / unique.

Now for those of you who are little more sociopathic in nature & don't value your friends / family, then perhaps you get the same feeling with some other item that you can never get another one of.

The same goes for art. We all inherently know why a piece of art goes up in value once the artist dies.

It all comes back to scarcity.

And the most scarce (fungible) resource we know of?

Time.

Time is a little different than the above because those items / people / etc are not fungible. Time is the "gold standard" of a unit or resource that is scarce and fungible, and that we (at least the more intelligent of us) value highly.

As you read this, you may ask how much would you pay, to have more time?

(probably ask yourself the same re: Bitcoin)

So if scarcity is at the core of the idea of "value".

Then for something to maintain "value" (for example a means of exchange, like money), than it must be scarce—else, it does this:

Purchasing Power of the U.S. Dollar (1913-2013)

1913: Federal Reserve is created

1933: FDR's executive order makes it illegal to hold gold coin, bullion or certificates

1944: Bretton Woods established the USD as the world's reserve currency

1971: Nixon closes "gold window," end of Bretton Woods, beginning of the modern-day fiat currency system

Source: U.S. Bureau of Labor Statistics

You've all probably seen this chart, and although it's become a bit of a cliche, it's important to be reminded.

Bitcoin, as far as I can ascertain, is the only fungible unit (other than time) that we can say is truly scarce—which follows that as a "money", it is more sound & will maintain its "store of value" over time.

This is the core of 'store of value', (not the day to day market price in USD as some mathematically inept individuals might tell you).

One final note on scarcity.

Bitcoin is the first time we've had a digital good, that functions like something physical.

And because it's bound my math, it's able to be made truly scarce & verifiably so, whilst maintaining the scalability that only comes with something that is natively digitally.

Digital Scarcity is the innovation. Not: "The Blockchain".

(Thanks Jimmy Song)

Next:

The unit & the Network
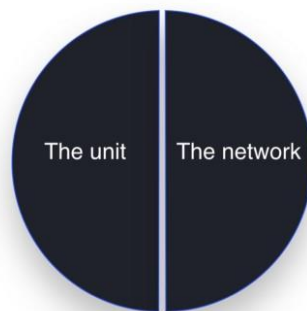
Before we can appreciate what it takes for a modern form of money to perform the functions defined above, and truly embody all those attributes, there are two important factors we need to understand better.

1. The Unit
2. The Network

1. The Unit

Must be

- Impossible / Hard to counterfeit
- Hard to produce (high stock to flow)
- Limited in Supply (harder the limit, the better)

These attributes make money sound, and it's the last one which to date, we as a species have not delivered on.

Why?

Because we're human, and our nature is one that desires more—which is also why the attributes of the unit are best codified & governed by math (not the whim of people).

2a. The Network

The unit must be part of a larger monetary network, and this network must BE:

Must **be resistant to**

• Change
(immutable)

• Shutdown
(robust)

• Censorship
(open, free)

• Manipulation & control
(decentralised)
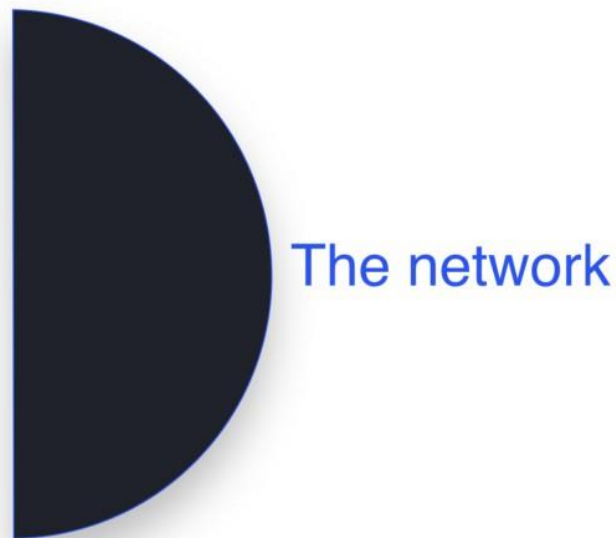
The network

getamber.io   amber.app

- Resistant to change because it Money is fundamental, and you cannot build anything on an ever-changing foundation.
- Resistant to shutdown because if a monetary network is not on, or can easily be shut down; then **everything** stops. This is a big reason why natively digital money has been a challenge.
- Resistant to censorship because similar to language / speech / communication; it's only truly functional when it's free & inclusive. If you try control it, it degrades.
- Resistant to manipulation & control, because it undermines all other attributes.

These are all critical, and non-negotiable for a broadly used monetary network.

2b. Network Functions

The above is what the network must _**be**_. The below is what it must _**do**_.

Must _**do:**_

First Order:

- Send
- Receive
- Store

Higher Order

- Escrow / Multi-party authenticate
- Anchors / Timestamps

The network

getamber.io   amber.app

A monetary network must perform these key functions VERY well, **without compromising on them. Ne** _**ver. Ever. Ever.**_

Money is about confidence.

It's a story / social contract that we broadly agree on and in order for it to function well (particularly when it's digital & ephemeral), it cannot risk failing at it's delivery of the first order functions.

A broadly functional monetary network must optimise for Send, Store, Receive above all else.

It can then also perform higher order functions like:

- Escrow / Multi-party authentication (eg; multisig)
- Anchors / Timestamps (smart contracts like HTLC)

But note that these higher-order functions are a combination or derivative of the first order.

That's it. That's all you need.

Not like these idiots out there trying to build all this complexity into the base layer of their networks, at the expense of the security & robustness of the first order principles!

(Yes Ethereum & every other shitcoin — I'm talking to you)

So to conclude this section:

It's the above attributes of both unit & network that the most fundamental layer of society (money) should have in order to function properly.

So why does Bitcoin Matter?

Well, if you haven't figured it out by now; I'll spell it out to you:

1. *Money is the foundational layer for everything in society.*
2. *Bitcoin is the most organic, stable, powerful form of money the world has ever seen.*

Bitcoin is both the only unit & network that executes on everything I've outlined as fundamentally important about money.

	Fiat	Bitcoin
Impossible to counterfeit	Pretty hard	
Hard to produce		
Limited in supply		
Resistant to change		
Resistant to shutdown	Pretty hard	
Resistant to censorship		
Resistant to manipulation & control		
Send & Receive	Pain in ass > $10k	
Store	Up to 250k	
Programmable		

@getamber.io   amber.app   amberexchange

	Fiat	Bitcoin
Store of value	Decreasing	
Simple means of exchange		
Unit of account/measure of wealth		Got a while to go
Fungibility	Mostly	
Divisibility	Mostly	
Recognizability		
Homogeneity		
Scarcity		

@getamber.io   amber.app   amberexchange

SoV is green because it's green. I'll write something on this in another article

But more importantly than the above, Bitcoin is an opportunity for a new beginning, in a new age.

Here we are today; with an incredible opportunity to not only learn from the mistakes of those who did not adhere to those core tenets, but with a technology that can both embody everything that money should be, and also evolve with society and the market into what it could be.

This is why Bitcoin matters..

Now one might say; what about some other clepto-currency?

My answer: *They don't matter.*

I'll show you why.

Why Bitcoin?

What makes it different?

First of all; it's a monetary phenomenon. Not a technological one. This is where most people get it wrong at the outset.

Most people new to the space, or who just don't understand money, or it's role in society think that Bitcoin is some "payments mechanism" designed to move internet money around the world.

So with that thesis, they set out to do it faster, or perhaps give it more features.

The problem with this approach is that they miss the entire point of what gives Bitcoin its "money-ness" !!

I've put together the following table to hit the key points (although there are many more) with respect to Bitcoin:

Why Bitcoin?

The Recipe	Grassroots growth
No founder / owner	Relentless focus on first-order principles
It's absolute (unit) scarcity	Born of the Internet
Robust, Basic, Adversarial deign + growth = Anti Fragile Network	

@getamber.io   amber.app   amberexchange

1. The Recipe

I call Bitcoin's entire formula, "The Recipe", because the fact that it works is because it combines so many previously disparate disciplines into one, cohesive, robust & functional whole.

The Bitcoin Recipe

Networks	Game Theory & Mechanism Design	Cryptography
Proof of Work / Byzantine Fault Tolerance	Social Engineering / Psychology	Computer Science
Decentralization/ Distributed Computing	Economics Incentive & Disincentives	Data Structure (Blocks of data, cryptographically chained)

@getamber.io   amber.app   amberexchange

Taking one ingredient out of context, does NOT yield the same result.

I've discussed this recipe at length, at a number of talks, and primiarly when I'm explaining why "blockchain" is such a stupidity on its own; or as an entire recipe applied to anything other that something as foundational as Money (as in the case of BTC). You can find me presenting "Blockchain's AOL moment" here:

"Blockchain" is the modern day AoL

2. The Grassroots Growth

Bitcoin was never sold to anyone via an ICO, nor via some VC funded start up, nor for any one person or institution's direct gain.

Bitcoin was adopted by people with a desire to be a part of it, because of what it was & what it represented. An idea. And all support of it in the beginning had a collective impact.

These early supporters and borderline crazy people formed the ever growing "stubborn minority" who form the base of support that Bitcoin has, which no other network in the world has. As Trace Mayer would call them: "the Hodlers of last resort".

You can't replicate this, and no amount of ICO money raised can compete.

This is missionary VS mercenary. They don't stand a chance.

In fact; just as a funny example, we saw EOS (Extremes Of Stupidity) raise $4 BN USD, and they're not only nowhere, but they're now using that money to buy property & land 🤣🤣🤣🤣

3. No founder

This is extremely hard (nigh on impossible) to replicate, and is one of the primary strengths that Bitcoin has.

The fact that it's something which has grown beyond its original founder, has grown as a function of the market, and can now ***not*** have the "head of the snake" cut off makes it incredibly hard to stop.

There's nobody to throw in jail, no corporation to shut down, and nobody to point to as the saviour or messiah (Sorry Roger, we don't need you).

Furthermore, the idea that it could be anyone, is not only functional; but also adds to the myth. The myth adds to the allure, and reinforces Bitcoin as an incredible, once in a lifetime creation.

When I say "anyone", I mean anyone but this douche bag..

Even Jap Satoshi was more shocked at Faketoshi's claims than the reporter's claim it was him..

Moving along..

4. Its relentless focus on first order properties

Bitcoin is THE ONLY network of it's kind that has displayed such a stubborn, relentless focus on the primary drivers that count (ie; the elements I described above in Unit & Network).

Everything else comes second to maintaining the integrity of the network.

Furthermore, because of the way it's grown & the broad mixture of participants (miners / validators, nodes, holders, speculators, etc) that are now involved, that desire to retain the first order principles has basically turned into a core mandate.

That's something that's very hard to replicate — and something you can't do with software tweaks alone, and especially hard with pumped up ICOs & shitcoins with no stubborn minority & flakey speculators.

5. It's absolute (unit) scarcity

Something else that's ossifying, if not yet already ossified (thanks Andreas M. Antonopoulos for the terminology) is the absolute unit scarcity of Bitcoin.

The fact that more capital is flowing onto the Bitcoin Network, ie; dollars in exchange for an amount of units on the network that can never be inflated, is further reinforcing this attribute as a guarantee.

When you exchange anything else (dollars, work, shitcoin, etc) for Bitcoin, it's like owning a portion of land somewhere. It's territory on this finite network (or landscape), and you're not only given the guarantee of, but you further reinforce the guarantee that *your attribution with respect to whole will remain that way.*

Again — no other digital network (nor anything else that I know of really) can give you this guarantee, let alone make that guarantee stronger with each day that passes (Lindy compatible).

6. It's digitally native, & born of the internet

I loved when <u>Jack Dorsey</u> said: "Bitcoin is born of the internet" on the Joe Rogan show.

It's absolutely correct.

If the internet is this new world of bits & software, then it follows that a medium of exchange and value transfer that should be used & proliferate on this network is one that should also emerge from it.

Just like Gold & physical money has emerged from the physical world, over the millennia.

Bitcoin is the first time we've had a digital object, function like a physical one, (where time moves in one direction), that can be used as a monetary medium and give the same hard money guarantees we have in the 'real' world (assuming we're not already in a simulation…more on that next time).

Gold was the first hard money we found in the real world, and was the basis for everything we built thereafter. Show me another money that's lasted as long. I don't think you can. It's still **the standard** for the real world. **

Bitcoin is **the standard** for the digital world; and because it's digitally native; it's truly scalable—and we'll build everything on top of it.

** ***The Keynesian experiment we're running in the world now is a disaster waiting to happen, and has been conveniently masked as "functional" because technology (and bullshit monetary narratives) have managed to carry productivity forward despite the facade.***

7. Overall.

Bitcoin's robust, basic, adversarial design the closest thing to an anti-fragile network we've ever seen.

Bitcoin's unit and its network perfectly embody everything that money should be.

It's unstoppable, it gets better with time (Lindy compatible) & there is nothing quite like it.

There is no other money, network or copy-cat klepto-currency that exists which can replicate that.

Bitcoin is not its code, or its community, or its miners, or it' block size, or its history—it's all of these things, all mixed together—and that's why it's the only one that matters.

So to conclude this now essay, I'll leave you with three over-arching reasons as to why Bitcoin matters:

Bitcoin Matters because:

1. It's a Hard Money
2. It's a stable, secure, scalable financial network
3. It has the best chance of success

1. Hard Money

As I mentioned earlier, Bitcoin is a monetary phenomenon. These phenomena only come around once every epoch.

There are multiple reasons why you'd want to take note of a hard money:

a) Dis-Inflationary, ie; It will not lose value/purchasing power (you can give it to your children & your children's children). There is no other monetary medium other than gold that can give you this. Except with Bitcoin you can store billions in your head, and there's a greater guarantee of scarcity.

b) Hedge against corruption / stupidity / malevolence / incompetence. Whether you think the world is run by Lizards, or complete buffoons, or somewhere in between; chances are mistakes will happen (ie; 2008), and holding a hedge is a very, very intelligent idea.

c) Self-sovereign Unit. This one is not appreciated enough by non-bitcoiners. There is no other monetary unit in the world that is yours & only yours when you hold the key to it. It's Unconfiscatable (as Tone Vays has termed). People underestimate how powerful a concept like this is; until of course they lose their money somehow, or are censored.

d) Truly Scarce. I've discussed this on ad-nauseam throughout, and I'll say it again: Bitcoin is the only resource, other than time, that's truly scarce. This alone makes it an extremely intelligent asset to hold, whether you believe in that Bitcoin will take over the world (hyper-bitcoinization) or not.

2. As a stable, secure financial network

If we're going to build a ROBUST global financial (read: cooperative) system, it should be built on something secure, stable, game-theoretically sound and digitally native. You wouldn't build cars to run on horse tracks, and neither should you build the next generation of human cooperation (ie; money, finance & capital), on old shit with a digital veneer.

It's like putting lipstick on a Pig.

I scratch my head a little when I see these "Neo Banks" building on top of the legacy financial system, although I should probably be grateful because they're giving projects like what I'm working on @ Amber an opportunity to reinvent the idea of banking, by using Bitcoin and for the first time in history being truly open & transparent.

What gets me excited the most about having an incorruptible foundation, is the ability to build & anchor a layer above, such as Lighting.

A layer of Abstraction, Complexity & Interoperability.

- Bitcoin's basic, robust, digital, nature allows for abstraction & complexity to be built on top via layers of trust & transparency (not for wanks sake; but for the inclusion of skin in the game & management of tail risk [fragility])
- It will be just like the Internet, where the majority of the economic activity these past 20 years has occurred. All built on top of a set of core, basic, secure protocols (information & packet routing).

Remember the points Jeff Bezos made in his 2003 TED Talk.

And for those of you who subscribe to the multi-fat-protocols-are-eating-the-world thesis, these few images might help give you context :)
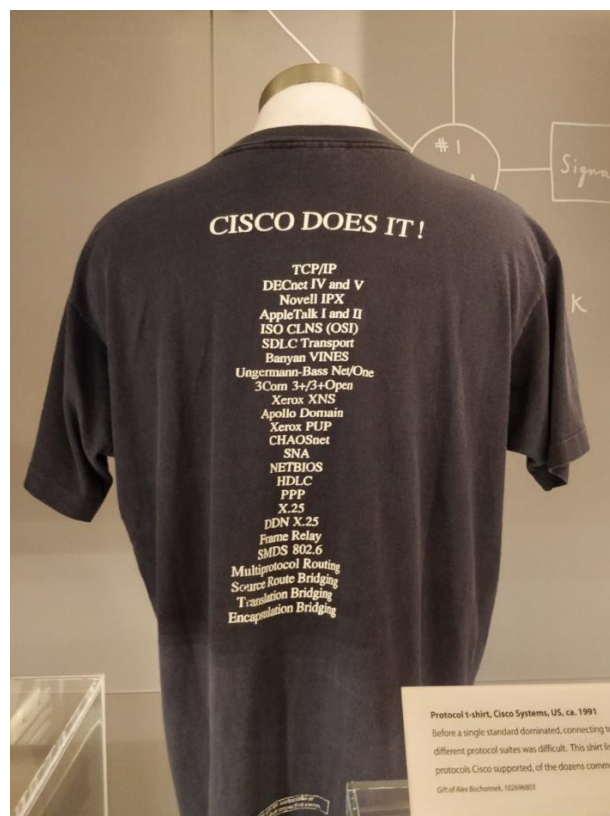
In the beginning, there were many…
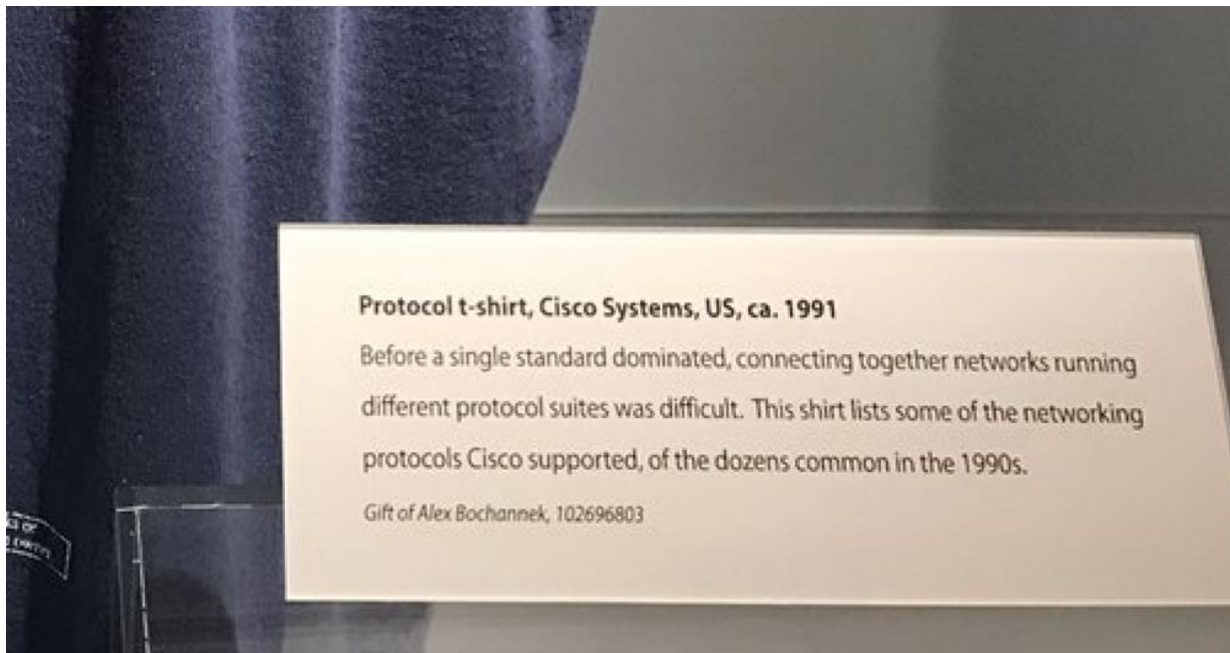
And it took a while for them to fade away

But one, won out. Does the above sound familiar at all???
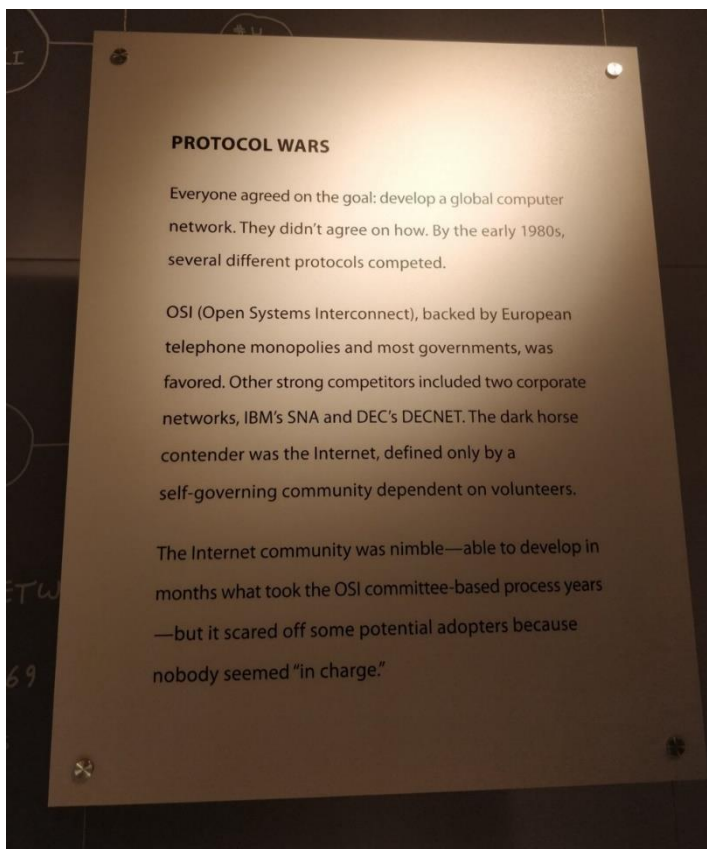
This last plaque is so very telling.

3. Bitcoin has the best chance of success

And last but not least:

If we're going to have a chance at creating a more open society, that resists censorship & the moronic attempts by the state (or the bureaucrats that run them) to centrally govern society via "theoretic" models that don't work in practice, then ***Bitcoin Matters.***

Wasting time looking for the next 'variation' of Bitcoin or pump & dump opportunity, created by the get rich quick schemers (scammers) and chased by the sheeple is a dangerous gig—because you don't know when the fools will run out & you're the last one holding the can.

This is why I'm often called a maximalist, but I don't care—because I'm adamant that we as a society have ONE chance at this, and if we dilute our impact by fucking around on other crap, we lose time & energy (at best), and at worst; we lose.

In saying that I don't think failure is likely—because Bitcoin has already won (we just can't see it yet, similar to the internet in the early 90s) —but I still believe we should save our other precious resource, ie; time, and FOCUS on what Matters. ***Bitcoin***
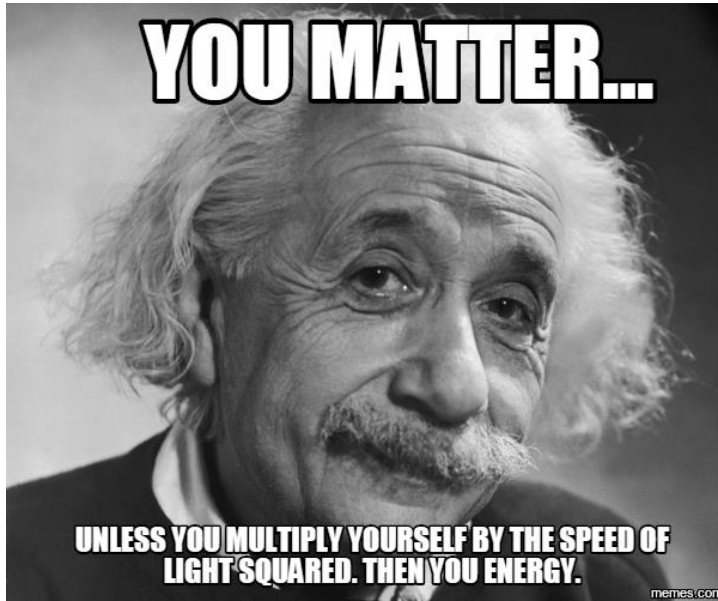
Conclusion

So to wrap this up:

Bitcoin matters.

- Just like the internet before it did.
- And electricity before that.

Bitcoin matters.

- Because it's the new **monetary operating system (OS).**
- It's the OS of the fair, skin in the game, robust form of capitalism that we all yearn for, that can drive humanity forward.

Bitcoin matters.

- Because it's the zeitgeist of our time.
- It's probably the biggest opportunity of mine and *your* life.

You don't want be the guy who missed out on this one—you'll feel like the biggest moron of all, probably worse than Ronald Wayne:

Sold his stake in Apple for $800. May have been worth > $50bn today.

So…take note & perhaps:

- Buy some Bitcoin.
- Hold some Bitcoin.
- Stop reading what the mainstream says.
- Support the industry.
- Work in it if you can.
- If you can't, buy some, use an app like what we're working on at Amber, and come back in a few years once things have matured further—you'll be glad you did.

I hope you got some value out of this. It's a message myself & all the team @ Amber strongly believe in, and it drives everything we're doing.

Wishing you all an amazing, prosperous new chapter ahead in 2019.

If you enjoyed this post, please show it some love, give it a clap (or a few) and pass it around to anyone you think should have a read.

Aleks Svetski

CEO & Co-Founder @ Amber Labs

www.getamber.io

Bitcoin Is a Cult, Fiat Is a Religion

Kay Kurokawa

Posted March 20, 2019

Frances Coppola, a long time critic of Bitcoin, declared that "Bitcoin is a Cult", which predictably stirred a lot of shit posting and ruffled feathers. Many Bitcoin'ers were offended by this declaration, resulting in name calling and ad hominem attacks, which ironically proved Coppola's points. Bitcoin is a cult, and no cultists likes to be pointed out as a cultist. She is not the first to point out this fact, others have said the same thing.

The cult label can be seen as a pejorative but I will attempt to explain here how it is a perfectly reasonable and necessary description of Bitcoin. A cult is just a religion with limited membership status and social acceptance. Musician Frank Zappa cleverly stated that "the only difference between a religion and a cult is the amount of real estate they own". So if Bitcoin is a cult, fiat money is a religion.

To demonstrate this point, I created the above meme which people really seemed to like. I believe this meme was popular because people are subconsciously aware of the religious nature of money. The fact that American paper money contains the phrase "In God We Trust" in capital letters is a confirmation of their awareness. It is only through faith that a piece of paper turns into some thing of value. In the modern age, it is a faith so firm and unshakable that it makes Jesus look like a second rate deity.

Once ideological faith has taken complete hold of an individual, the individual is no longer aware that he believes. A true believer does not see his ideology as an ideology, and divine facts are just facts. They do not practice religion, they practice the truth. Or as Marx would say of someone who is under the spell of a powerful ideology: "They do not know it. But they are doing it." (he is talking here about the ideology of capitalism). It is through this ideological lens that people are able to declare Bitcoin as a cult. It is akin to a Catholic declaring Mormonism a cult. Such ignorance can only be achieved when you have been ideologically compromised to accept your own ideology as the plain truth. Bitcoin cultists also suffer from the

same syndrome when they reject the cult status of Bitcoin, while at the same time participating in carnivore dinners, and engaging in emotionally charged social media attacks against heretics.

Readers may be skeptical of the intrinsic connection between money and faith. When we pay our electricity bill or buy some food at the grocery store, we do not feel any special connection to the divine, nor do we feel that we are practicing some religious activity. But yet, the foundations of our economic lives are directed by an object which only exists in the mind. Even though fiat money is just a piece of paper, or digits on a bank's computer, we devote our daily lives in pursuit of it. We do not know it, but we are doing it. We place an enormous amount of faith in our money, without knowing it.

Philip Goodchild writes in *Theology of Money*, that "All religion, in essence, direct and distribute time, attention, and devotion. Religions enrich life by establishing patterns for living." Does money not have the same effect ? Is money not the method in which our modern capitalist society direct and distribute time, attention, and devotion? If this is indeed the purpose of money, than the question of what money should be is inherently a moral, ethical, and political question. The answer to such a question cannot be monopolized by economists masquerading as scientists, for the answer we seek is not scientific in nature. We are not measuring the effects of physical phenomenons or proving a mathematical theorem. We are not mere automatons in a system designed to optimize GDP, employment numbers, and trade surplus.

If we define money as the method in which society direct and distribute time, attention, and devotion, than that means any attempts to redefine money is inherently a political activity rooted in an ideology of how society should be structured. Given how radically opposed Bitcoin is from the prevailing modern fiat system, there is no way for Bitcoin to succeed without true believers. True believers will be at the front lines in a fight against the inquisitors of the fiat system, who will do everything they can to to keep their money printable and censorable. These two properties of the fiat system are the cornerstones of the modern capitalist society. By presenting an alternative, Bitcoin is not only challenging a prevailing ideology, it is challenging the established hierarchy and power structure that has been constructed around it.

Those that believe that this fight is not coming, either misunderstands the above stated fact, or is overestimating what Bitcoin as a technology can achieve. They erroneously believe that "blockchain technology" magically secures itself and can autonomously impose its own will on society without human intervention. As Eric Voskuil writes: "Technology is never the root of system security. Technology is a tool to help people secure what they value. Security requires people to act. A server cannot be secured by a firewall if there is no lock on the door to the server room,

and a lock cannot secure the server room without a guard to monitor the door, and a guard cannot secure the door without risk of personal harm. Bitcoin is no different, it is secured by people who place themselves at personal risk (Risk Sharing Principle)."

Casual users and profit seekers driven purely by economic incentives will not place themselves at personal risk to protect Bitcoin. They are weak hands that will scatter at the first sight of trouble. It is only the true believers who will place themselves at personal risk. When propaganda starts to fill the social media channels, true believers will fight back with education. When the law comes knocking on people's door, true believers will keep their Bitcoin hidden. When the state starts to perform a 51% attack, true believers will deploy hashing power to fight back. And it is the true believers who are tirelessly developing on Bitcoin; trying to make it more secure and easier to use without enforcing a tax on the system or rent seeking for personal profit.

Bitcoin can only succeed as a cult for all money is a religion. It is only when Bitcoin has won that it will shed its cult status. When Bitcoin becomes a religion, as fiat is now, we will no longer be aware that we are believing. One Bitcoin will simply be one Bitcoin, and one dollar will be a memory of an irrelevant and dated ideology.
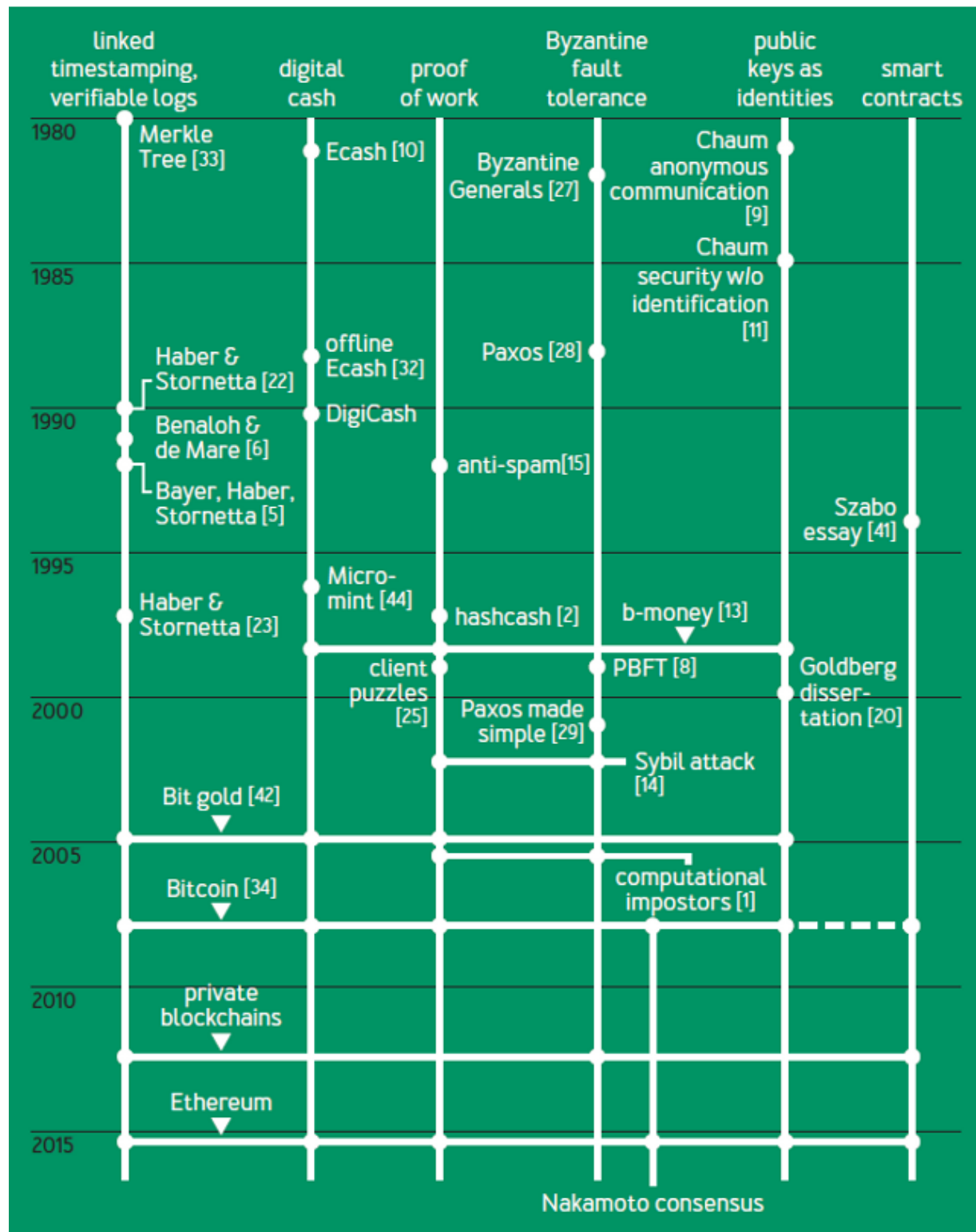
On Bitcoin's Academic Lineage

By ElSeidy

Posted March 22, 2019

Stiglers law of eponymy states that no scientific discovery is named after its original discoverer. For example, the pythagorean theorem was well known to the Babyolnians much before Pythagoras. Other examples include Hubble's law, Haley's comet, and Stigler's law itself—being self-referential. It comes as no surprise that Bitcoin is no different. There is a common misconception that Bitcoin bears no resemblance to earlier academic work. Prof. Arvind Narayanan, from Princeton university, challenges this view, in his published article named " _ Bitcoin's Academic Pedigree _ ". He shows that almost all of the technical components of Bitcoin originates from the academic literature of the 80s and 90s. This is not to diminish Nakamoto's contribution but to turn attention towards the fact that they stood on the shoulders of giants. Nakamoto's genius was in the intricate way they assembled the components together into a resilient and secure system. Narayanan's positioning of Bitcoin within academic literature helps us appreciate its novelty in the right dimension.

Bitcoin's intellectual history also serves as a case study demonstrating the relationships among academia, outside researchers, and practitioners, and offers lessons on how these groups can benefit from one another. In this article we summarize the main points from Narayanan's article and conclude with a set of lessons learned.

FIGURE 1: CHRONOLOGY OF KEY IDEAS FOUND IN BITCOIN

Chronology of key ideas found in Bitcoin. Image taken from Bitcoin's Academic Pedigree.

The ledger

The public ledger is the most fundamental component of Bitcoin. To understand Bitcoin's history, we first need to understand the ledger. It is where all transaction records are saved and trusted by all system participants. Bitcoin converts this system for recording payments into a currency. The ledger, as a datastructure, should be **a)** immutable, meaning that its historical state can never be changed, and should be able to **b)** obtain a succinct *cryptographic digest* of the ledger-state at any time, and have a **c)** consistent global view across all distributed nodes.

Linked Timestamping

Bitcoin's ledger data structure is borrowed from a series of papers by Stuart Haber and Scott Stornetta written between years 90-97. Their work addressed the problem of document timestamping as they aimed to build a "digital notary" service. Their abstraction of a document is quite general and could be of any data type. They mention financial transactions as a potential application, but it wasn't their focus.

In their design, documents are constantly being created and broadcast. The creator of each document declares a creation timestamp and signs both, the current document and the previously broadcast document. This previous document has signed its own predecessor as well, thereby, creating a long chain of documents with pointers backwards in time. This chain-signing property is essential to provide the **immutability** properties of the datastructure. As followup to their initial work, they introduced other ideas that make this data structure more effective and efficient:

Hashes: Documents are interlinked with each other using hashes rather than signatures as hashes are simpler and faster to compute.

Batching: Instead of chaining individual documents, one can group them into batches or blocks such that all documents within a block have the same timestamp.

Indexing: Within each block, rather than representing the documents using a linear chain, one can link them together using a binary tree of hash pointers, called a Merkle tree.

Clearly, if you replace documents with transactions, this design resembles bitcoin to a great extent. Nakamoto cites Stuart and Scott's work in his original paper.

FIGURE 2: **THE LEDGER DATA STRUCTURE IN LINKED TIMESTAMPING**
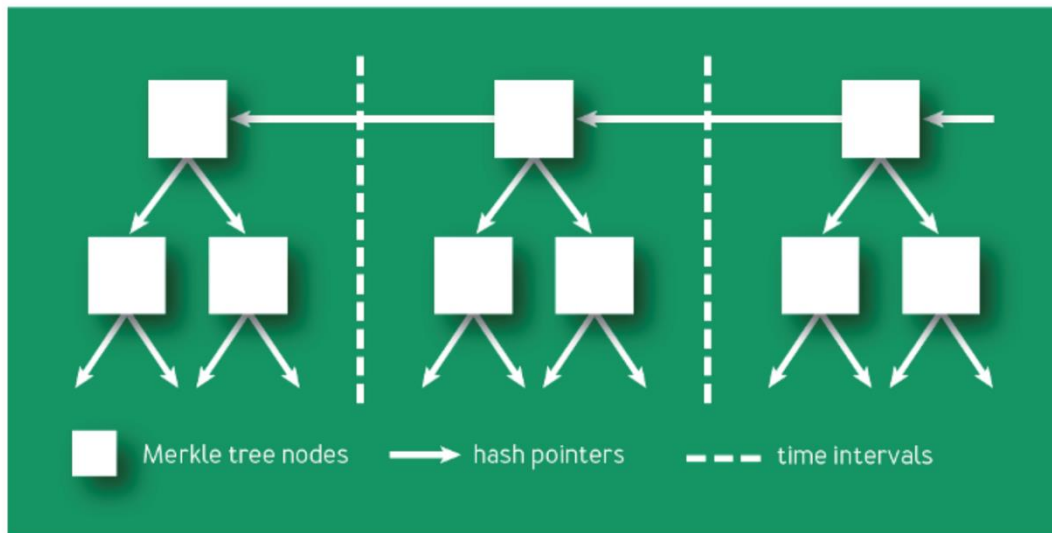
The ledger data structure in Linked Timestamps. Image taken from Bitcoin's Academic Pedigree.

Merkle Trees

As mentioned earlier, it is more efficient to represent blocks using trees rather than a linear-chain. Abstractly, each block is represented as a Merkle tree, where the leaf nodes are transactions, and internal nodes consist of two pointers pointing to its children and a digest computed by their hashes as depicted in Fig. x. This data structure has two important properties:

1. The hash of the latest block acts as a **b)digest**. Any small change to any of the transactions will have a rippling effect all the way to the root of the current block, and the roots of all following blocks. Therefore, knowing the latest hash is sufficient to download a verified ledger from untrusted sources.
2. Another important property is the ability to efficiently prove that a particular transaction is included in the ledger. This is a highly desirable property for performance and scalability reasons.

Merkle trees have been around long before. They are named after Ralph Merkle, a pioneer in asymmetric cryptography who proposed the idea in his 1980 paper. By cryptographic standards, this idea is ancient, but its power has been appreciated since late.

Bitcoin may be the most well-known real-world instantiation of Haber and Stornetta's data structures, but it is not the first. For example, Guardtime started offering document timestamping services in 2007.

Consensus & Byzantine Fault Tolerance

Another important requirement for public ledgers is to achieve a **consistent** transaction (or block) ordering across all nodes. **Consensus** across all nodes about state-consistency is inevitable for the ledger, or else, the collective ledger can spawn to different chain-forks. Linked timestamping alone is not enough to resolve forks.

A different research field called, **fault-tolerant distributed computing**, has studied this problem for decades. Generally speaking, the solution to this problem is one that enables a set of nodes to adopt the same state/transaction transitions in the same order. The particular order doesn't matter as much as the consistent view across all nodes.

Early solutions, including Paxos, proposed by Turing Award winner Leslie Lamport in 1989 had constraints on the definition of faulty nodes. A prolific literature followed with more adverse definitions. The definition of *faulty* was generalized to handle any deviation from the protocol. Such Byzantine faults includes both naturally and maliciously occurring faults. In 1999, a landmark paper by Miguel Castro and Barbara Liskov introduced PBFT which accommodated both Byzantine faults and unreliable networks.

The literature of fault tolerance is huge and encompasses hundreds of variants and optimizations of Paxos, PBFT, and other seminal protocols. Nakamoto does not cite this literature or use its language in his original white paper. This is in stark contrast to linked timestamping. However, all of this work makes assumptions about the definition of honest nodes as being procotol-compliant behavior among a subset of participants. On the other hand, Nakamoto suggests that it is not necessary to blindly assume honest behavior because it is incentivized. A richer Nakamoto consensus analysis that takes into account the role of incentives does not fit cleanly into past fault-tolerant systems models.

Proof of Work

Nearly all fault-tolerant systems assume that most nodes in the system, e.g. 50 percent, are both honest and reliable. Nodes freely join and leave in an open P2P network. An adversary can therefore create enough nodes to overcome the system's consensus guarantees. John Douceur formalized the attack on Sybil in 2002 turning to a cryptographic construction, called proof of work to mitigate it. A large segment of the Bitcoin community has the misconception that Nakamoto invented proof of work. The first proposal that could be called PoW today was created in 1992 by Cynthia Dwork and Moni Naor. Their aim was to deter spam by forcing email recipients to process only those emails that were accompanied by evidence that a moderate amount of computational work had been performed by the sender-hence, "proof of work."

Hashcash

In 1997, Adam Back, a postdoctoral researcher at the time who was part of the cypherpunk community, invented a very similar idea called hashcash. Hashcash is much simpler than the idea of Dwork and Naor, because it uses hash functions. It is based on a simple principle: a hash function acts as a random function, which means that the only way to find an input that hashes a particular output is to try different inputs until the desired output is produced. As the name suggests, proof of work in hashcash was seen as a form of cash. However, the design of hashcash has no protection from double spending.

Incidentally, only in 1999 was the term work proof <u>coined in a paper</u> by Markus Jakobsson and Ari Juels, which also includes a nice survey of the work up to that point.

Digital Cash

Proof of work did not succeed as an anti-spam measure. One possible reason is the dramatic difference in the puzzle-solving speed of different devices. That means spammers can make a small investment in custom hardware to increase their spam rate by orders of magnitude.

In economics, the natural response to an asymmetry in the cost of production is trade—that is, a market for proof-of-work solutions. But this presents a paradoxical situation, because that would require a working digital currency. Indeed, the lack of such a currency is a major part of the motivation for proof of work in the first place. As hashcash tries to do, one crude solution to this problem is to declare puzzle solutions as cash. More coherent approaches to treating puzzle solutions as cash are found in two essays that preceded bitcoin, describing ideas called <u>b-money</u> and Nick Szabo's <u>bit gold</u> respectively. However, if there is disagreement between servers or nodes about the ledger, there is no clear way to resolve it. These mechanisms are not very secure because of the Sybil problem.

Bitcoin

Understanding all these predecessors that contain pieces of bitcoin's design leads to an appreciation of the true genius of Nakamoto's innovation. In bitcoin, for the first time, puzzle solutions don't represent cash by themselves. on the contrary, they are merely used to secure the ledger. Solving proof of work is performed by specialized entities called miners.

A miner who contributes a block is rewarded with newly minted units of the currency in exchange for the service of maintaining the ledger,whereas malicious

activity is penalized. In this way, miners ensure each other's compliance with the protocol due to the monetary incentives.

Bitcoin neatly avoids the double-spending problem plaguing *proof-of-work-as-cash* schemes because it avoids puzzle solutions themselves having value. In fact, puzzle solutions are decoupled twice from the economic value: the amount of work needed to produce a block in proportion to the global mining power, and the number of bitcoins issued per block.

Nakamoto's genius, then, wasn't any of the individual components of bitcoin, but rather the intricate way in which they fit together to breathe life into the system. The timestamping and Byzantine agreement researchers didn't hit upon the idea of incentivizing nodes to be honest, nor, until 2005, of using proof of work to do away with identities. Conversely, the authors of hashcash, b-money, and bit gold didn't incorporate the idea of a consensus algorithm to prevent double spending. In bitcoin, a secure ledger is necessary to prevent double spending and thus ensure that the currency has value. A valuable currency is necessary to reward miners. In turn, strength of mining power is necessary to secure the ledger. Without it, an adversary could amass more than 50 percent of the global mining power and thereby be able to generate blocks faster than the rest of the network, double-spend transactions, and effectively rewrite history, overrunning the system. Thus, bitcoin is bootstrapped, with a circular dependence among these three components. Nakamoto's challenge was not just the design, but also convincing the initial community of users and miners to take a leap together into the unknown — back when a pizza cost 10,000 bitcoins and the network's mining power was less than a trillionth of what it is today.

Public Keys as Identities

Bitcoin uses public keys as identities in the system. Transactions transfer value from and to public keys, which are called addresses. This notion of decentralized identity management dates back to David Chaum, the father of digital cash. In his 1981 paper, he states: "A digital 'pseudonym' is a public key used to verify signatures made by the anonymous holder of the corresponding private key". The public-keys-as-identities idea is also seen in b-money and bit gold. Thus Bitcoin proved to be the most successful instantiation of Chaum's idea.

Blockchains

Nakamoto makes no mention of the term blockchain. In fact, the term blockchain does not have a standard technical definition but is a loose umbrella term used by different parties to refer to systems with varying levels of resemblance to bitcoin and its ledger. Narayanan injects a dose of skepticism around blockchains for the following reasons:

Many proposed blockchain applications, especially in banking, don't use Nakamoto consensus. Instead, they use the ledger data structure and Byzantine agreement which date back to the '90s. This negates the claim that blockchains are a new and revolutionary technology. Instead, the buzz around blockchains has helped banks launch collective action to deploy shared-ledger technology, like the "stone soup" parable.

Blockchains are frequently presented as more secure than traditional registries which is a misleading claim. The *systemic* risk of blockchains may be lower than that of many centralized institutions, but the *endpoint-security* risk of blockchains is much worse. For example, in a blockchain-based stock registry, if a user loses control of her private keys, she loses her assets.

Conclusions and Lessons

The history described in Naryanan's survey provides practitioners and academics rich and complementary lessons:

Practitioners should be skeptical about revolutionary technology claims. Most of the ideas in bitcoin that have generated excitement in the enterprise, such as distributed ledgers and Byzantine agreement, actually date back 20 years or more. Recognize that no breakthroughs may be required for your problem.

Academia seems to have the opposite problem of resisting to radical, extrinsic ideas. The bitcoin white paper was more novel than most academic research. We've seen repeatedly that ideas in the research literature can be gradually forgotten or unappreciated, particularly if they are ahead of their time.

Both practitioners and academics would do well to revisit old ideas to glean insights for present systems. Bitcoin was unusual and successful not because it was on the cutting edge of research on any of its components, but because it combined old ideas from many previously unrelated fields. This is not easy to do, as it requires bridging disparate terminology and assumptions.

It should be possible for practitioners to identify overhyped technology. Some hype indicators include, difficulty identifying the technical innovation; difficulty of finding meaning of supposedly technical terms, because of companies eager to attach their own products to the bandwagon; difficulty identifying the problem that is being solved; and finally, technology claims solving social problems or creating economic & political upheaval.

In contrast, it is difficult for academia to sell its inventions. For example, it's unfortunate that the original proof-of-work researchers do not get credit for bitcoin, possibly because the work wasn't well known outside academic circles. Engaging
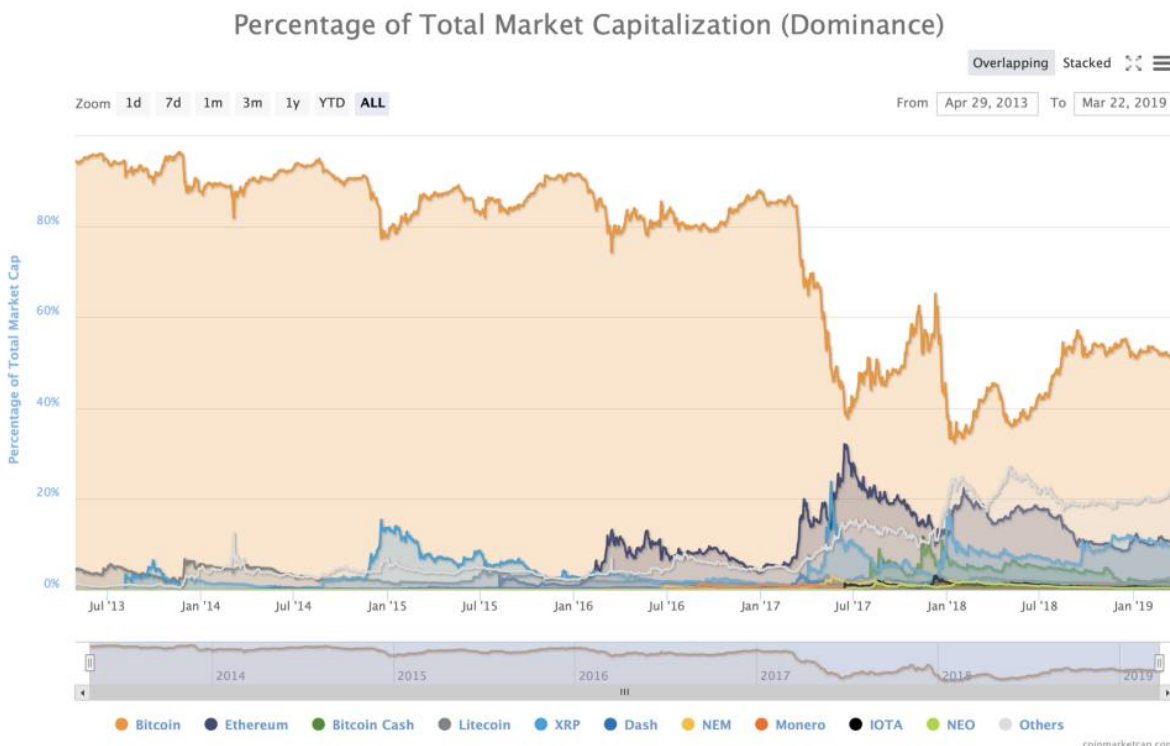
with the real world is a source of fresh ideas that not only helps get credit but also reduces reinvention.

Bitcoin's True Market Dominance

Analysing Bitcoin's true market dominance, taking liquidity into account. A new metric, Volume-Weighted Cap, is derived and shows that Bitcoin has Pareto dominance (>80%) on the market.

By JP Thor [₿ ⚡]

Posted March 22. 2019

CMC's Market Dominance—a flawed metric

Browsing twitter recently I saw a tweet quoting Vitalik, the infamous founder of Ethereum, from some podcast:

I took the comment to be rather disingenuous, knowing that Vitalik enthralls at every chance to show mathematical edge. He seemed to be referring to CoinMarketCap's "Market Dominance", a metric fixated on by many, despite being based on "market cap"—a lamented metric. Market Cap on CMC is simply the market price multiplied

by circulating supply, which many argue can easily be manipulated by things such as low volume, pre-mines and circulating supply malfeasance.

I immediately wondered if market share was some form of Pareto-distribution, "the **law of the vital few,** or the **principle of factor sparsity".**Pareto Distribution is itself a form of Power Law, and is often observed in nature where the rule of equilibrium abounds.

Considering that cryptocurrency trading is practically a free market (very few externalities), I posed the hypothesis that it *was* a Pareto distribution, and set out to test it.

Pareto Distribution

The Pareto Distribution is given by the equation:

```
y = 20% ^(log(x)/log(80%))
```
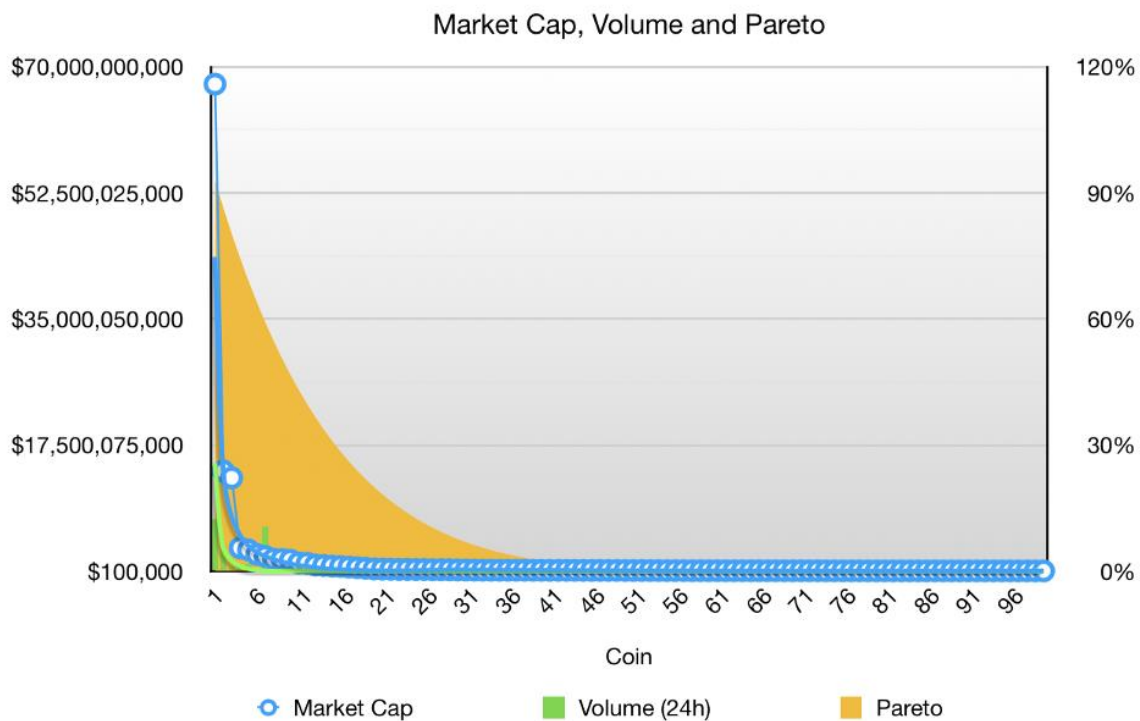
Pareto Distribution
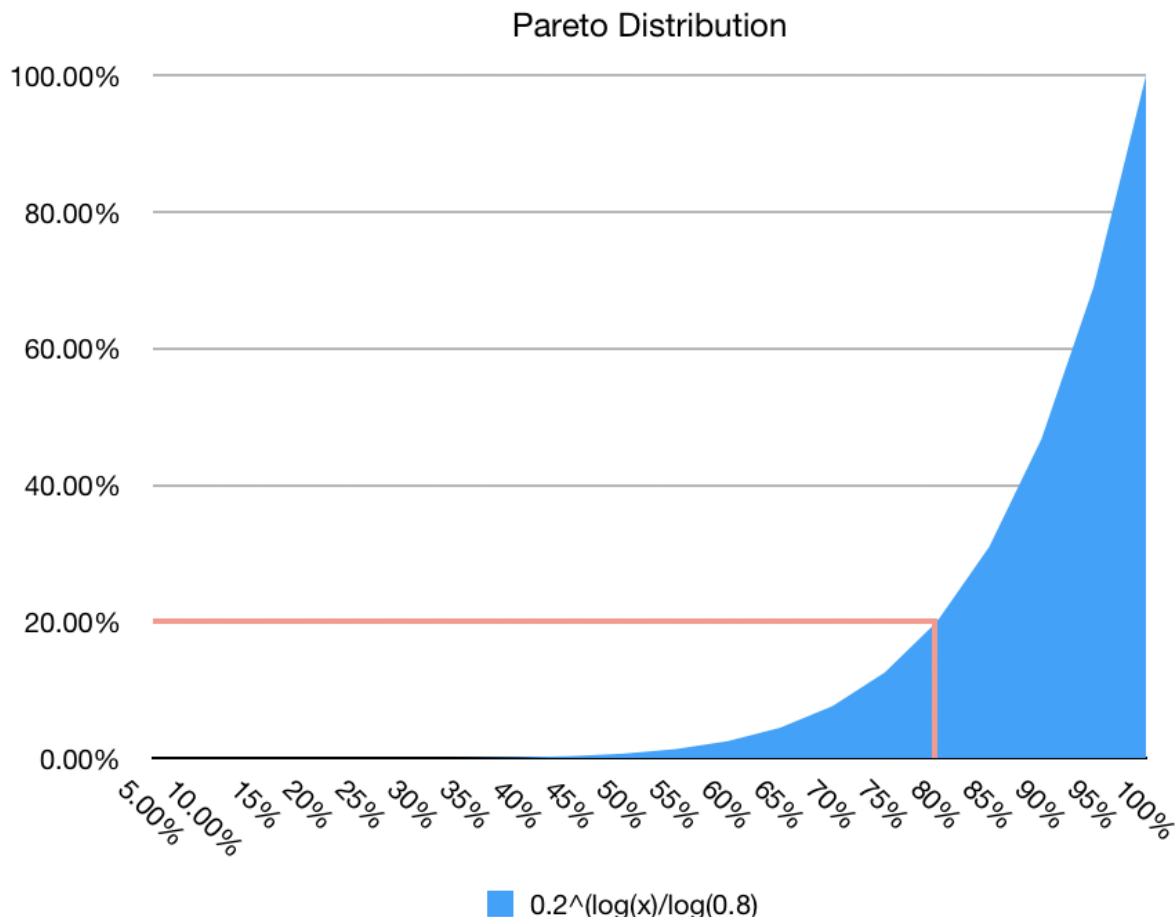
Pareto Distribution

The characteristic that is most notable is *"80% is owned by the 20%, 20% is owned by the 80%",* which is quite easy to highlight. It is scale invariant—essentially no matter

the scale spectrum, the distribution is the same. It can also be referred to as a fractal distribution since it looks the same at any level of zoom.
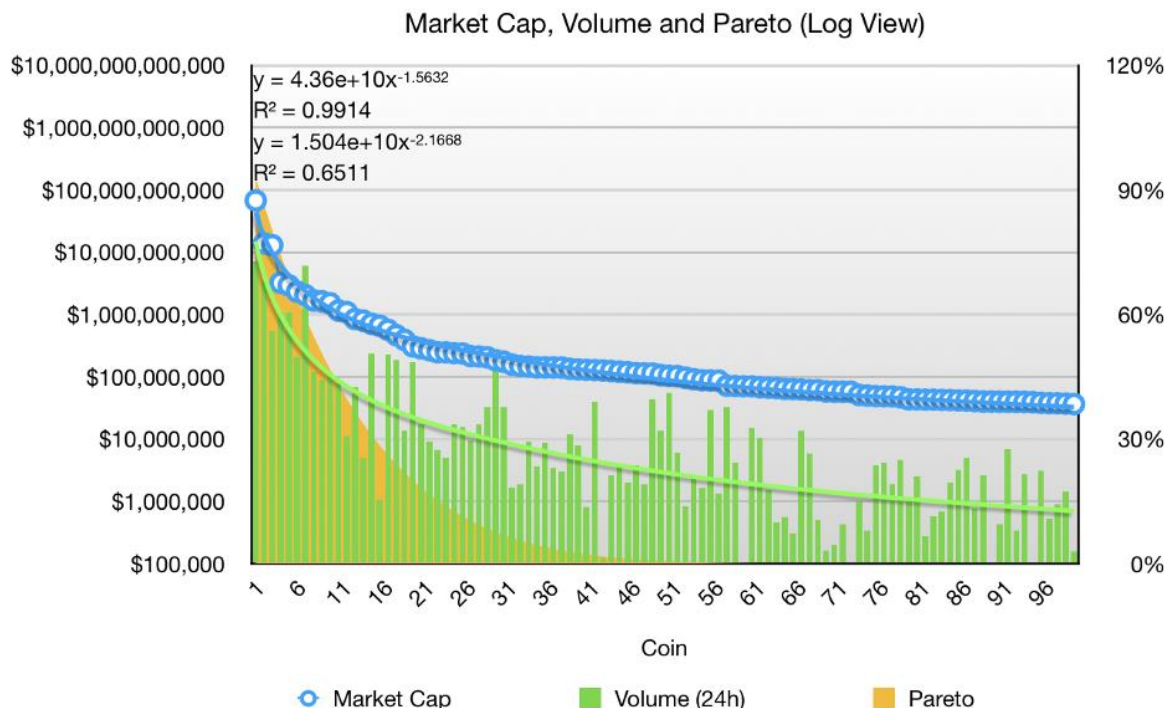
The Volume Problem

The Top 100 Coins and their MarketCap and Volume were plotted against a generic Pareto Distribution:

Not a Pareto Distribution

It wasn't even closely aligned with a Pareto Distribution, and the linear scale wasn't appropriate.

Switching to Log view, it was clear there *was* some form of <u>Power Law Distribution</u>.

Market Cap, Volume and Pareto (Log View)

$$y = 4.36\mathrm{e}{+}10x^{-1.5632}$$
$$R^2 = 0.9914$$
$$y = 1.504\mathrm{e}{+}10x^{-2.1668}$$
$$R^2 = 0.6511$$

Legend: ○ Market Cap   ■ Volume (24h)   ■ Pareto

Poor volume correlation

While **MarketCap** had high a R^2 value (best-fit), which seemed natural since the coins were ranked in order of market cap, what was concerning to me was the low R^2 for **Volume.**I expected this to share the same distribution as market cap.

Low volume in some coins was indicative of a trapped market, and artificial market cap—some coins had less than 0.1% of their market cap in daily volume, compared to the Top 10, which all had >30% in volume/cap; a difference of more than two factors.

Volume-Weighted Cap

I deduced that Volume (liquidity) *had to be* weighted as a metric, so they were multiplied together to form another metric: **"Volume-Weighted Cap ($²)".**The lower the volume, the lower the overall score.

Aggregating the last 12 months of records, averaging, then capturing the proportion of **"Volume-Weighted Cap"** over the Top 100 coins, the following plot was obtained:

Volume Weighted Cap (Log Distro)
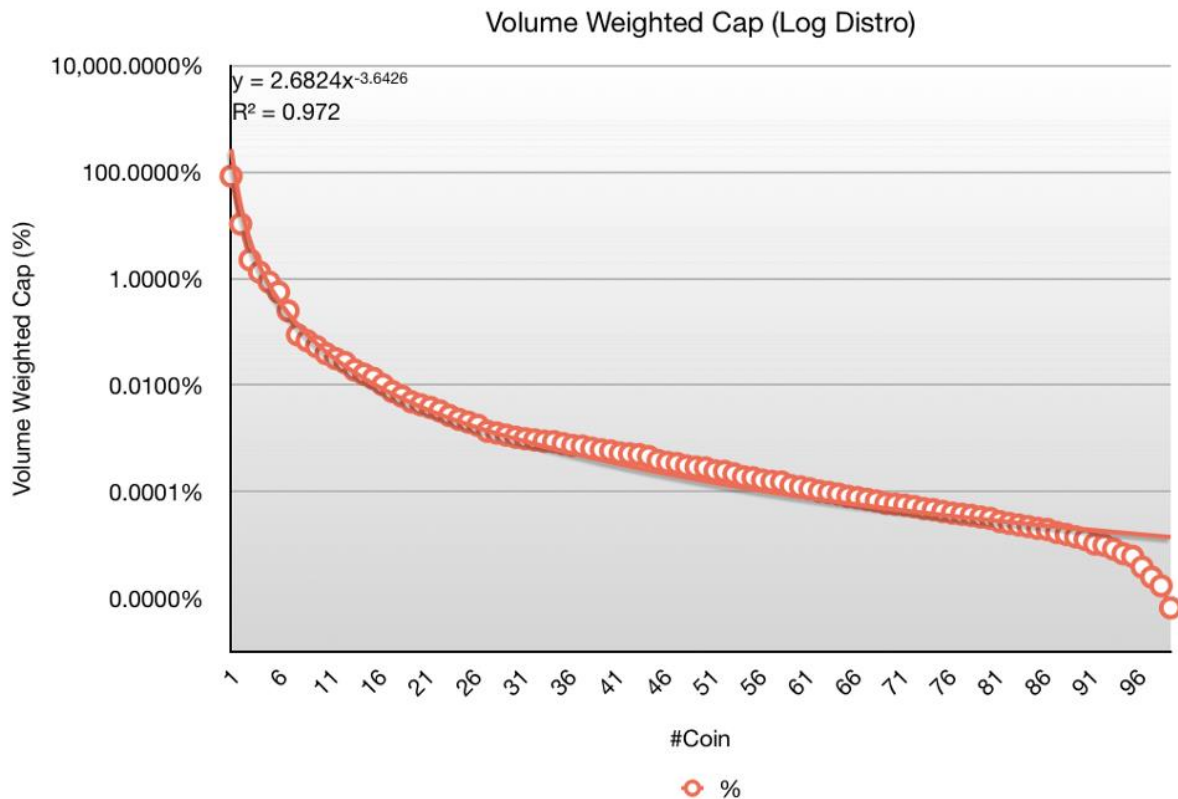
A surprising S curve

Firstly the R² value was noticed to be much higher, and an interesting "S" curve was observed. It seemed that the bulk of the average Top 100 complied with Power Law, before dropping precipitously towards the final 10 coins. Without doing further research into this, I hypothesised that it was the "Page 1 effect", where coins that are in the Top 100 of CMC attract the most attention, and coins towards the end of the page drop in and out of the first page, losing interest as a result.

Removing the final 1/3rd of coins, the first 67 were plotted on a Log-Log scale, with very high correlation to Power Law:

Volume Weighted Cap (Log-Log Distro)

$$y = 1.3273x^{-3.3807}$$
$$R^2 = 0.9961$$
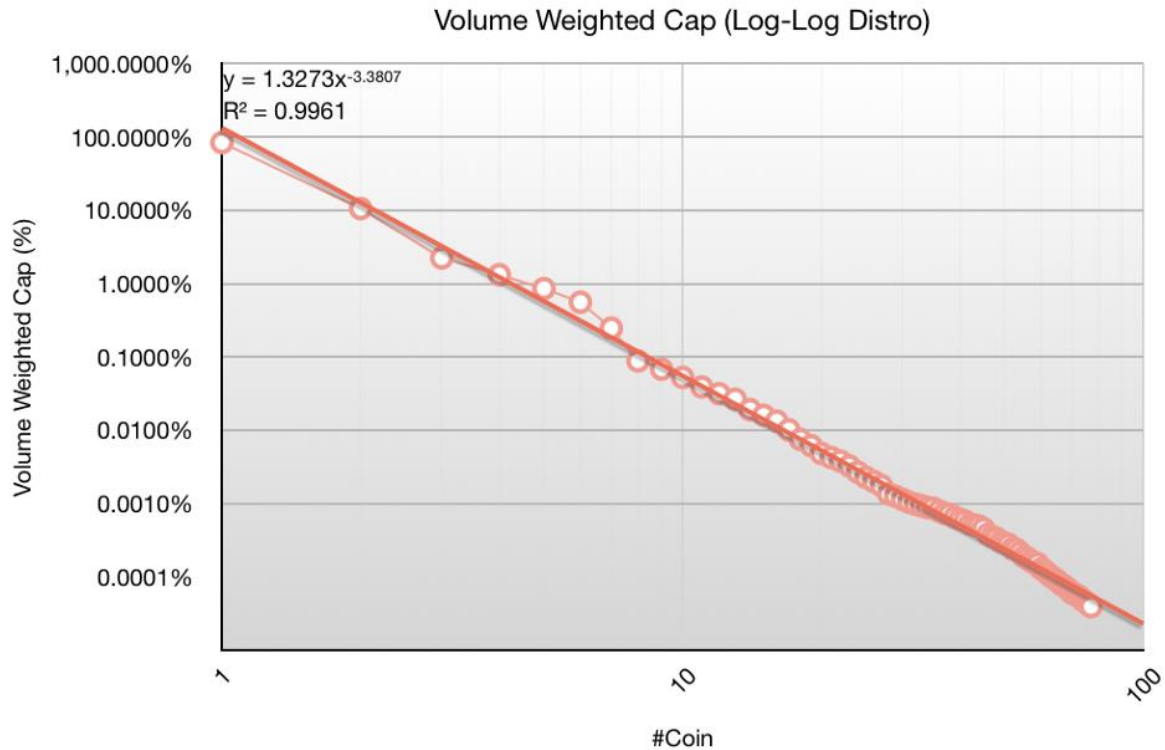
High correlation with Power Law

Sorting the Top 67 coins by Volume-Weighted Cap, and then plotting Market Cap and Volume, it was **immediately obvious** that the Power Law best-fit scores were cumulatively *much higher.*
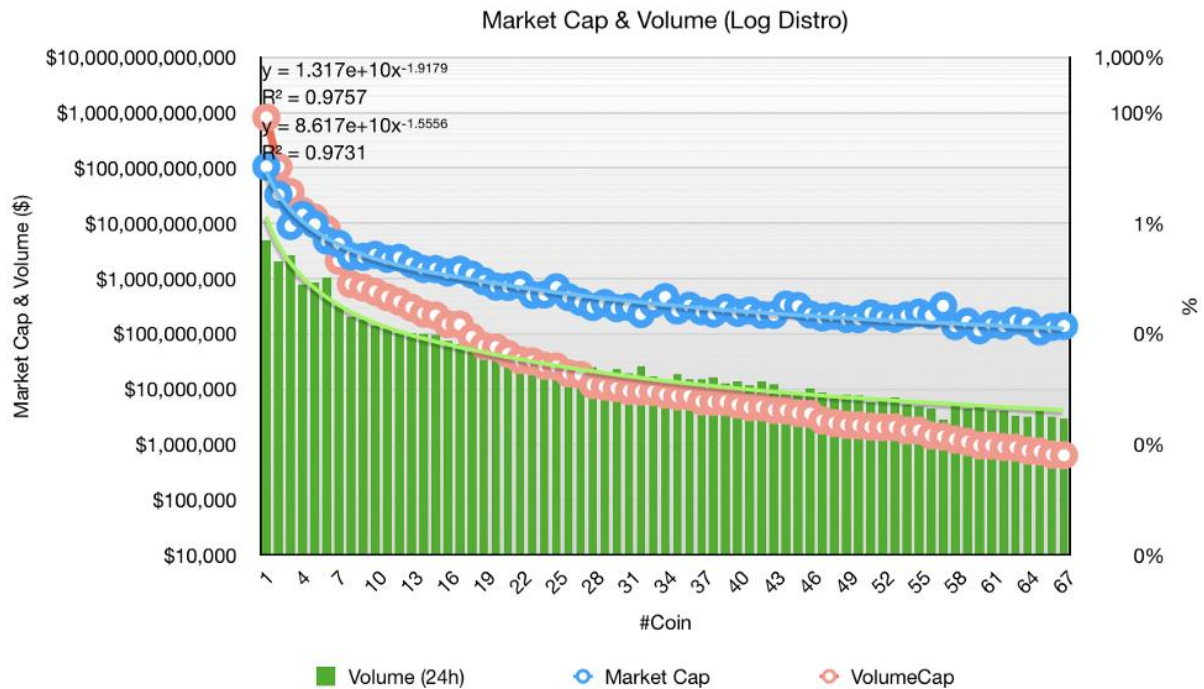
A much better sort for both Volume and MarketCap

Thus I concluded that the market spread *was* in fact a Power Law Distribution (but not strictly Pareto), and it required factoring in liquidity.

Volume-Weighted Market Dominance

Now returning to the original inspiration for the research, I sort to address what was the true dominance of Bitcoin, taking volume into account.

The last 12 months of Volume-Weighted Cap were plotted for Bitcoin, Ethereum and Others (which included Ethereum):

Volume-Weighted Market Dominance for Bitcoin is 80% and trending up

It is clear that Bitcoin *is* the dominant currency when taking liquidity into account. In terms of *share*, it is consistently over 80% and trending up.

In fact, just taking into account the Top 5 coins, Bitcoin (the 20%) captures over 85% of the market—thus it is a Pareto distribution, and actually *much stronger.* This is only testament to how strong the Schelling Point around Bitcoin is.

Top 5 Distro
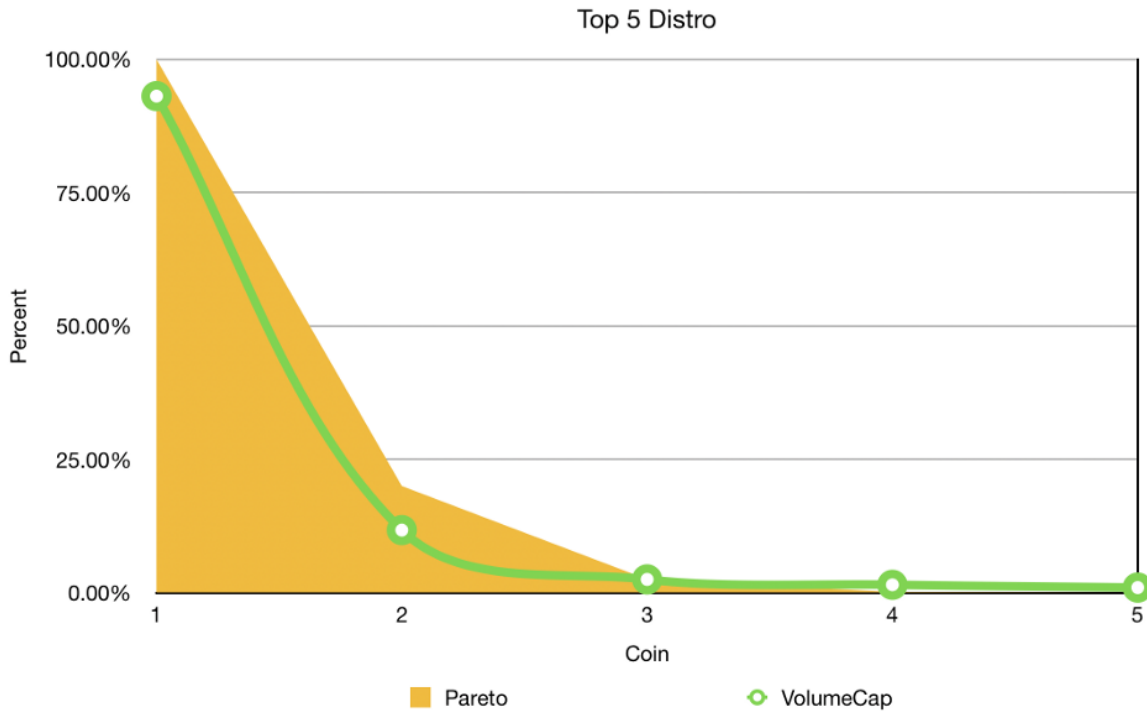
Bitcoin (#1) has Pareto Dominance in the Top 5

It is my opinion that Bitcoin will continue to preserve its Schelling Point, and maintain greater than 80% market dominance. CoinMarketCap's **"Market Dominance"** is flawed since it does not factor in liquidity and the reported 55% is significantly understated.

Thus I conclude that Vitalik is mis-informed and lazy in his reference to CMC's flawed market share of Bitcoin, when in fact, it is stronger than ever.

Follow me on twitter, I research and write about Bitcoin.

https://twitter.com/jpthor__

Modeling Bitcoin's Value with Scarcity

By PlanB

Posted March 22, 2019

Introduction

Satoshi Nakamoto published the bitcoin white paper 31/Oct 2008 [1], created the bitcoin genesis block 03/Jan 2009, and released the bitcoin code 08/Jan 2009. So begins a journey that leads to a $70bn bitcoin (BTC) market today.

Bitcoin is the first scarce digital object the world has ever seen. It is scarce like silver & gold, and can be sent over the internet, radio, satellite etc.

" As a thought experiment, imagine there was a base metal as **scarce as gold** but with the following properties: boring grey in colour, not a good conductor of electricity, not particularly strong [..], not useful for any practical or ornamental purpose .. and one special, magical property: **can be transported over a communications channe**l" — Nakamoto [2]

Surely this digital scarcity has value. But how much? In this article I quantify scarcity using stock-to-flow, and use stock-to-flow to model bitcoin's value.

Scarcity and Stock-to-Flow

Dictionaries usually define scarcity as 'a situation in which something is not easy to find or get', and 'a lack of something'.

Nick Szabo has a more useful definition of scarcity: 'unforgeable costliness'.

"What do antiques, time, and gold have in common? They are costly, due either to their original cost or the improbability of their history, and it is difficult to spoof this costliness. [..] There are some problems involved with implementing **unforgeable costliness** on a computer. If such problems can be overcome, we can achieve bit gold." — Szabo [3]

"Precious metals and collectibles have an **unforgeable scarcity** due to the costliness of their creation. This once provided money the value of which was largely independent of any trusted third party. [..][but] you can't pay online with metal. Thus, it would be very nice if there were a protocol whereby unforgeably costly bits could be created online with minimal dependence on trusted third parties, and then securely stored, transferred, and assayed with similar minimal trust. Bit gold." — Szabo [4]

Bitcoin has unforgeable costliness, because it costs a lot of electricity to produce new bitcoins. Producing bitcoins cannot be easily faked. Note that this is different for fiat money and also for altcoins that have no supply cap, have no proof-of-work (PoW), have low hashrate, or have a small group of people or companies that can easily influence supply etc.

Saifedean Ammous talks about scarcity in terms of stock-to-flow (SF) ratio. He explains why gold and bitcoin are different from consumable commodities like copper, zinc, nickel, brass, because they have high SF.

"For any consumable commodity [..] doubling of output will dwarf any existing stockpiles, bringing the price crashing down and hurting the holders. For gold, a price spike that causes a doubling of annual production will be insignificant, increasing stockpiles by 3% rather than 1.5%."

"It is this consistently low rate of supply of gold that is the fundamental reason it has maintained its monetary role throughout human history."

"The high **stock-to-flow ratio**of gold makes it the commodity with the lowest price elasticity of supply."

"The existing stockpiles of Bitcoin in 2017 were around 25 times larger than the new coins produced in 2017. This is still less than half of the ratio for gold, but around the year 2022, Bitcoin's **stock-to-flow ratio**will overtake that of gold"—Ammous[5]

So, scarcity can be quantified by SF.

SF = stock / flow

Stock is the size of the existing stockpiles or reserves. Flow is the yearly production. Instead of SF, people also use supply growth rate (flow/stock). Note that SF = 1 / supply growth rate.

Let's look at some SF numbers.

	Stock (tn)	Flow (tn)	SF	supply growth	Price $/Oz	Market Value
gold	185,000	3,000	62	1.6%	$ 1300	$ 8,417,500,000,000
silver	550,000	25,000	22	4.5%	$ 16	$ 308,000,000,000
palladium	244	215	1.1	88.1%	$ 1400	$ 11,956,000,000
platinum	86	229	0.4	266.7%	$ 800	$ 2,400,000,000

Gold has the highest SF 62, it takes 62 years of production to get current gold stock. Silver is second with SF 22. This high SF makes them monetary goods.

Palladium, platinum and all other commodities have SF barely higher than 1. Existing stock is usually equal or lower than yearly production, making production a very important factor. It is almost impossible for commodities to get a higher SF, because

as soon as somebody hoards them, price rises, production rises, and price falls again. It is very hard to escape this trap.

Bitcoin currently has a stock of 17.5m coins and supply of 0.7m/yr = SF 25. This places bitcoin in the monetary goods category like silver and gold. Bitcoin's market value at current prices is $70bn.

Supply of bitcoin is fixed. New bitcoins are created in every new block. Blocks are created every 10 minutes (on average), when a miner finds the hash that satisfies the PoW required for a valid block. The first transaction in each block, called the coinbase, contains the block reward for the miner that found the block. The block reward consists of the fees that people pay for transactions in that block and the newly created coins (called subsidy). The subsidy started at 50 bitcoins, and is halved every 210,000 blocks (about 4 years). That's why 'halvings' are very important for bitcoins money supply and SF. Halvings also cause the supply growth rate (in bitcoin context usually called 'monetary inflation') to be stepped and not smooth.

source: https://plot.ly/~BashCo/5.embed
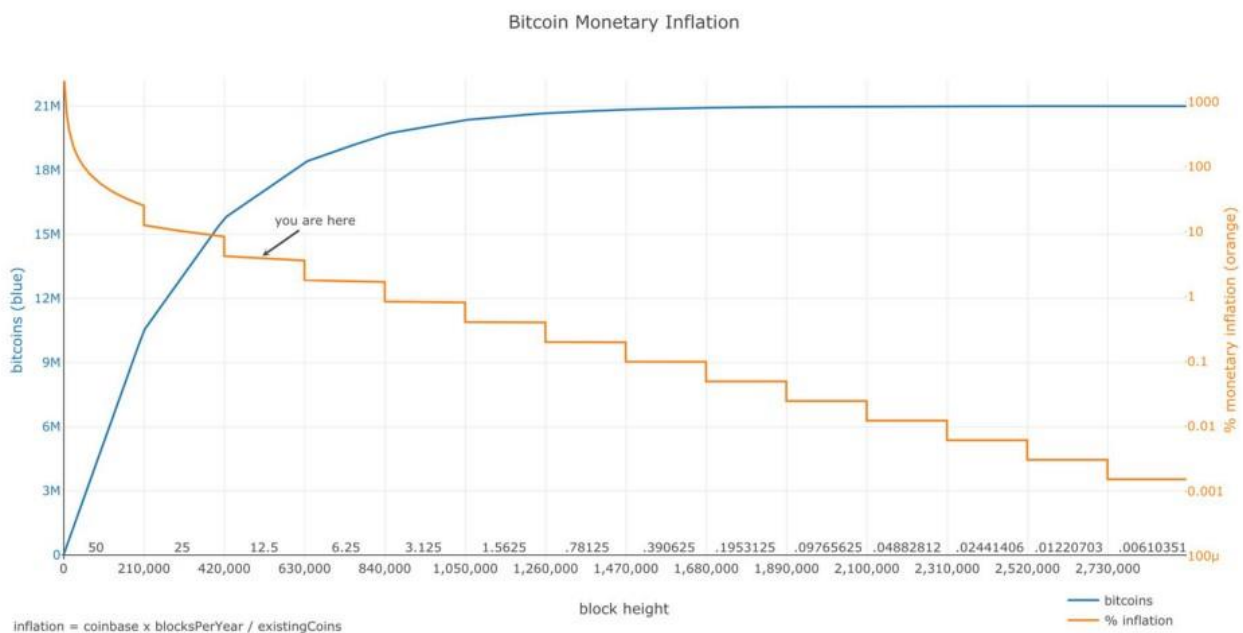
Stock-to-Flow and Value

The hypothesis in this study is that scarcity, as measured by SF, directly drives value. A look at the table above confirms that market values tend to be higher when SF is higher. Next step is to collect data and make a statistical model.
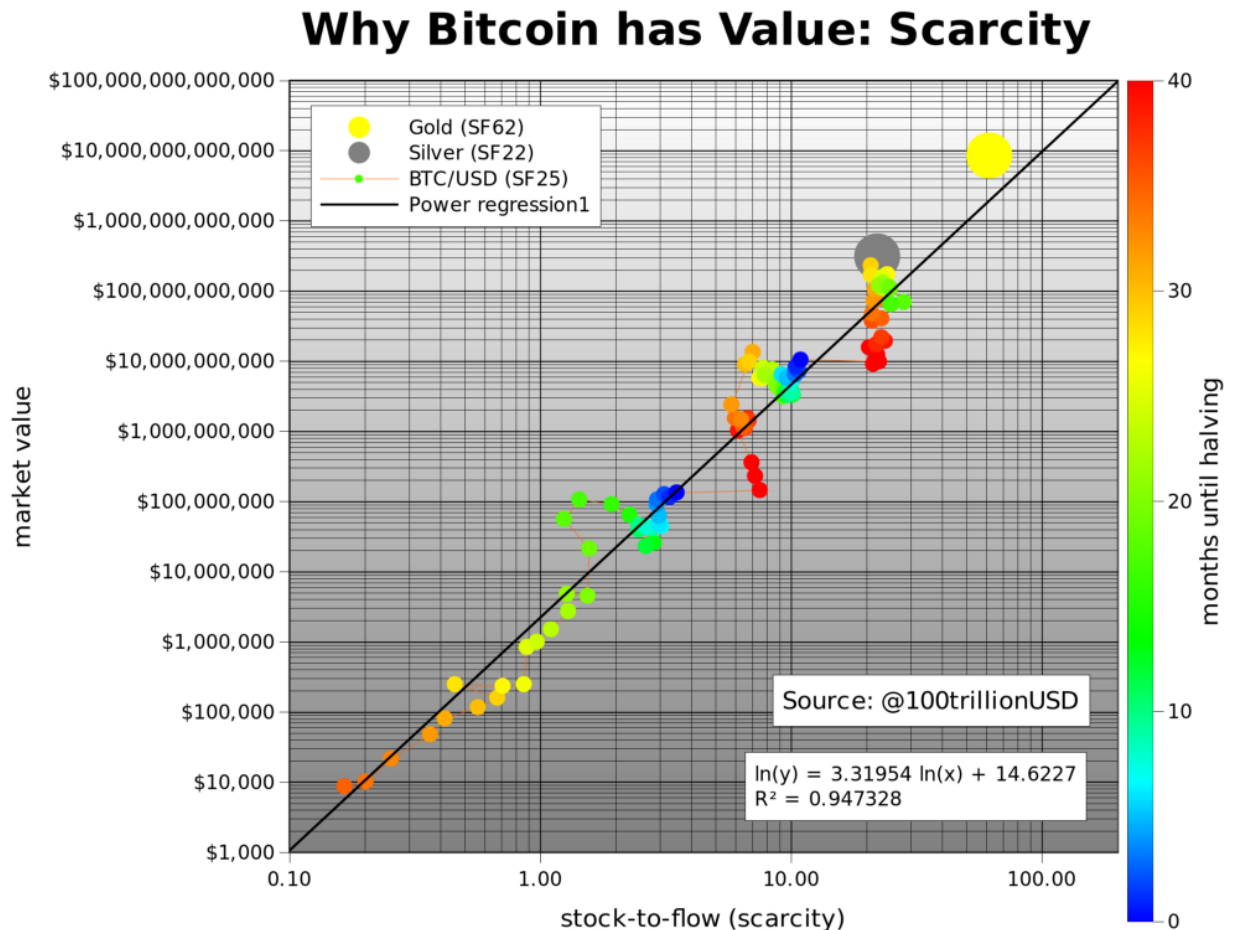
Data

I calculated bitcoin's monthly SF and value from Dec 2009 to Feb 2019 (111 data points in total). Number of blocks per month can be directly queried from the bitcoin blockchain with Python/RPC/bitcoind. Actual number of blocks differs quite a bit from the theoretical number, because blocks are not produced exactly every 10 minutes (e.g. in the first year 2009 there were significantly less blocks). With the number of blocks per month and known block subsidy, you can calculate flow and stock. I corrected for lost coins by arbitrarily disregarding the first million coins (7 months) in the SF calculation. More accurate adjusting for lost coins will be a subject for future research.

Bitcoin price data is available from different sources but starts at Jul 2010. I added the first known bitcoin prices (1$ for 1309 BTC Oct 2009, first quote of $0.003 on BitcoinMarket Mar 2010, 2 pizza's worth $41 for 10,000 BTC May 2010) and interpolated. Data archeology will be a subject for future research.

We already have the data points for gold (SF 62, market value $8.5trn) and silver (SF 22, market value $308bn), which I use as a benchmark.

Model

A first scatter plot of SF vs market value shows that it is better to use logarithmic values or axis for market value, because it spans 8 orders of magnitude (from $10,000 to $100bn). Using logarithmic values or axis for SF as well reveals a nice linear relationship between ln(SF) and ln(market value). Note that I use natural logarithm (ln with base e) and not common logarithm (log with base 10), which would yield similar results.

Why Bitcoin has Value: Scarcity

Charts made with gnuplot and gnumerics

Fitting a linear regression to the data confirms what can be seen with the naked eye: a statistically significant relationship between SF and market value (95% R2, significance of F 2.3E-17, p-Value of slope 2.3E-17). The likelihood that the relationship between SF and market value is caused by chance is close to zero. Of course other factors also impact price, regulation, hacks and other news, that is why R2 is not 100% (and not all dots are on the straight black line). However, the dominant driving factor seems to be scarcity / SF.

What is very interesting is that gold and silver, which are totally different markets, are in line with the bitcoin model values for SF. This gives extra confidence in the model. Note that at the peak of the bull market in Dec 2017 bitcoin SF was 22 and bitcoin market value was $230bn, very close to silver.

Because halvings have such a big impact on SF, I put months until the next halving as a color overlay in the chart. Dark blue is the halving month, and red is just after the halving. Next halving is May 2020. Current SF of 25 will double to 50, very close to gold (SF 62).

The predicted market value for bitcoin after May 2020 halving is $1trn, which translates in a bitcoin price of $55,000. That is quite spectacular. I guess time will tell and we will probably know one or two years after the halving, in 2020 or 2021. A great out of sample test of this hypothesis and model.

People ask me where all the money needed for $1trn bitcoin market value would come from? My answer: silver, gold, countries with negative interest rate (Europe, Japan, US soon), countries with predatory governments (Venezuela, China, Iran, Turkey etc), billionaires and millionaires hedging against quantitative easing (QE), and institutional investors discovering the best performing asset of last 10 yrs.

We can also model bitcoin price directly with SF. The formula of course has different parameters, but the result is the same, 95% R2 and a predicted bitcoin price of $55,000 with SF 50 after May 2020 halving.

I plotted bitcoin model price based on SF (black) and actual bitcoin price over time, with the number of blocks as color overlay.

Bitcoin and Number of Blocks per Month
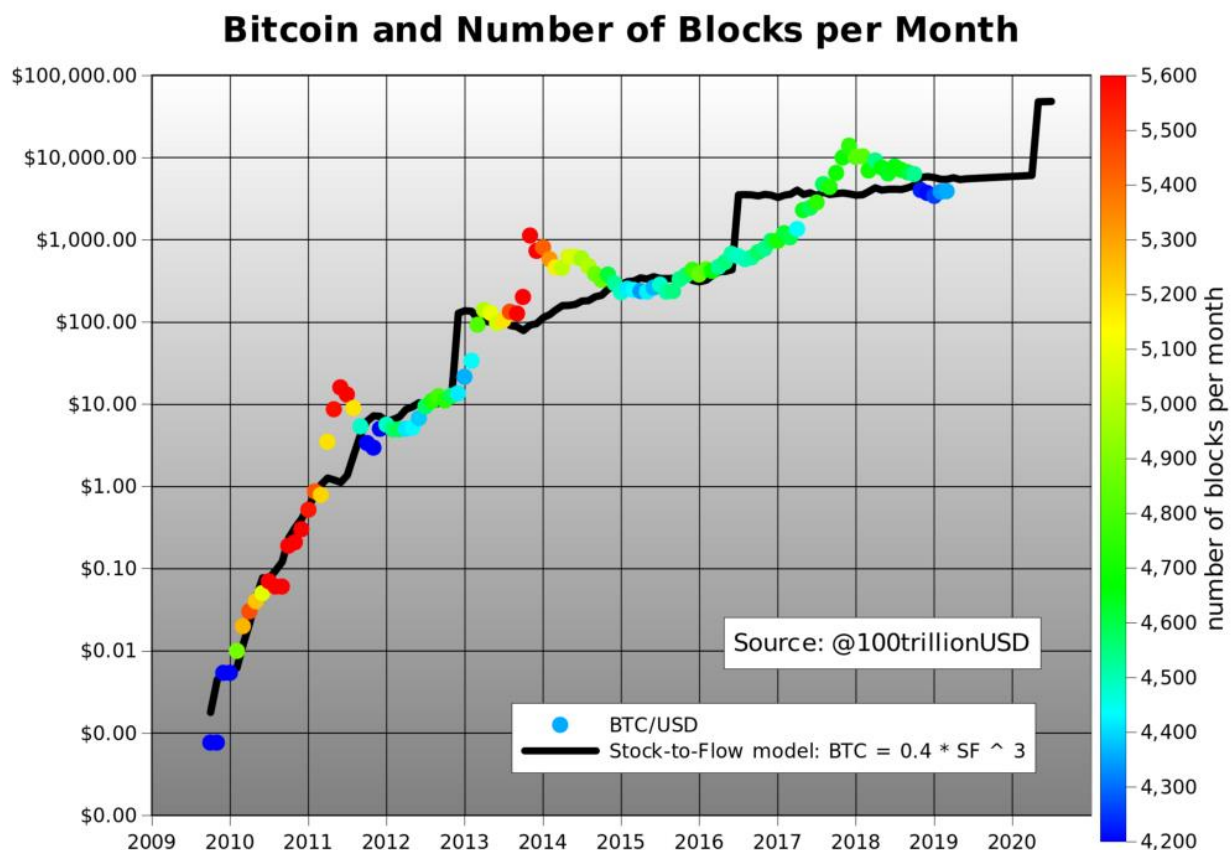
Charts made with gnuplot and gnumerics

Note the goodness of fit, especially the almost immediate price adjustment after Nov 2012 halving. Adjustment after Jun 2016 halving was much slower, possibly due to Ethereum competition and the DAO hack. Also, you see less blocks per month

(blue) in the first year 2009 and during downward difficulty adjustments end2011, mid2015 and end2018. Introduction of GPU miners in 2010-2011 and ASIC miners in 2013 resulted in more blocks per month (red).

Power Laws and Fractals

Also very interesting is that there is indication of a power law relationship.

The linear regression function: ln(market value) = 3.3 * ln(SF)+14.6

.. can be written as a power law function: market value = exp(14.6) * SF ^ 3.3

Power laws are scarce, you don't find them very often. The possibility of a power law with 95% R2 over 8 orders of magnitude, adds confidence that the main driver of bitcoin value is correctly captured with SF.

A power law is a relationship in which a relative change in one quantity gives rise to a proportional relative change in the other quantity, independent of the initial size of those quantities. [6]. Every halving, bitcoin SF doubles and market value increases 10x, this is a constant factor. See appendix for some famous power law examples.

Power laws are interesting because they reveal an underlying regularity in the properties of seemingly random complex systems. Complex systems usually have properties where changes between phenomena at different scales are independent of the scales we are looking at. The picture we take at one scale is therefore similar in some way to the picture we take at another scale. This self-similar property underlies power law relationships . We see this in Bitcoin too: 2011, 2014 and 2018 crashes look very similar (all have -80% dips) but on totally different scales (resp. $10, $1000, $10,000), if you don't use log scales, you will not see it. Scale in-variance and self-similarity has a link with fractals. In fact, parameter 3.3 in the power law function above is the 'fractal dimension'. For more information on fractals see the famous length of coastlines study [7]. Power laws and fractals in bitcoin will be a subject for future research.

Conclusion

Bitcoin is the first scarce digital object the world has ever seen, it is scarce like silver & gold, and can be sent over the internet, radio, satellite etc.

Surely this digital scarcity has value. But how much? In this article I quantify scarcity using stock-to-flow, and use stock-to-flow to model bitcoin's value.

A statistically significant relationship between stock-to-flow and market value exists. The likelihood that the relationship between stock-to-flow and market value is caused by chance is close to zero.

Adding confidence in the model:

- Gold and silver, which are totally different markets, are in line with the bitcoin model values for SF.
- There is indication of a power law relationship.

The model predicts a bitcoin market value of $1trn after next halving in May 2020, which translates in a bitcoin price of $55,000.

References

[1] https://bitcoin.org/bitcoin.pdf—Satoshi Nakamoto, 2008

[2] https://bitcointalk.org/index.php?topic=583.msg11405#msg11405—Satoshi Nakamoto, 2010

[3] https://unenumerated.blogspot.com/2005/10/antiques-time-gold-and-bit-gold.html—Nick Szabo, 2008

[4] https://unenumerated.blogspot.com/2005/12/bit-gold.html—Nick Szabo, 2008

[5] The Bitcoin Standard: The Decentralized Alternative to Central Banking—Saifedean Ammous, 2018

[6] https://necsi.edu/power-law

[7] http://fractalfoundation.org/OFC/OFC-10-4.html

Appendix —Power Law Examples

Kepler (planets)
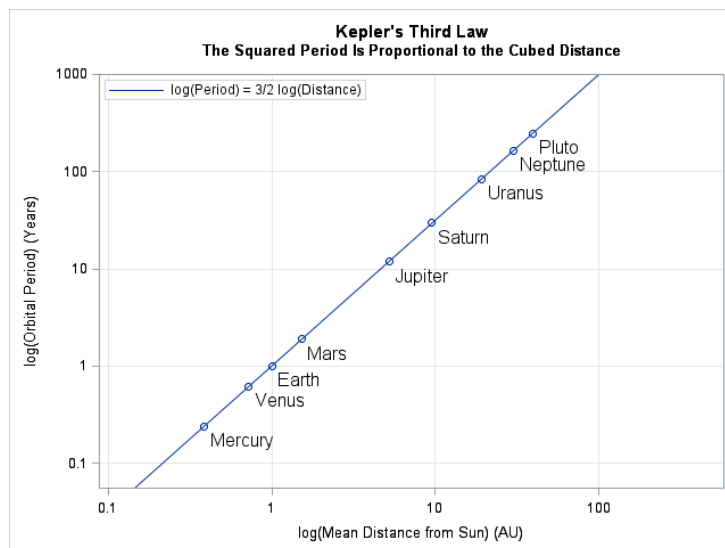
Richter (earthquakes)

Gutenberg-Richter law of earthquake magnitudes

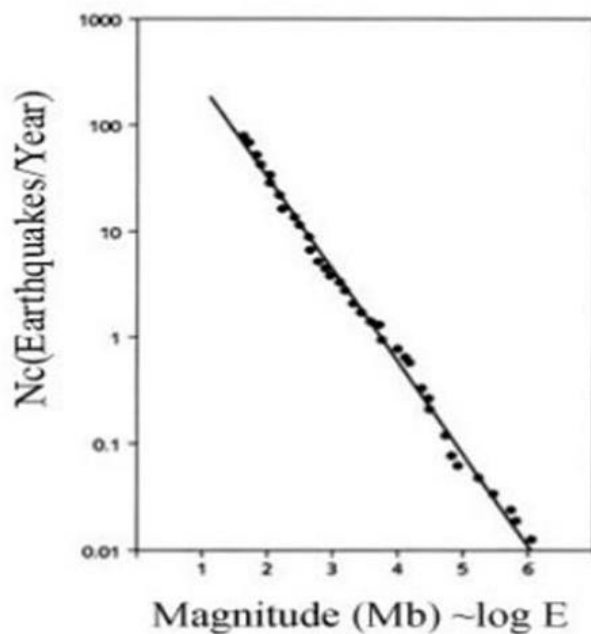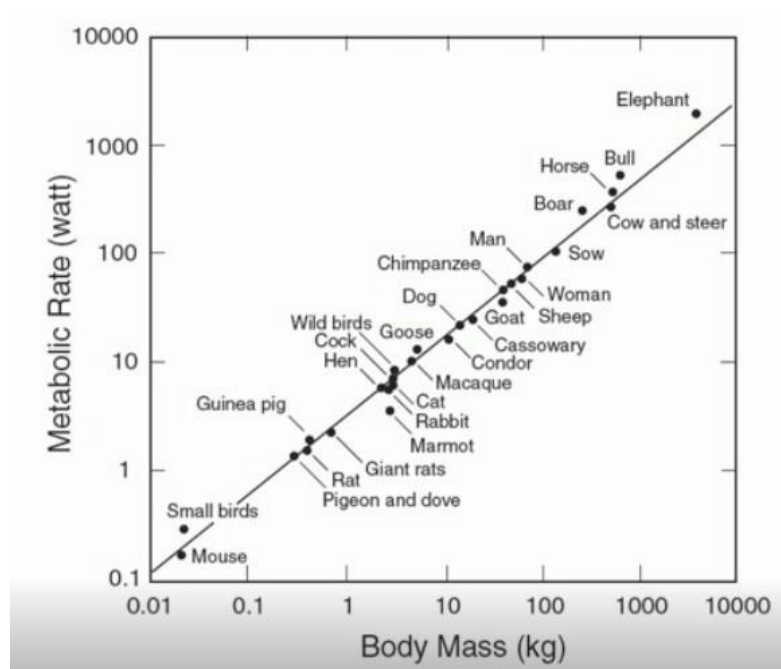By: Bak

Kleiber (animals)

The Ethics of Money and Bitcoin

By Nicolas Dorier

Posted March 30, 2019

When I am bored coding, I read about coding. But once in a while, I read something else, and Rothbard is often a good bet to not bore me.

For those who never read Rothbard, his thoughts are always derived logically from very simple premises, it is almost like following a mathematical demonstration, but one that you can actually understand. It is hard to disagree with him as you need to find a flaw in his logical reasoning or you need to dismiss his premises. The conclusions of his thoughts are often associated as "radical libertarianism", to which he is able to convince anybody open to strict logical reasoning.

I don't consider myself radical libertarian, but neither could I find any flaw in his arguments in the books I read from him. If I read again, I will eventually end up radical libertarian.

Anyway, recently, I peeked up the ethics of liberty from Rothbard.

I can't explain his idea better than himself, so if you are interested, read him directly, not me. He spent way more time than I did shaping up his reasoning than me spending time writing this blog post.

Loose definition of Ethics

Ethics is like a set of value which define if a behavior can be considered immoral. There are many ethics around there, from religion or philosophy, which can contradict each other.

A moral dilemma is when you hold conflicting values where in a given situation, all actions are immoral. This can lead an individual to madness or to abandon his values to save his sanity.

A religion ethic is in generally non conflicting, as any conflict will result to either the madness of the believers, or to the destruction of its values, or a split, in short, the disappearance of this ethic. Religions, surviving for a long time, has shaped themselves and built stronger set of ethics over time. (Religions are Lindy)

In the bitcoin world, some are shocked by the fundamentalist of catholic christian bitcoin developer Luke-Jr, but this all come down to religion having strong ethics in the sense that any particular behavior can be considered clear-cut as immoral or not.

Human Nature

So Rothbard, starts defining human nature.

In everyday life, when people refers to "human nature" it is often in a pejorative way of pointing out greed, selfishness and long term unsustainable of current technological development.

Religions refer to human nature as something arbitrarily defined by a superior non-human entity.

All those definitions contradict one another and are always subjective to the person preaching it. A christian will have a different view on what human nature is than a Buddhist, Atheist or Agnostic.

Rothbard definition of human nature is objective in the sense that his definition does not change depending on what religion you are. This does not dismiss other definitions, this is just the definition of Human Nature Rothbard builds his ideas upon.

So how to define Human Nature in an absolute way? Rothbard states that human nature should be based on characteristic proper to humans.

Characteristics which only humans depend on for their survival as opposed to other species.

He claims that instead of relying on instincts, the proper characteristic of human is the use of reason. We aim at a specific goal with our inalienable free will (as opposed to instinct), then reason lead our actions to find the most efficient way to reach it. It turns out that the most efficient way is often by the help of other fellow humans and by making tools, as our body is not self sufficient for surviving (no fur, no built-in poisonous fang etc…). This lead to specialization of skills and the need of being a social creature. Rothbard contrasts the inalienable free will with the alienable labor service one can render. The fact that the fruit of our labor is voluntarily alienable make social cooperation possible. Our reason lead us to cooperate for attaining our goal in the most efficient way. The result of our civilization is just the natural outcome of those principles unique to human.

Other animals have some degree of social skills, but they don't have the free will to aim on a specific goal and to use their fellows as a mean to such end. They select goal by instinct, and reach the goal by themselves.

In a nutshell, the nature of human is selection of a goal by inalienable free will then action guided by reason to reach it in the most efficient way. This lead to cooperate with other fellow and to the division of labor.

Human Ethics, the case of slavery

So human ethics is then considered as a set of values which do not oppose to Human Nature as defined above. In this ethic, everything that oppose the nature of human is deemed immoral, everything that help human nature is deemed moral.

Let's just see how to judge slavery in such ethic:

- It is clear that both slave and slave master follows Human Nature as defined above, so one can't define the slave as non-human.
- Slavery is when the fruit of labor of the slave's labor is being taken with compulsion by the slave master.

Now, let's have a thought experience in a imagine a world where everybody is slave and slave master.

- Nobody can reap the fruit of his own labor,
- Everybody can take by force another person's labor

It is easy to see that in such situation, labor will eventually cease to exists and human specie disappear. Even if one is hungry to death and reap an apple, this apple will be confiscated by somebody else, so he can only chose to die, or wait that somebody else take an apple, but this somebody else will die as he can't eat the apple. Eventually everybody will die, the last of them can eat all the apples but will not be able to reproduce and will die from old age. Thus, slavery is against human nature, and thus it is immoral by Human Ethic.

Rothbard analyses way more situation than this in a completely logical way, I can't do him any justice, I just wanted to tell this example so you get a taste of his strictly logical reasoning.

If you want to defend slavery you need to reject human ethic (replacing it with another ethic going against human nature) or find a flaw in the reasoning. This is typically the Rothbardian way of defending any position he takes.

The Nature of Money

I came under the realization that Rothbard's reflection about the nature of human can be applied to Bitcoin such that we can develop an ethic of bitcoin rooted in the objective Nature of Bitcoin.

In the bitcoin community, we likely already know the Nature of Money kind of well. And there are books talking about it so we won't be long.

The nature of money, what distinguish it from any other things, is that **money can be easily exchanged at any time in future against another good by another party, where, the specific time, the future good and the other party don't need to be known in advance**. This is the nature of money.

The less you know about which future good it will be, when the future exchange will happen and which party it will be, the more money is needed. This is why in uncertain time people prefers saving.

Some characteristic of money, are:

- Durability

If money was not durable, it would worthless when you want to exchange, non durable money is against the nature of Money.

- Fungibility

If money was not fungible, you would be unable to know whether you will be able to exchange it in the future, and so unable to value it, so non fungible money is against Money Nature.

- Portability

If money was not portable, you can't exchange it, which goes against the nature of Money. Rai Stones seems to go against this idea, as Rai stones were not moving, instead ownership was orally passed by, but this is quite similar to gold being stuck in a vault and exchanging paper claims instead of the actual gold. The money is not the gold or the Rai stone, but the paper or oral claim.

Even if we do claim that the stone was the money, portability issues limit socially the parties who will accept it (only in possible in small tribes), thus being against the nature of money.

In the case of Bitcoin, **censorship** naturally refer to **portability**. If miners could censor you, it means they will prevent you to exchange your bitcoins.

- Divisibility

If money was not divisible, then it would severely limit the things to exchange with it to big purchases, thus being against the nature of money.

Bad divisibility limit the minimum (or maximum) value of the thing you can buy with it. Note, under this point of view, **bitcoin fees are actually a divisibility issue.**While bitcoin are in theory divisible to 8 decimals, practically the minimum value of thing you can buy with it is limited by the mining fee. (… in a world where lightning network does not exist)

- ~~Scarcity~~Scarcity

I think that scarcity is actually the same as **portability**. All resources are scarce. If oxygen was money, the problem would not be that we have too much oxygen, but that it would be impracticable to transfer. If bitcoin was not scarce the problem would be portability: A transaction would be infinitely big just representing the number of bitcoin you want to transfer.

- **Distributed**

This one is important but often overlooked. Imagine a money infinitely centralized such that suddenly I get 100% of the supply right in my hand (Practically speaking, an ICO). Now, you could speculate on this, and buy it from me, but speculation is not the nature of money.

Money can be exchanged in the future against another good by another party, where both the future good and the other party don't have to be known in advance

In speculation, you know which party you will resell to in advance (… Binance) and you know against what. (money, like Bitcoin or fiat) Thus, speculatively buying my ICO token does not make my ICO token money.

However, gold is widely geographically distributed, thus people from different background could somewhat agree on its value. Note that fiat money have a distribution issue which limit where it can be accepted.

Because the only reason why you would buy an asset I own 100% is for speculative purpose, you can see how non-distributed money goes against the nature of money. As far as distribution is concerned, there is a spectrum between me doing an ICO and gold. Bitcoin is actually very distributed as the source of renewable energy (which are the cheapest form of energy for mining) are distributed.

- **Defensibility**

Somehow, I never saw this one mentioned anywhere else. But it is easy to see that a money which can't be defended would be immediately stolen, and thus completely useless as money.

Bitcoin is the most defensible form of money as it requires very few resource to protect even a large amount from any kind of attacker. (included nation states) What we call privacy is nothing but an attempt at improving **defensibility**.

The Ethic of Bitcoin

Bitcoin's nature is money's nature. Certainly its design has been created to fit this purpose, and it is widely accepted in the context of money.

Lot's of people accept bitcoin because they know they can exchange it at an unknown future date, with an unknown party, against an unknown future good.

So when we talk about the Nature of Bitcoin, we really talk about the Nature of Money. As if Bitcoin could not be money by any characteristic of money infinitely abused, it would cease to exist.

In Bitcoin we talk:

- Mining fee instead of Divisibility
- Censorship instead of Portability
- Privacy and self-validation instead of Defensibility
- Fixed supply instead of Durability

But those terms are really the two faces of the same coin.

Thus, we can declare objectively if an action is immoral for Bitcoin or not. By **We**, I don't want to give the impression of superior value that must be shared by a community.

I mean **We** in the neutral sense of: If you agree with me about what is the Nature of Bitcoin, and that the Ethic of Bitcoin are values which can logically prove that an action is immoral when it goes against the Nature of Bitcoin.

I don't really mind if you personally want to follow such ethic or not, as you are free to hold onto whatever value you want. But as far as Bitcoin is concerned, I will judge your action against this ethic.

With this ethic, you can judge what is "bad for Bitcoin" or "good for Bitcoin" without any subjectivity involved.

Bitcoin can be immoral for you because it conflicts with your values, but this is a separate issue.

Any development on Bitcoin which hurt its nature as Money, or hurt free expatriation, or the enforcement of property by software should be objectively considered **immoral**.

The case of Lightning Network

So now we are equipped with values which objectively allow us to debate whether a technology is good or bad for Bitcoin, I start with the Lightning Network.

As I talked about in The Nature of Money, I consider that mining fee in Bitcoin is bad for the **divisibility** of Bitcoin by making it unsuitable to use for low value payments. Not only this, but Bitcoin, because of its pseudo anonymous nature, have various hostile forces trying to decrease its **fungibility**.

In this sense, Lightning increases **the divisibility** of Bitcoin by decreasing the minimum value of good Bitcoin can be exchanged against.

Secondly, Bitcoins sent through the lightning network are completely **fungible** as it is impossible to know with on-chain information the source of the payment that someone receive.

Thus lightning is virtuous. Chain analysis companies are bound to lose this battle and will become obsolete.

The case of trusting block validation to miners

Needless to say, if there was no miner, we can't preserve the "free expatriation" characteristic of Bitcoin. So miners are vital to the Nature of Bitcoin.

Some people assert that we should just follow whatever rule miners decide.

But then, nothing would guarantee that such miners does not act immorally against the Nature of Bitcoin. History shows again and again that whenever a social group take control over the rules on money, they behave against the Nature of Money via debasing, or inflation (impacting **durability**of money).

Miners are nothing but a social group, we should assume history will repeat itself, thus assume they will go against the Nature of Money and thus trusting them is **immoral**.

The case of Bigger Blocks and inflation

A point was made for Bitcoin to have bigger blocks. Since mining fees impact **the divisibility** of Bitcoin, some people defend that it is virtuous to decrease the fees by increasing the block size.

Surely, a world where mining fees are absolutely zero can work for a while. It already did in the past. This can works thanks to inflation which keep miners mining. But if you want zero fee, you also need bigger block as the space is eventually too scarce to accommodate every users.

So let's start by analyzing the case of adding inflation to Bitcoin.

If inflation was 99% per year, it is easy to see that inflation is nothing but an attack on the **durability** of money.

Thus actions attempting to add inflation should be considered **immoral**. We can't say that **durability** (no inflation) is objectively better than **divisibility** (low fees) but we can say that the particular action of raising inflation is an attack on the Nature of Money by impacting **durability** negatively.

In the same way, assume an altcoin becomes money like Bitcoin one day and has inflation. Is dropping inflation immoral? And it actually is! Either this inflation is balanced by higher fees and **divisibility** is damaged. Or miners get less revenue and we increase risks of immoral money control if they collude. We can't quantify it, but such ethical analysis does not require quantitative analysis, just the fact than one action damage some property of the Nature of Bitcoin is enough to consider it immoral.

Under this notion, needless to say that a central bank consistently playing with the inflation rate is completely immoral as it goes against the Nature of Money.

However, inflation is not enough for keeping fee to zero. You also need to increase the block space, let's analyze this.

The need for cheap outsourced durable storage is unlimited. So there is no fixed size which will be good enough at all time high to please everybody. Let's take the extreme case of unlimited block size: We don't have to make complicated model to understand that this would end up with having one single giant database somewhere on the planet, and then will hurt the Nature of Bitcoin by impacting **defensibility**, as this giant database owners can now confiscate bitcoins or censor them.

If an unlimited block size increase hurt the very nature of Bitcoin by hurting the free expatriation characteristic of Bitcoin, then it must be considered immoral.

Obviously, a small increase will not have the same impact as an unlimited increase, but still, it impacts the very Nature of Bitcoin, it should be considered immoral.

This mean that **the block size bump introduced by Segwit was immoral and Luke-Jr have been 100% right on this**. (Note that myself I did not opposed to it, this was a mistake)

But what about dropping the block size? It would be as much immoral as it would impact **divisibility** negatively by increasing the fees.

Not doing anything is also an action by itself, but an action which does not modify the Nature of Bitcoin and thus can't be claimed immoral.

People claiming that the Nature of Bitcoin changed by itself because fee became expensive and caused harm to their business are only admitting they failed to understand the Nature of Bitcoin.

The case of miners mining small blocks

Miners are free to mine smaller blocks if they want. This would effectively mean, as we saw, that the fee would increase and thus **divisibility** would be impacted.

Let's take the extreme case of miners mining only one transaction per block. It seems clear that in such case, the **divisibility** of bitcoin would be so damaged that it would cease to be a useful form of money. This mean that the miner would be **immoral** despite it being their right as per the Bitcoin protocol.

The case of SPV wallets

I recently wrote about why <u>Neutrino is dangerous for my self sovereignty</u>.

BIP37 (Bloom filters) are actually quite neutral. There is a legit use case, which is low bandwidth SPV wallet paired to your own full node.

On the other hand, Neutrino is only useful for delegating block validation to somebody else. Using Neutrino to pair to your own node does not make sense as BIP37 is way more efficient.

If 100% of users where delegating validation to somebody else, then again, Bitcoin's **defensibility** would be hurted, as this party would be able to censor and steal your coins. That said, even without Neutrino, this could already be the case with centralized block explorers, so Neutrino itself is not preventing this situation to become the norm.

Actually, some people made the case that it improve the Nature of Bitcoin because instead of having a bunch of centralized block explorer, we will have more people serving their own family, friends or community because setting up a node supporting Neutrino is easier than setting up a block explorer. This argument actually convinced me clearly that Neutrino is not immoral.

However, things are different for SPV wallets following Proof of Work.

If 100% of users of Bitcoin were following proof of work, then collusion of miners like happened in B2X would prove fatal to Bitcoin, because as we saw, history tell us that any social group in control of money ends up going against the Nature of Money. A world run like the FED, but with anonymous miners instead.

Any SPV wallets following proof of work must be treated as immoral. Giving to users the ability to follow a specific node instead of the most proof of work chain does not, in any case, save them. A murderer should be considered immoral even if he saved a kitten.

The case of Schnorr signature

Schnorr signature are an improvement to Bitcoin which allow a bunch of amazing feature like signature aggregation which would basically cut down dramatically the size of transactions in some situation.

Unlike a block size increase which would hurt the "free expatriation" characteristic of Bitcoin, this is not the case of this feature whose main effect would be to **improve divisibility** of Bitcoin.

Some people might protest saying that any change to Bitcoin is a risk to ruin the Nature of Bitcoin by mistake. Such concern should not be taken seriously given that:

1. Changes can be reviewed so you can be personally sure the code does what it says
2. Any mistake, while embarrassing and potentially damaging to the reputation of Bitcoin, are fixable.

Damaging the reputation of Bitcoin is not immoral, as hurting the reputation does not impact the Nature of Bitcoin. Mt Gox damaged Bitcoin reputation, but I became Bitcoin developer since I understood that the Nature of Bitcoin was perfectly unscratched by this news. And so do all Bitcoin developers who were here before me, I don't have one example of any of them stopping working on Bitcoin because of Mt Gox.

Conclusion

I tried to make the case for ethical bitcoin development following the model that Rothbard is taking to define objective human ethics.

This approach to ethics is taking minimal agreed premises on what make Bitcoin special, in other words, what is the Nature of Bitcoin, and define anything that goes against it as **immoral**.

There should be no gray area when judging actions people have on Bitcoin. Most of actions have no particular effect on the Nature of Bitcoin and are harmless, but when one action can be in anyway affecting its nature, this must be pointed out and treated as such. Subjective values such as "Divisibility is better than Fungibility" are unacceptable justification. If divisibility is hurt in favor of fungibility or vis versa, such action should be considered immoral.

If the Ethic of Bitcoin is conflicting with your own ethic, then you have no other way than to declare Bitcoin itself immoral.

Some cases can be harder to draw a line, but in any case can be discussed and debated in an objective way. I personally thought Neutrino was fundamentally immoral, I recognize that there is moral case for it as long as the wallet don't follow proof of work. Maybe some cases I discussed above might be discussed in the same way.

Schnorr Signatures & The Inevitability of Privacy in Bitcoin

By Lucas Nuzzi

Posted March 13, 2019
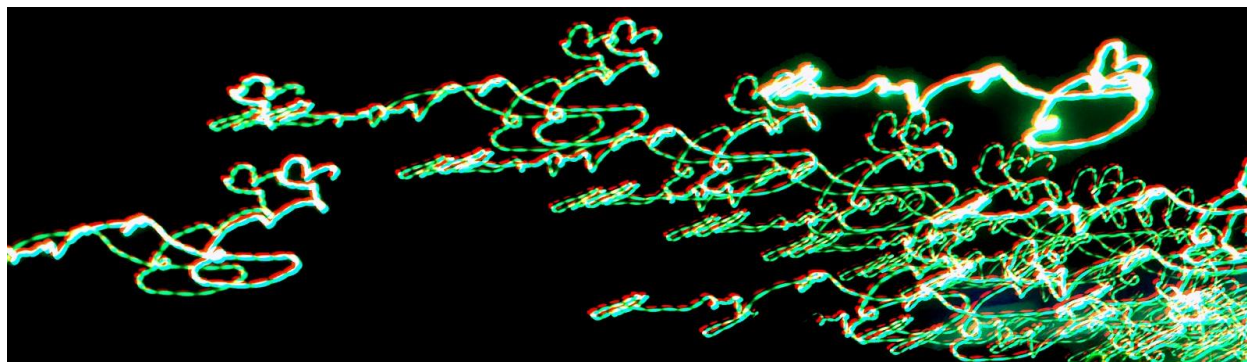
Schnorr Signatures in the void.

Thanks to Pieter Wuille for generously providing feedback on this article and educating me on Schnorr. Since his review, I've made lots of changes to simplify key concepts presented here. *Any errors & opinions found herein are my own*

Digital signatures are the backbone of online sovereignty. The advent of Public-key cryptography in 1976 paved the way for the creation of a global medium of communication, the *internet*, and an entirely new form of money, *bitcoin*. While the fundamental properties of public key cryptography have not changed much since then, there are now dozens of open-source digital signature schemes available in the cryptographer's toolbox.

When Satoshi Nakamoto began to work on Bitcoin, one of the key design choices to be considered was *which* signature scheme to use in this open, permissionless financial system. The requirements were clear; Satoshi needed an algorithm that was widely-used, well-understood, sufficiently secure, lightweight, and, most importantly, open-source. Out of all options available at the time, he went with the one that fit that criteria the most: the Elliptic Curve Digital Signature Algorithm, or ECDSA.

Back then, ECDSA was natively supported by OpenSSL, a set of open-source encryption tools developed by cypherpunk veterans to improve the privacy of online communications. Relative to other popular schemes, ECDSA carried the benefits of leaner computational requirements and shorter key lengths; useful attributes for a digital form of money. At the same time, it also provided a

proportionate level of security to schemes like RSA: a 256-bit ECDSA key, for example, has equivalent security to a 3,072-bit RSA key, but it is a fraction of its size.

The hard work of Pieter Wuille and others on an improved curve (*as in Elliptic Curve*) called secp256k1 made Bitcoin's ECDSA faster and more efficient. However, there are still inherent deficiencies in ECDSA that justify replacing it all along. After a couple of years of research and experimentation, a new signature scheme is set to increase the privacy and efficiency of Bitcoin transactions: the Schnorr Digital Signature Scheme.

In this article, I provide a general overview of the multiple implementations of Schnorr signatures and their corresponding benefits. Then, I explore MuSig, a new multi-signature standard that serves as a building block for novel Bitcoin technologies like Taproot. Lastly, I describe how the fully realized version of Schnorr can break the heuristics used in blockchain analysis and, at the same time, help develop a strong fee market in Bitcoin's main layer.

THE RISE OF SCHNORR SIGNATURES

Even though the Schnorr digital signature scheme carries many benefits over ECDSA, it is certainly not new. It was invented by Claus-Peter Schnorr, a German cryptographer and academic, while he was a professor and researcher at the University of Frankfurt in the 1980s. His proposed signature scheme was an amalgamation of the research and work of David Chaum, Taher ElGamal, Amos Fiat and Adi Shamir. Nevertheless, before publishing it, Claus Schnorr filed multiple patents for his newly invented scheme, which, for years, prevented its _direct _use.

Interestingly enough, ECDSA's predecessor, DSA, was a hybrid of the ElGamal and Schnorr schemes that was solely devised to circumvent Claus Schnorr's patents. In fact, only two months after Schnorr's U.S. patent was issued, DSA's progenitor, the U.S. National Institute of Standards and Technology (NIST), also filed a patent for its workaround. And here's a bit of prime cypherpunk history: after that happened, Claus Schnorr became very defensive of his patents, and directly responded to his critics in the Coderpunks mailing list; an offshoot of the original Cypherpunks mailing list. His responses can be read here and here. An internal NIST memo describing _Patent Issues _can also be found here.

In 2008, nearly two decades after the introduction of the Schnorr signature scheme, Claus Schnorr's patent expired. Coincidentally, 2008 was also the year our favorite cypherpunk, Satoshi Nakamoto, was implementing Bitcoin. Even though Schnorr signatures could have been used at the time, they were not standardized nor widely used, which was probably Satoshi's motivation to go with ECDSA instead. Although frequently described as _atrocious _by cryptographers and

mathematicians alike, ECDSA was (and still is) widely used and it provided safer option for Bitcoin back then.

SCHNORR ON BITCOIN

Fast forward another decade and Schnorr's scheme is much less esoteric today, with standardized implementations like ed25519 becoming a popular option for some *altcoins*. Informal talks about potentially implementing Schnorr on Bitcoin date back to this 2014 BitcoinTalk thread, but a proposal was only formalized after years of research and experimentation, when Pieter Wuille wrote the Schnorr BIP. This draft BIP describes the specifications and technicalities of a potential Schnorr implementation, which would carry the following benefits over ECDSA:

· Security proof: The security of Schnorr signatures is easily provable when a sufficiently random hash function (random oracle model) is used and the elliptic curve discrete logarithm problem (ECDLP) used in the signature is sufficiently hard. Such a proof does not exist for ECDSA.

· Non-malleability: ECDSA signatures are inherently malleable, which may enable a third party without access to the private key to alter an existing valid signature and double-spend funds. This issue was formally discussed in BIP62. In comparison, Schnorr signatures are provably non-malleable.

· Linearity: Schnorr signatures have the remarkable property that multiple parties can collaborate to produce a signature that is valid for the sum of their public keys. This is the building block for various higher-level constructions that improve efficiency and privacy, such as multi-signatures and other smart contracts.

The security proofs provided by Schnorr, as well as its non-malleability guarantees, offer clear benefits over ECDSA. A soft-fork could be justified solely on the basis of these two benefits. However, it is Schnorr's *Linearity* property that is particularly exciting. In essence, this enables multiple signers in a multi-signature (multisig) transaction to combine their public keys into an aggregated key that represents the group; a property that has been called key aggregation.

While the ability to fuse keys may sound trivial, the benefits of key aggregation should not be underestimated. Since multisigs are not natively supported by ECDSA, they had to be implemented in Bitcoin via a standardized smart contract (*yes, Bitcoin has smart contracts too*) called Pay-to-ScriptHash (P2SH). This enables users to add spend conditions called _encumbrances _to specify how funds can be spent e.g. "only unlock balance if both Alice and Bob sign this message."

The first problem with P2SH is that it requires knowledge of the public keys of all signers participating in the multisig, which is not an efficient system. Aggregating

these keys would allow for more efficient validation as only one key needs to be verified by the network, rather than _n _keys. That also means less footprint on the blockchain, lower transaction costs, and improved bandwidth.

The second problem with P2SH is that it offers very little privacy guarantees. As specified by BIP 13, P2SH transactions require different addresses that begin with the number 3. This allows *blockchain observers _to not only identify all P2SH transactions in the network, but also pin point the identities _within* the multisig:
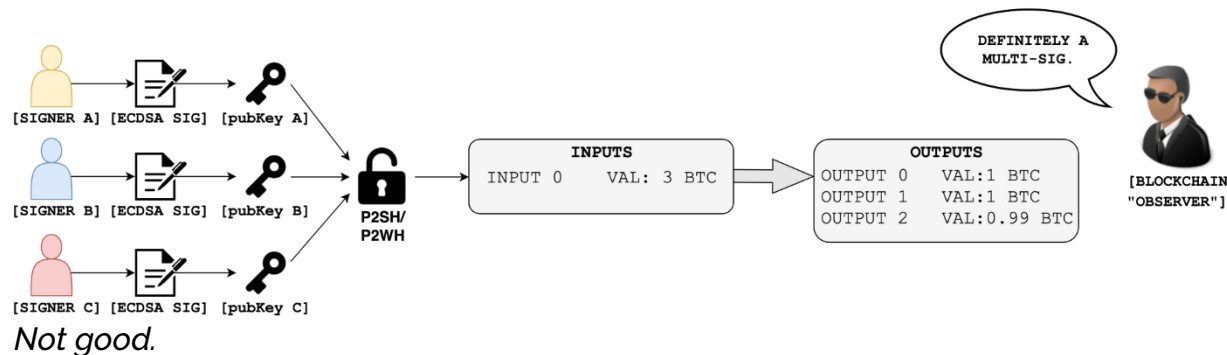
Not good.

In the example above, the network would be aware of (1) the existence of a multisig transaction, (2) how many signers it is comprised of and (3) who the signers are. Not good for operational security, especially for use cases like 2FA. Not good for privacy.

Key aggregation, on the other hand, allows signers to remain anonymous and does not compromise operational security by revealing the keys required to unlock a balance. Most importantly, key aggregation makes it so that multisigs can become indistinguishable from regular transactions:

Good.
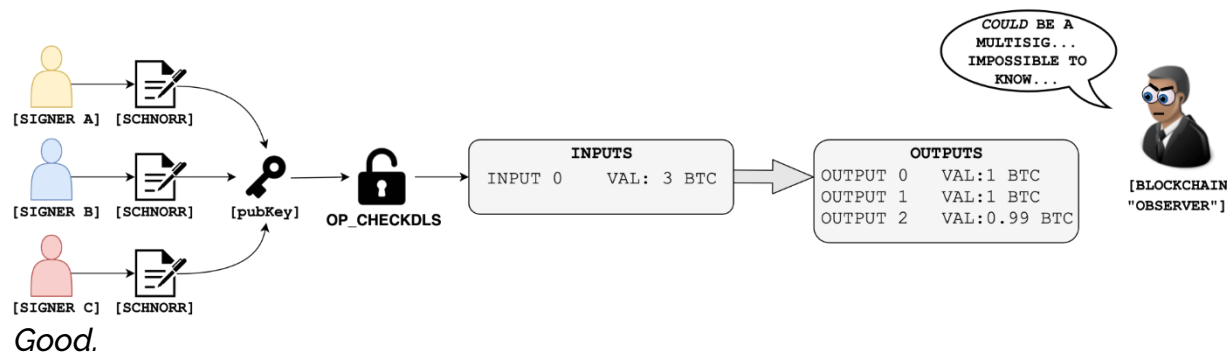
The first iteration of Schnorr in Bitcoin will retire the OP_CHECKSIG and OP_CHECKMULTISIG family of opcodes currently used with ECDSA in favor of a new class that has been called OP_CHECKDLS. Without going into too much detail, DLS stands for Discrete Log Signature and it allows signatures to be verified more efficiently with less opcodes.

Back in early 2018, Gregory Maxwell, Andrew Poelstra, Yannick Seurin, and Pieter Wuille published a white paper on a new Schnorr-based multi-signature scheme called MuSig. Since the publication of MuSig, they have been working hard to translate the proposed multisig scheme into usable code.

One of the most interesting things about MuSig in the context of key aggregation is the possibility for the creation of private smart contracts outside of the blockchain. In essence, MuSig enables multisig participants to attach encumberances to the aggregated keys *off-chain*, which does not require Bitcoin's consensus rules to be aware of it.

In December 2018, Anthony Towns was the first Core developer to make a semi- formalized proposal for the activation of Schnorr, which was posted on the bitcoin-dev mailing list. I expect more conversations about a potential softfork to come up in the following months.

To summarize: the first iteration of MuSig in Bitcoin will natively support key aggregation, which can immediately (1) improve the privacy of multisigs, (2) increase the efficiency of transaction validation, (3) improve security by eliminating the inherent problems of ECDSA, and (4) enable smart contract solutions like Taproot, which I plan to cover soon.

But this is just the beginning.

CROSS-INPUT AGGREGATION: THE NEXT STEP FOR BITCOIN PRIVACY

As covered in the last section, key aggregation is an incredibly useful feature for multisigs that spend a single input. Since Bitcoin transactions usually have more than one input, future iterations of Schnorr can also be leveraged to create an interactive aggregate signature (IAS) scheme, where all inputs in a transaction are spent simultaneously with a single signature.

Once again, the interactions between signers occurs entirely off-chain, but now, a single signature can be used to spend all inputs of a transaction. Each input would still have its own public key, but spendable by a Schnorr IAS:
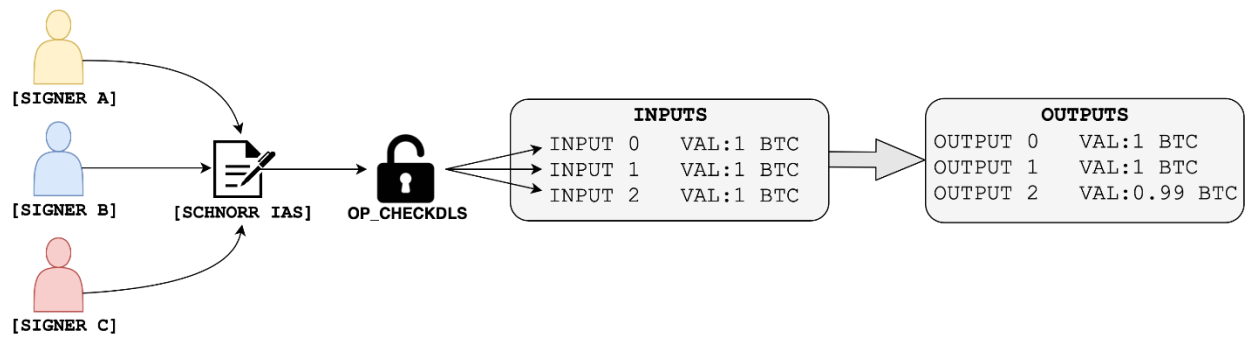
Greg Maxwell, Pieter Wuille, Anthony Towns and others have been working on an evolution of the Taproot smart contract scheme to facilitate this functionality. They call this scheme *Generalized Taproot*, or G'root, and it can make the transition from key aggregation to cross-input aggregation much easier in the future.

Like key aggregation, cross-input aggregation further increases the efficiency of Bitcoin transactions. But, most importantly, it may enable strong privacy-preserving mechanisms on Bitcoin's base layer.

One of the most exciting aspects of cross-input aggregation is the way it can improve CoinJoin transactions on Bitcoin. For context, CoinJoin is a privacy-preserving technique where multiple senders and receivers are combined within a single transactions. The goal is to make it difficult for a _blockchain observer _to link specific senders and receivers, thereby enabling the entities within the CoinJoin to claim plausible deniability.

This technique was originally proposed by Greg Maxwell on BitcoinTalk in 2013, and has since been offered through various services inlcuding JoinMarket, SharedCoin, ShufflePuff, DarkWallet and CoinShuffle. Variations of CoinJoin, such as the Chaumian CoinJoin scheme used in the Wasabi Wallet greatly improved upon the original model. However, since *anonymity loves company*, it still relies on a sufficiently large number of users to obfuscate their balances as well.

Another issue with CoinJoin today is the identifiability (and potential censoring) of the entire transaction type. Consider that the most used heuristic in blockchain analysis today is to follow specific inputs in order to determine if two or more addresses belong to the same entity. If Alice sent Bob 1.982723 BTC, for example, a *blockchain observer* could track the decimals of that specific input to map the *transaction graph*, or the historical breakdowns and changes of ownership of a UTXO.

To prevent that, CoinJoin implementations require common value denominations, whereby everyone within the CoinJoin sends the same amount. Users of the

Wasabi wallet, for example, send the same denomination of 0.1BTC in CoinJoin transactions of 100 participants. Although it is still hard to pinpoint the connection between specific senders and receivers, the *blockchain observer* can look for common denominations to identify that a CoinJoin took place and advise its client to censor *all* entities involved.

Cross-input aggregation can help with that, as it introduces an additional obfuscation mechanism at the protocol level. In essence, **cross-input aggregation can enable the construction of Schnorr-based CoinJoin transactions with *n _signers that look like regular, single-signer transactions to outsiders.** That may also enable CoinJoin to be more easily implemented in popular wallets without strenuous engineering, which may increase the network's overall _anonymity set*, or the number of users using this technique.

The common-denomination issue can further be resolved with additional techniques, such asPay-to-EndPoint (P2EP), which combines Satoshi's early work on privacy (see P2IP) with CoinJoin, whereby both senders and receivers contribute inputs to a transaction. This novel technique deserves a standalone post, but you can read more about it here, here and here.

P2EP is backwards compatible, and when used in conjunction with Schnorr, it may enable *sufficient* privacy in Bitcoin's base layer.

2 BIRDS, 1 STONE

It is reasonable to assume that Bitcoin's mass adoption depends upon the strength of its privacy guarantees. At the same time, the popularity of the Lightning Network and its own potential to host private payments has also generated uncertainty about future demand for on-chain settlement after the last bitcoin has been mined. As such, the need for privacy and the long-term sustainability of Bitcoin without block rewards are perhaps two of the most most alarming issues surrounding Bitcoin today. Thankfully, the privacy mechanisms enabled by Schnorr can potentially address these two issues simultaneously.

I've spent thousands of hours reviewing sophisticated privacy technologies, including different implementations of Ring Signatures, Confidential Transactions, Bulletproofs, zkSNARKs, STARKs, and MimbleWimble. While some of these technologies are mature enough to be implemented on Bitcoin's base layer, they still carry unique risks and trade-offs. As you have probably heard, Bitcoin is hard-fork averse, which makes it difficult to envision a scenario where any of these technologies get implemented *at all.*

A reoccurring concern people seem to have with the use of homomorphic encryption or non-interactive zero-knowledge proof systems is that they prevent

the full audibility of Bitcoin's monetary base. In other words, when transaction values are encoded, it becomes difficult to verify whether Bitcoin's supply cap is, in fact, 21M BTC. Similarly, inflation bugs and double spends become harder to pin point when transaction amounts are hidden. This is a considerable trade-off, and a push for the implementation of cutting-edge privacy on Bitcoin's base layer could divide the community.

But what if these technologies don't even need to be implemented in order for Bitcoin's base layer to gain _sufficient _privacy?

Schnorr can definitely help with that. If most Bitcoin transactions were to use Schnorr's cross-input aggregation feature in conjunction with P2EP, it would be become nearly impossible to de-obfuscate specific senders and receivers over time by simply looking at the blockchain. Bitcoin's supply would still be auditable, but its transactions would also provide much stronger privacy guarantees.

If there is demand for privacy, it is also reasonable to assume that Bitcoin users and businesses may want to engage in CoinJoin transactions passively, and let their wallets constantly mix their balances in the background. In this case, demand for privacy directly translates into an increase of on-chain transaction fees. Like SegWit, users will most likely champion the adoption of the technology at first, but businesses will have to follow suit at some point to remain relevant.

In time, the adoption of these technologies will make blockchain analysis obsolete and effectively removed from the _required _AML/KYC procedures that Bitcoin businesses are subject to, just like physical cash. When you deposit cash to your bank account, the bank won't check the bills for traces of drugs and prevent your deposit if they find any. There is no reason why this is done with bitcoin, other the proliferation of blockchain analysis coupled with the shortcomings of techniques like CoinJoin without Schnorr.

When performing AML/KYC on specific addresses and UTXOs becomes irrelevant, and the focus turns onto individuals rather than balances, Bitcoin businesses will fully embrace privacy. In fact, I suspect that when that happens, privacy and fungibility will become an integral part of value proposition of future Bitcoin businesses.

Ultimately, the adoption of stronger privacy mechanisms on Bitcoin's base layer will further empower its users and, at the same time, could contribute to the creation of a vibrant fee market after the last bitcoin has been mined. My guess is that it all starts with Schnorr's activation, which everyone seems to be onboard with.

Further reading:

If you want more technical details on MuSig, <u>Pieter Wuille's blog post</u> is a must-read.

<u>Andrew Poelstra's recent blog post on MuSig</u> is also a great read and it describes the work on the Schnorr-compatible <u>libsecp256k1-zkp</u>.

If you want better privacy **_now,_** I highly recommend reading nopara73's work on <u>ZeroLink: The Bitcoin Fungibility Framework</u>.

<u>Eric Wall's recent article</u> on the state of privacy of Bitcoin is definitely worth checking out. It goes into the specifics of the common-input-ownership heuristic that is often used in blockchain analysis.

Disclaimer:

WORDS

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

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

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

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

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

DYOR | BTFD | HODL

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

- @_joerodgers