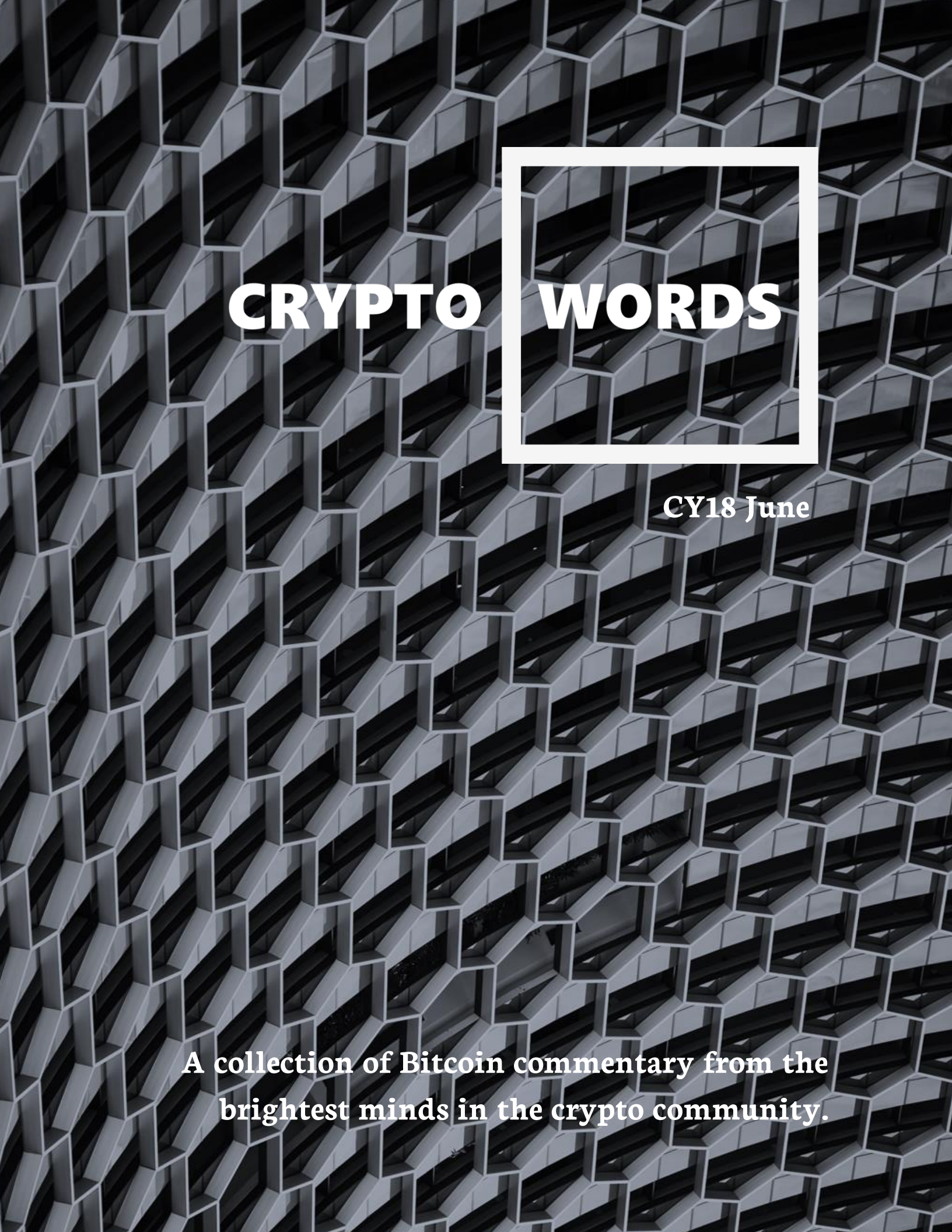
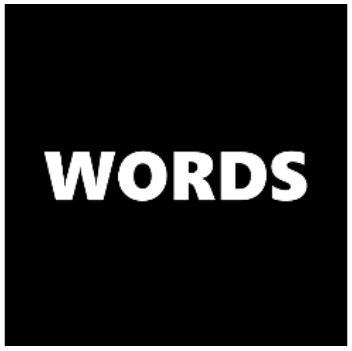


CY18 June

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

Contents

Goals and Scope



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

History

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

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

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

Support Crypto Words

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

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

Spread the word

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

Follow us on social media

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

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

Twitter

Subscribe to our newsletter

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

Our pledge

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

Subscribe

Bitcoin Miners Beware: Invalid Blocks Need Not Apply

Bitcoin is an impenetrable fortress of validation.

By StopAndDecrypt

Posted June 1, 2018

Like my Moore's Law article , this is an excerpt from a much larger article . It's good enough to serve as a standalone piece because the misconception this aims to put to rest is a commonly raised one that becomes annoyingly repetitive.

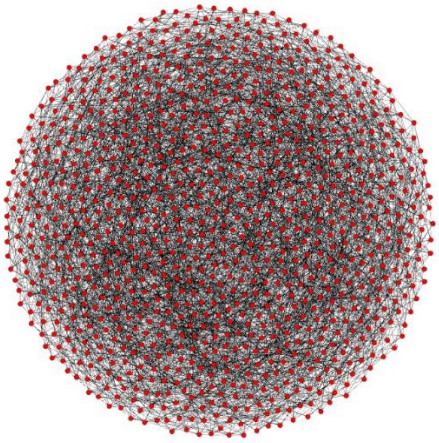
Understanding the Bitcoin network without math.

Bitcoin is more than just a chain of blocks. I want to help you understand how Bitcoin's blockchain *network* is designed because it'll help you fill in some gaps as you begin to acquire more knowledge in this field. I say *blockchain* network because Bitcoin also has a *payment channel* network *(lightning)* layered on top of it that doesn't effect the structure of the blockchain network. I won't be discussing Bitcoin's lightning network in this article though, as it's not that relevant to the points I'll make.

Below is a rough example of the Bitcoin network scaled down to 1000 fully validating nodes *(there's really 115,000 currently)*. Each node here has 8 connections to other nodes, because this is the default amount of connections the client makes without any changes made to it. My node is in here somewhere, and if you're running one, it's in there too. Coinbase's nodes are in there, Bitmain's nodes are in there, and if Satoshi is still around, Satoshi's node is in there too.

Please note that this is just a diagram, and that the real network topology can (and probably does) vary from this. Some nodes have more than the default amount of connections while others may opt to connect to a limited number or stay behind just

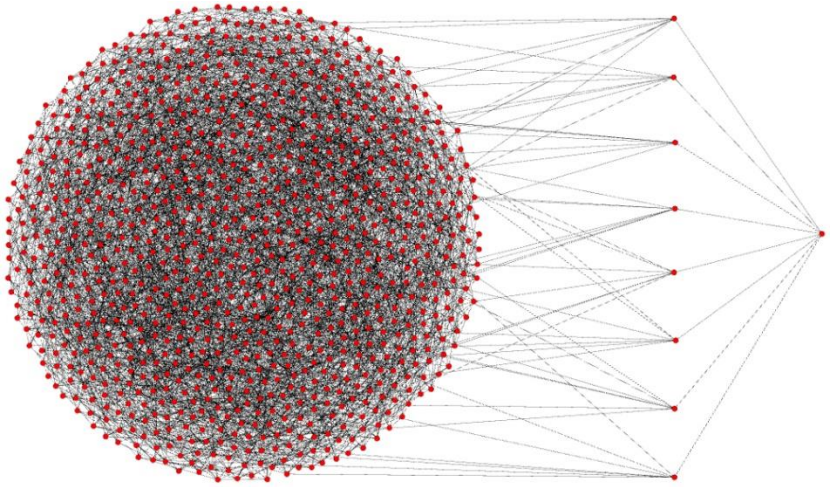
*one other node. There's no way to know what it actually looks like because **it's designed with privacy in mind** (although some monitoring companies certainly try to get very close approximations) and nodes can routinely changed who their peers are.*



I started with that diagram because I want you to understand that there are no differences in these nodes because **they all fully validate.** This means they all check the entire chain to make sure each and every transaction and block follow the rules. This will prove to be important as I explain further.

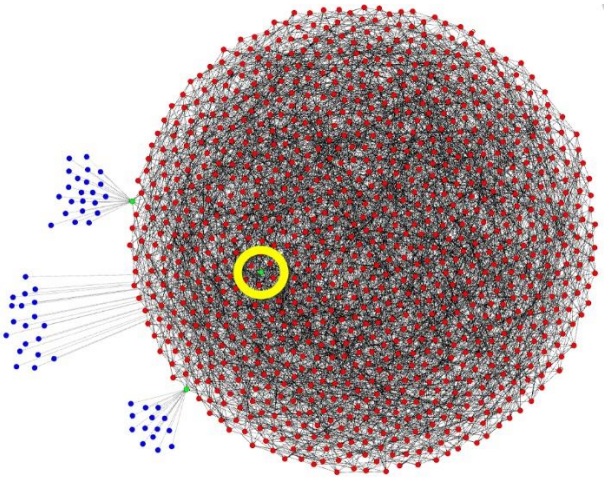
The ones on the inside are no different than the ones on the outside, they all have the same amount of connections. When you start up a brand new node, it finds peers and becomes one of the hive. The longest distance *in this graph* from any of these nodes to another is 6. In real life there are some deviations to this distance because finding new peers isn't a perfectly automated process that distributes everyone evenly, but generally, adding more nodes to the network doesn't change this. There are 6 degrees of Kevin Bacon, and in 6 hops my transaction is in the hands of *(almost)* every node, **if it's valid.**

I'm going to select "my" node from this group and drag it out, so I can demonstrate what happens when I create a transaction and announce it to the network. Below you'll see my node all the way to the right, and then you'll see the 8 other nodes *(peers)* that mine is connected to.



When I create a transaction and "send it out to the world", it's actually only going to these 8 peers. Since Bitcoin is designed from the ground up to make every node a fully validating node, when these 8 nodes receive my transaction they check to see if it's valid before sending it out to *their* 8 peers. **If my transaction is invalid it will never break the "surface" of the network.** My peers will never send that bad transactions to their peers. They actually don't even know that I created that transaction. There's no way for them to tell, and they treat all data as equal, but if I were to keep sending invalid transaction to any of my 8 peers, they would all eventually block me. This is done by them automatically to prevent me from spamming my connection to them. No matter who you are, or how big your company is, **your transaction won't propagate if it's invalid.**

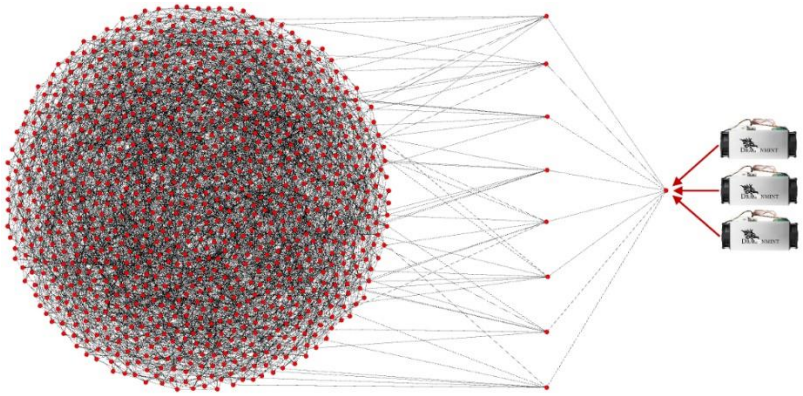
Now let's say you're not running a full-node, but you're using a light-client instead. Various light-clients exist for the desktop, and for your mobile phone. Some of them are Electrum, Armory, Bread, and Samourai Wallet. Light-clients tether to a specific node. Some can be set up to change the one they connect to over time, but they are still ultimately tethered. This is what tethering looks like:



I want you to note that this is just a diagram, and it's easy to demonstrate tethering using a node that *happens* to be on the rim, but there is no *real* rim, and tethering is tethering wherever that node happens to be within this diagram. I've highlighted this in yellow. The nodes being tethered to are green, and the blue dots are light-clients. All information going to or coming from the light-client goes through the node they're tethered to. They depend on that node. **They are not part of the network. They're not nodes.**

Here's where it gets fun, and where other people try to misrepresent how the network actually works: **What if I wanted to start mining?**

Mining a block is the act of *creating* a block. Much like a transaction you want to send, you must create the block and announce it to the network. Any node can announce a new block, there's nothing special about that process, *you just need a new block*. Mining has gotten increasingly difficult, but if you want you can purchase specialized hardware and connect it to your personal node.

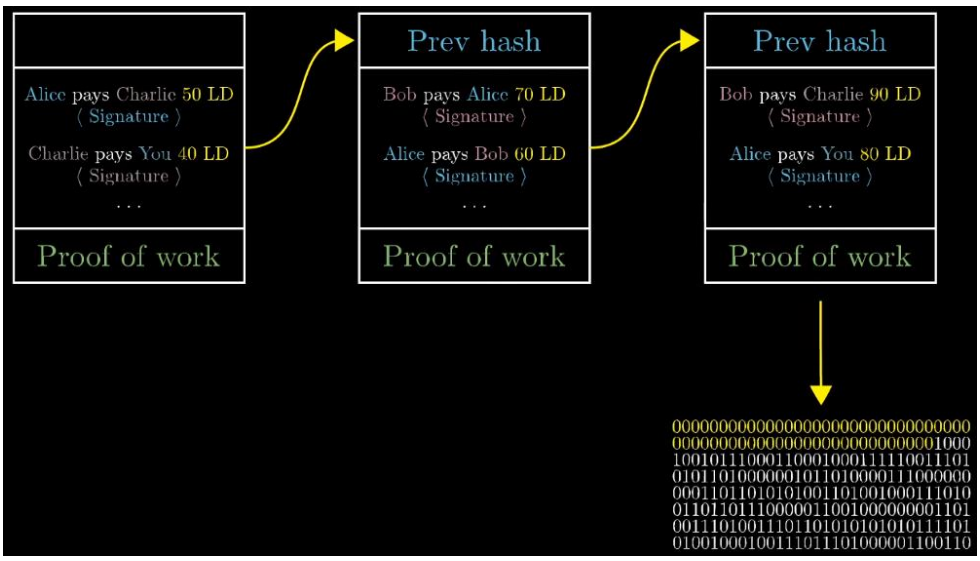


Remember that bit about invalid transactions? Same goes for blocks, but you need to understand something very specific about how blocks are created.

First watch this video. I skipped to the important part about hashing, using nonces *(random value)* and appending the chain with that new block **header**:

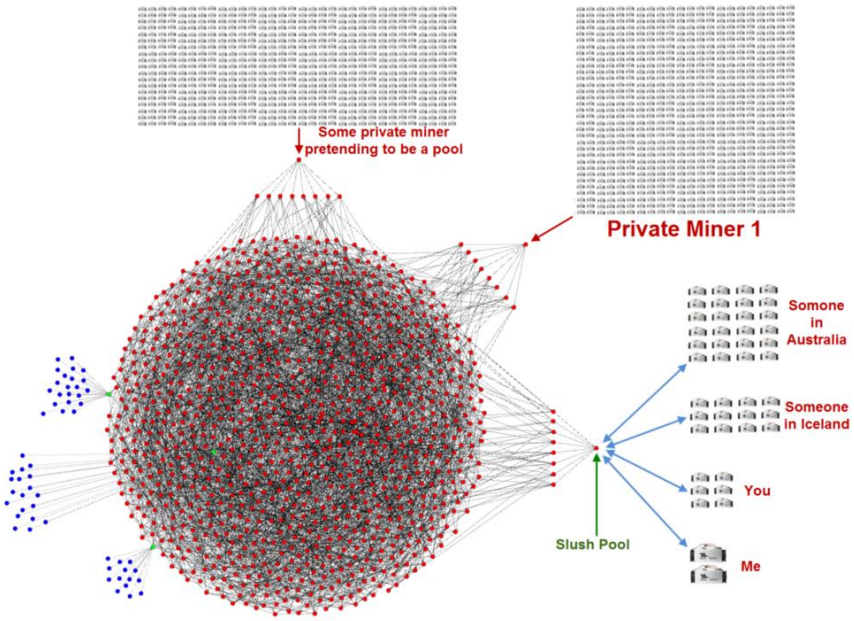
Please watch the entire thing if you have time. It's personally my favorite video explaining how mining works.

When you get to the following part in the video where the labels "Prev hash" are applied, those are the block headers:



What's not mentioned in this video is you can create valid blocks headers **even if all the transactions inside the block are invalid**. It still requires the same amount of time to mine blocks with invalid transactions as it does to mine a block with valid transactions. T he incentive to spend all that time and energy creating such a block would be to push through a transaction that rewards you with Bitcoin that aren't yours. This is why it's important that all nodes check not just the block headers, **but the transactions as well**. This is what stops miners from spending that time. Because **all** nodes check, **no** miners can cheat the system. If all nodes didn't check you'd have to rely on the ones that *do* check. This would separate nodes into "types", and the only type that would matter would be the ones that check.

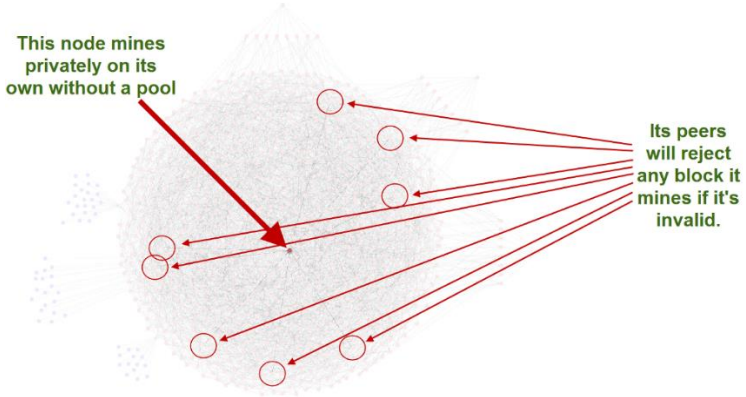
So what if you join a mining pool? You might do this because mining is too difficult for you to do alone, or if you're a slightly larger entity you might prefer a steady income as opposed to a sporadic one. Many miners do this, and they connected their specialized hardware directly to a mining pool using an entirely different protocol call the Stratum mining protocol. Just like creating a transaction with your non-node cellphone, **you don't have to run a node to connect your hardware to a mining pool.**You can mine without running a node, and many miners do exactly that. Here's what that looks like below in blue. I've used Slush Pool for this example:



Remember, I dragged these pool-run nodes out of the diagram for demonstration purposes. Just like any other node, these pool-run nodes need peers. They need peers to receive transactions & blocks, and they need peers to announce blocks they create. Allow me to reiterate again: **All nodes validate all blocks and all transactions.**

If any of these pools announce an invalid block, their peers will know **because they fully-validate**, and they won't send it out to other nodes. Just like transactions, **invalid blocks do not enter the network.**

Here's another way to look at this without pulling these nodes out from the diagram. Below is a private miner who doesn't want to be known, it has 8 random peers, and **none of those peers knows that it's a miner**. Again, this is intensionally designed this way for privacy reasons. There's no way for any node in the network to know that the block they received was *created* by their peer, or *relayed* by their peer. All they know is if it's valid or not, and if it is they send it along, if it's not, they don't.

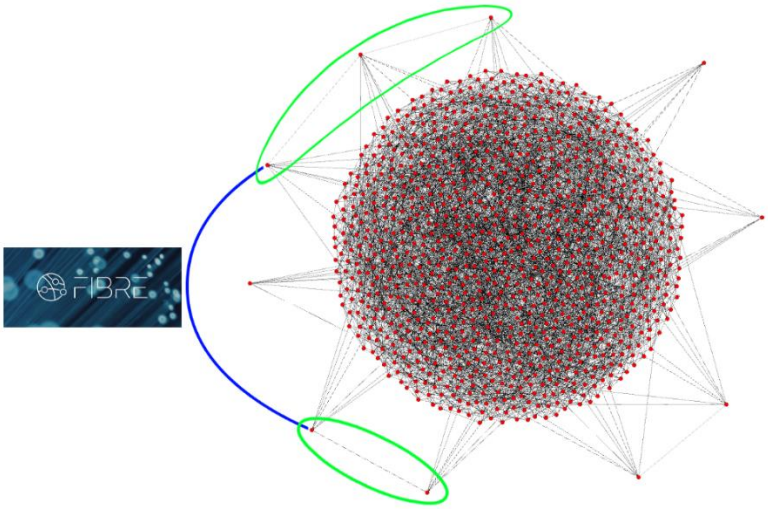


Hopefully you're getting the picture, and I don't believe I used any fancy math or equations to get here. I'd like to move on because I feel like this is complete coverage, but there is one final thing I'd like to address because it's this final aspect that is used to confuse others who don't fully understand everything I just explained. It's so rampantly used that I need to address it.

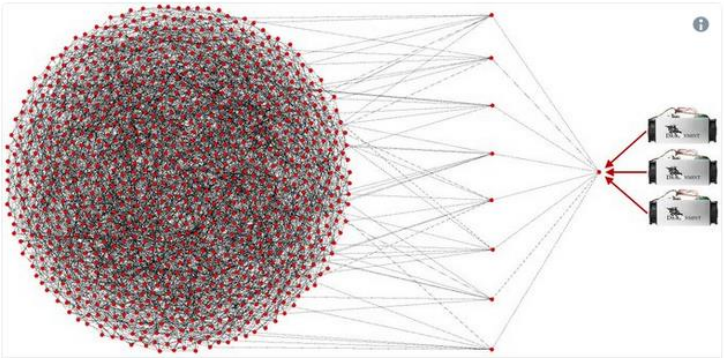
https://twitter.com/VitalikButerin/status/1000232465540136960

My original comment was talking about light-clients, also called SPV clients, and how they aren't part of the network. I demonstrated this above with the blue tethered dots. His follow-up comment tries to imply that nodes that mine are the only nodes who's rejection matters. *Remember: nodes have no way of knowing which other nodes mined a block versus who relayed a block,* ***this was designed intentionally.***

Now for a final diagram so I can try and explain the logic that's used when people say "only mining nodes matter". Some miners connect directly to other miners so that out of their peer list with the network, some of them are also other miners. **Not all miners do this**. Some of these miners that connect directly also use *optional* relay networks like the FIBRE network being designed by Bitcoin Core developer Matt Corallo, but even this side-network isn't exclusive to miners, anyone can join including you or me and it's just there to help block relay across the network. E ither way, people try to argue that this interconnectivity of "nodes that mine" *(whether using something like FIBRE or not)* implies they're the only ones that matter, and it's absurd:



In this example I left the node's peers inside the diagram. You should get the point by now. They reject invalid blocks. That group of nodes inside the green circles are most definitely not the only set of nodes that matter in this network.



Dr. Drecrypt
@StopAndDecrypt

Bitcoin is an impenetrable fortress of validation.

It doesn't matter if you created the transaction/block, or if someone else sent it to you: If it's not valid it's not getting in.

All nodes enforce validation in tandem.

Some people still don't seem to understand this concept.

♡ 852 4:41 PM - Jun 1, 2018

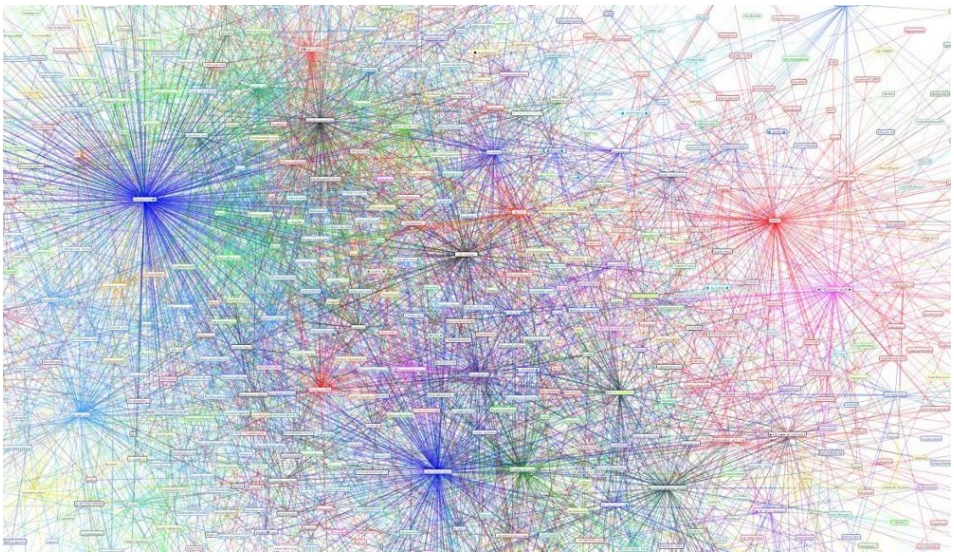
375 people are talking about this

The Time Value of Bitcoin

By Nik Bhatia

Posted June 8, 2018

1. 1/4 The Bitcoin Second Layer
2. **2/4 The Time Value of Bitcoin**
3. 3/4 The Bitcoin Risk Spectrum
4. 4/4 The Lightning Network Reference Rate



tl;dr

The HTLCs in Lightning Network give bitcoin a path to become a global reserve currency.

Abstract

Lightning Network provides a framework to measure the time-value of bitcoin, a precursor for a capital market and reserve currency status. Observable variables in Hashed Time Locked Contracts can be used to calculate the interest rate received on bitcoin held in payment channels, allowing investors to measure their opportunity cost of capital. Lightning Network wallet software should include ways to calculate interest and prove the rate received in a trust-minimized way. A reference rate should be developed akin to US Dollar LIBOR, using consensus to dictate how the rate is calculated. This reference rate can anchor off-chain bitcoin lending into the global economy, leading to bitcoin-denominated banks, credit

ratings, debt capital markets, and eventually an entire financial system: a path toward status as a global reserve currency.

Calculation Method

Three observable variables are needed to calculate an interest rate: principal, cash flows, and time. In Lightning Network, the principal is the amount of bitcoin in a payment channel; cash flows are routing fees; time is the block-time in which the fee collection is measured. Wallet implementations should experiment with different interest rate calculation methods with the eventual goal of a consensus method. The US Dollar has Treasuries, Fed Funds, LIBOR, OIS, and SOFR all acting as reference rates within the capital market for lending, borrowing, and swapping cash flows. Bitcoin needs to establish a reference rate of its own, referred to in this writing as LNRR (Lightning Network Reference Rate).

There are many possible ways to calculate LNRR. Principal may be measured once per block or using an average over time. Fees may be measured for individual HTLCs, individual payment channels, or Lightning Network nodes with multiple channels. Block-time may be measured by the locktime of HLTCs or measured one block at a time. Compounding conventions may be discrete or continuous. On-chain fees paid to open and close channels may be included or excluded in the calculation. We need to experiment with calculation methods because bitcoin is an entirely new asset class and shouldn't adhere to financial conventions of the past, even though traditional fixed income markets set the bar extremely high for financial sophistication.

Time-value of bitcoin

Fees, time-value, and security risk premiums are discussed in the *The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments* by Joseph Poon and Thaddeus Dryja:

*The **time-value of fees** pays for consuming time (e.g. 3 days) and is conceptually equivalent to a gold lease rate without custodial risk; it is the time-value for using up the access to money for a very short duration.*

*Historically, one of the largest component of fees and interest in the financial system are from various forms of counterparty risk—in Bitcoin it is possible that the largest component in fees will be derived from **security risk premiums** .*

Fees in Lightning Network can be attributed to two components, time-value and security risk premium. Fees compensate the leasing of bitcoin which translates into **time-value**. Positive interest rates should attract capital and competition. But Lightning Network node operators investing capital are not doing so purely risk-free. They are taking on a variety of risks, most notably the risk of using hot wallets to stake liquidity to the network. Therefore, interest rates will vary between nodes due

to different security practices, captured here by the catch-all variable **security risk premium**.

r = time-value + security risk premium

Lightning Banks

Lightning Network will birth Lightning banks. Their first function will be to provide liquidity to Lightning Network by funding payment channels. They will try to position themselves as central routing hubs, capturing as many fees as possible. Competition will be open and fierce. Those with the greatest ability to efficiently manage payment channels and actively optimize routing positioning will profit.

Reference Rate

LIBOR was originally intended as an inter-dealer interest rate, however market conditions and manipulation scandals have significantly changed its role. Despite its evolution, LIBOR's model could serve as an example for LNRR to follow. The calculation method for LIBOR is essentially a panel: banks are asked to submit rates and these rates are aggregated to form a reference rate published once a day. Lightning banks can publish their interest rates to each other in order to foster a dealer community similar to the LIBOR panel banks. Any node that can publish an interest rate can potentially contribute to LNRR, and ideally all interest rates that are published would be cryptographically provable by all participants to assure complete transparency.

Once Lightning banks establish LNRR, they can reference this rate and charge a spread for loans that are not secured by the Bitcoin blockchain. They can use the reference rate to attract deposits which would also not be secured by the blockchain. While off-chain, trusted, bitcoin denominated capital market activity does not benefit from Bitcoin's immutability, it is essential for the establishment of bitcoin as a currency capable of global economic activity. Economic activity requires a tradeoff between time preferences which can only be achieved when savers are allowed to lend capital.

Conclusion

LNRR is not some magic solution. This paper is a suggestion to the Lightning developer community to start experimenting with the translation of HTLCs to a financial framework. We cannot go from Trace Mayer's sixth network effect of financialization to the seventh network effect of reserve currency status without the correct financial tools. Bitcoin has already emerged as a new asset class and is now acting as a reserve asset for millions around the world. Transitioning from reserve asset to reserve currency will present a challenging path. Ideas like LNRR should be discussed and explored so that we can continue to push bitcoin forward as the world's best abstraction of money.

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

Sources

Bitcoin: A Peer-to-Peer Electronic Cash System by Satoshi Nakamoto

https://bitcoin.org/bitcoin.pdf

The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments by Joseph Poon and Thaddeus Dryja

https://lightning.network/lightning-network-paper.pdf

Mastering Bitcoin 2nd Edition—Programming the Open Blockchain by Andreas M. Antonopoulos

https://github.com/bitcoinbook/bitcoinbook

CRYPSA event with Trace Mayer

http://www.bitcoin.kn/2015/06/crypsa-event-with-trace-mayer/

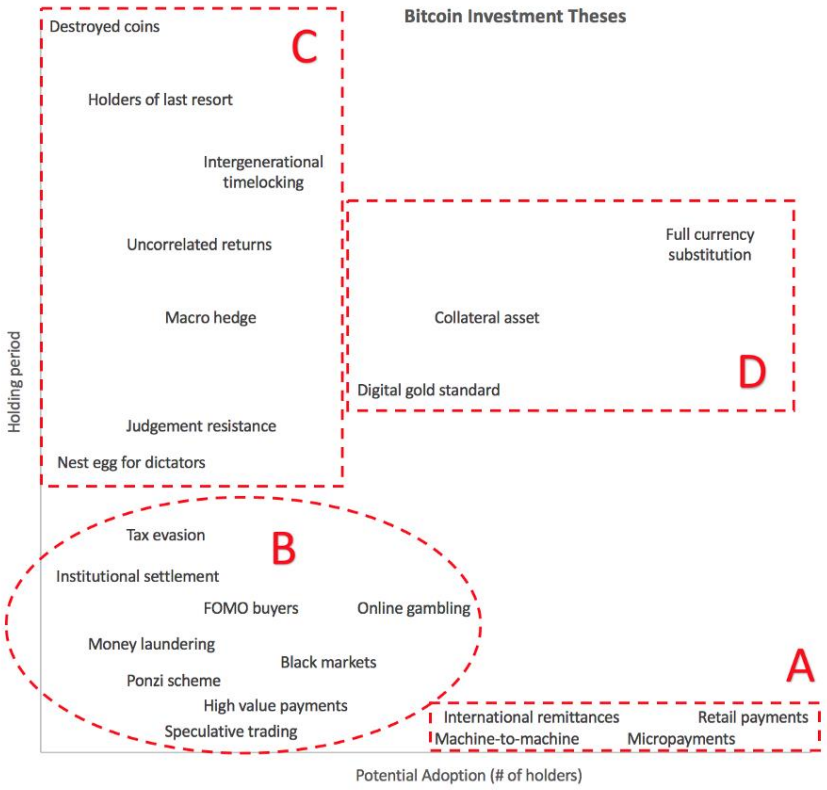
Bitcoin Investment Theses (Part 1)

By Pierre Rochard

Posted June 9, 2018

- Bitcoin Investment Theses Part 1
- Bitcoin Investment Theses Part 2
- Bitcoin Investment Theses Part 3 NOT YET PUBLISHED

We can classify the investment theses for (and against) investing in Bitcoin into categories. This helps clarify how much of an impact a given narrative could have to Bitcoin's valuation. Investment theses that have a short holding period are less meaningful for investors than ones with a long holding period. Likewise, theses with a large number of potential adopters are more meaningful for investors than ones with a small number of potential adopters. This is an imperfect heuristic that should be debated and refined.



Investment theses with a short holding period are focused on using bitcoins as a method of payment. Some of these theses would find ubiquitous usage while others are niche verticals. If you disagree with anything written here, feel free to contact me on Twitter or on GitHub.

A. Short holding period, wide adoption

1. Retail payments

Thesis: Bitcoin, whether it's on-chain, off-chain, or Lightning, will supplant current retail payment methods including cash, checks, and credit cards. Bitcoin's advantage over cash and checks is that it is digital, the consumer only needs a smartphone and the retailer does not have to worry about handling cash or depositing checks. Bitcoin's advantage over credit cards is lower transaction fees, irreversibility which protects the merchant, and a "push" system with no credit card numbers—which protects the consumer. Fast settlement means that merchants require less in working capital.

Anti-thesis: Reversibility increases consumer confidence. A "pull" system enables subscriptions which are an important business model. On-chain transactions can not scale without centralizing the Bitcoin network. Off-chain and layer 2 transactions have an up-hill battle against entrenched debit and credit card payment systems. Credit cards give consumers flexibility in financing their purchases. Many countries have already deployed payment systems that are instant with low to zero fees. Consumers who acquire bitcoins with the intent of making retail payments end up just holding the bitcoins for price appreciation instead.

2. Micropayments

Thesis: Bitcoin's Lightning network enables instant, high-volume micropayments. Micropayments will be leveraged by online games, content publishers, and social media tipping services to monetize interactions and consumption.

Anti-thesis: Subscriptions provide a better revenue model for content publishers and social media tipping ignores why people actually engage with each other. Game creators and players currently have no serious issues with in-game purchases. If there are any complaints, it's from players who feel nickel-and-dimed, which would only be worse with micropayments.

3. Machine-to-machine payments

Thesis: The Internet of Things (IoT) means your refrigerator could communicate with several grocery business APIs to negotiate for the best value replenishment. Soon

the grocery business itself will automatically be negotiating with self-driving cars providing delivery services. This network of machine-to-machine payments will all be with Bitcoin's Lightning Network.

Anti-thesis: It's unclear why the businesses, which own the machines, would not invoice each other on a monthly basis, instead of continuously streaming payments. Companies will continue to keep track of their payables and receivables, and netting them out for payment, in which case Bitcoin is not a necessity. Today Amazon Web Services charges by the second and can be controlled by an API, but payments are made monthly with fiat-denominated credit cards, wire transfers, or ACH.

4. International remittances

Thesis: Money transfers between countries are expensive and slow; Bitcoin can make them fast and cheap. Anyone, anywhere in the world who has an internet connection can receive bitcoins.

Anti-thesis: Senders want to send their local fiat currency and recipients want to receive their local fiat currency. Neither side has bitcoins. Using Bitcoin means adding an FX conversion on the sender's side and on the recipient's side. This inherently increases cost. The cost of sending $200 anywhere in the world has declined from 10% in 2008 to 7% in 2017. Money transfers are expensive due to physical locations, marketing, licensing, and compliance. Bitcoin on its own does not solve any of those issues. The slow fiat payment rails are being improved by fintech startups using fiat banks and SQL databases.

B. Short holding period, narrow adoption

1. Tax evasion

Thesis: Just as restaurant waiters can under-report their cash tips, a person or business receiving bitcoin revenues could under-report them. There is no financial institution which the IRS can subpoena for records. If the tax evader is careful about how they use Bitcoin's public blockchain ledger then they can also avoid being caught with data analysis.

Anti-thesis: Tax auditors have experts in computer forensics and there's always a paper trail for the creation and sale of a good or service. It would be risky and time consuming to convert the proceeds into fiat. Tax evasion does not scale due to whistle-blowers, reporting by third parties (1099's in the US), and the lifestyle/income mismatch.

2. Black markets

Thesis: Before it was shutdown in 2013, the Silk Road was a marketplace for illegal drugs. It had tens of thousands of users and $22 million in annual sales. In 2017, a successor of the Silk Road called AlphaBay was also shut down. It was ten times the size of the Silk Road with hundreds of thousands of users. Bitcoin enables the sales of illegal goods and services because it is a permissionless, censorship-resistant payments network.

Anti-thesis: Ultimately most goods and services have to be delivered in the real world, so even if the payment is pseudonymous the delivery can reveal the identities of buyers and sellers. Additionally, even if the bitcoins are bought and sold in person for fiat cash, there is a risk that the bitcoin broker is an informant or government agent. Buying and selling bitcoins on an online exchange with KYC/AML is even riskier. This problem is compounded by the visibility of on-chain Bitcoin transactions.

3. Ransomware

Thesis: Ransomware is when malicious software encrypts a user's data, locking them out of personal or business information. The virus demands payment in bitcoins to decrypt the data.

Anti-thesis: Increasing awareness of the problem is leading to effective mitigation strategies, whether with anti-virus software or offline data backups.

4. Online gambling

Thesis: While online poker is legal in the United States, in practice the Unlawful Internet Gambling Enforcement Act of 2006 made it illegal for financial institutions to service online poker platforms and players. This eventually led to the wide usage of Bitcoin for funding online poker games. The phenomenon has expanded beyond poker. There are Bitcoin-funded sites for sports betting, blackjack, dice, and slots.

Anti-thesis: If US legislation changes to be more favorable towards online gambling then this niche for Bitcoin could disappear.

5. Unbanked businesses

Thesis: Payment processors and banks are facing pressure to not service businesses for political reasons. These businesses include gun stores, marijuana dispensaries, and sex workers. Other businesses and individuals do not have access to banking services due to redlining or credit history. A Bitcoin wallet enables these demographics to "be their own bank" with a checking account and the ability to send and receive payments.

Anti-thesis: As long as the rest of the economy is using fiat currencies, the unbanked still need a way to exchange their bitcoins for fiat. They can use in-person cash exchange services, though there are cases of people being robbed and it is not a scalable solution for anything but the smallest business.

6. Speculative trading

Thesis: Bitcoin exchanges are open for trading 24/7. On top of Bitcoin's volatility, they also offer up to 100x leverage. Tech-savvy traders are building bots that use the exchanges' public APIs to execute their strategies. The matching engines of exchanges are moving from AWS to dedicated hosting, in the same facilities where US equities trade. Exchanges are the most profitable businesses in the Bitcoin ecosystem, offering both spot and futures products. Speculators can now profit by going long or going short. The limited supply of bitcoins has led to repeated speculative frenzies, where fortunes have been made and lost.

Anti-thesis: Speculation is zero-sum, eventually bad traders will run out of capital and good traders will see diminishing profits and move to greener pastures. Bitcoin's volatility has been decreasing as its liquidity increases. The markets are manipulated to favor whales and they will be shutdown or become boring when government regulators intervene to stop manipulation. The speculative frenzies are faked by wash-trading volume and fractional reserve exchanges.

7. Ponzi scheme

Thesis: While Bitcoin may not fit the definition of an actual Ponzi scheme, it has a lot of similarities. Preston Byrne popularized the concept of a Nakamoto Scheme. Early buyers of bitcoins recruit and sell to later buyers, at ever higher prices. The cries to "HODL" are there to prop up the price and keep the scheme from falling apart. "Tulips" and "greater fool theory" are used as shorthand for this thesis. Once the number of gullible buyers runs out, the price will crash as everyone tries to get out at the same time, much like a bank run.

Anti-thesis: Every money has no intrinsic value. They are bubbles, shared illusions, inter-subjective Schelling points. A money is an unproductive asset which is best suited to be society's medium of exchange, store of value, and unit of account. Bitcoin is bootstrapping to potentially fill that role from a value of zero. This has led to an astounding run-up in its fiat price. What goes unexplained in the Ponzi scheme thesis is why severe drawdowns (most recently a 91% peak to trough drawdown in 2014) are not a deathblow. So far, the value of Bitcoin has recovered and ultimately has increased beyond the previous all time high.

8. Money laundering

Thesis: Corrupt politicians who were bribed with bitcoins want to convert them into legitimate assets without raising suspicions. The money launderer can take advantage of Bitcoin's fragmented market by sending small amounts to many different exchanges to sell for fiat, a form of structuring. A money launderer can also mix the illegal Bitcoin revenues with legal Bitcoin revenues, for example from an online poker business they control or partner with. A growing strategy is purchasing property with bitcoins, and then selling the property for fiat.

Anti-thesis: Any involvement of Bitcoin raises suspicion, so laundering bitcoins is ultimately harder than laundering fiat. Data indicates that Bitcoin money laundering has been an increasingly marginal activity. Bitcoin faces stiff competition from large international banks, which continue to be the go-to providers of money laundering services.

9. Routing around capital controls

Thesis: Countries which have a currency peg, like China, have to rely on capital controls to prevent their currency's exchange rate from appreciating or depreciating in an unexpected manner. For example, Chinese citizens can only purchase up to $50,000 of foreign currency per year. Chinese regulators have also recently prevented offshore investments into U.S. real estate. Bitcoin allows people to route around capital controls, by buying bitcoins locally, sending them to an exchange abroad, and selling them for the foreign currency.

Anti-thesis: While Bitcoin can help small-scale evasion of capital controls, it is not liquid enough to capture market share from other forms of evasion. Governments have and will crackdown on their local Bitcoin exchanges to further reduce liquidity.

10. FOMO buyers

Thesis: Retail investors see the price going up and experience a "fear of missing out" on further price gains and the social phenomenon. Individuals want to be able to relate to each other, i.e. if your friends are talking about investing in Bitcoin then you feel a need to do so yourself. When the price stops going up parabolically the social fad quickly passes. Conversation turns to embarrassing losses and moves on to the next trendy investment.

Anti-thesis: The FOMO buyers become FOCO (fear of cashing out) holders. They sit on the bitcoins they impulsively bought, waiting for the next bubble. A small percentage start to research what Bitcoin is and continue accumulating during the bear market.

11. Vehicle Currency

Thesis: In 1979 Paul Krugman published a paper titled “Vehicle Currencies and the Structure of International Exchange”. In this paper he explained that “People who want to exchange one currency for another will not necessarily make the exchange directly. They may make the exchange by way of some third currency, which becomes a “vehicle” for the transaction. Historically, certain currencies—the pound sterling before 1914, the U.S. dollar in recent years—have come to be widely used as vehicle currencies.” Bitcoin has the potential to become the vehicle currency of international trade.

Anti-thesis: Bitcoin is not nearly liquid enough to be a vehicle currency. Competing with the U.S. dollar for this is extremely difficult, the most likely candidate has been the euro and it has made little progress.

12. Electricity monetization

Thesis: Governments and individuals that are struggling to get hard currency can use cheap local electricity to mine for bitcoins. The Venezuelan government has been seizing imported Bitcoin mining equipment so that they can use it themselves. The North Korean government acquired 11,000 bitcoins through a combination of mining and hacking.

Anti-thesis: As Bitcoin mining finds increasingly inexpensive sources of electricity, it will become less and less profitable for governments to mine even if they have favorable access to fossil fuels.

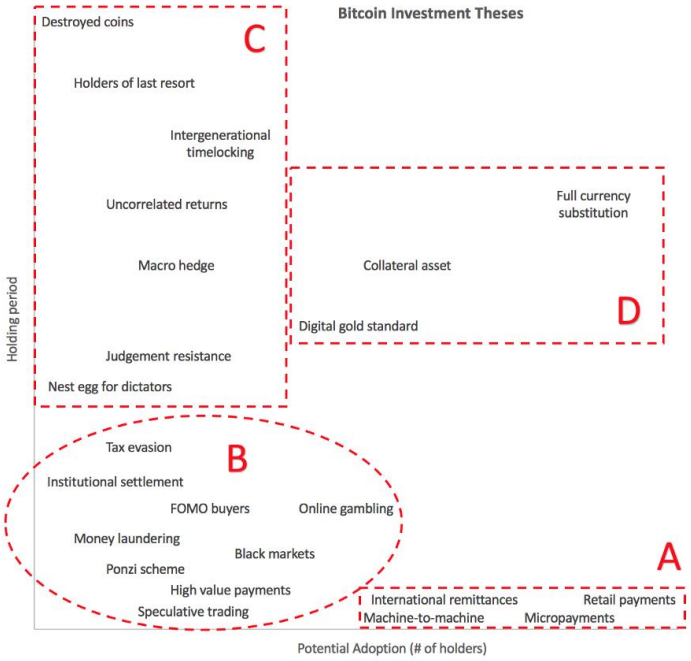
Bitcoin Investment Theses (Part 2)

By Pierre Rochard

Posted June 24, 2018

- Bitcoin Investment Theses Part 1
- **Bitcoin Investment Theses Part 2**
- Bitcoin Investment Theses Part 3 NOT YET PUBLISHED

These descriptions of the numerous Bitcoin investment theses are all open source on GitHub. Feel free to open an issue here if you have an investment thesis you'd like to see listed but are unfamiliar with how to use git.



C. Long holding period, low adoption

1. Nest egg for dictators

"Normally when you have a parabolic curve, eventually it has a very sharp break," Soros said Thursday. "But in this case, as long as you have dictatorships on the rise you will have a different ending, because the rulers in those countries will turn to Bitcoin to build a nest egg abroad." George Soros, January 25, 2018

Thesis: While we don't have any evidence that dictators are currently holding bitcoins abroad, George Soros suggests that they will in the future. Dictators amass fortunes by seizing private businesses, demanding bribes from resource producers, and exploiting government monopolies. For example, the dictator of Equatorial Guinea has a net worth of $600 million. This is small compared to the $95 billion belonging to the Supreme Leader of Iran. Dictators could include bitcoins in their asset allocation so that they have an unseizable slush fund in case they get ousted and exiled.

Anti-thesis: The wealth of dictators is often just the wealth of their government and is already invested in productive assets or used to stay in power by buying supporters. Even if dictators are holding cash abroad, they will continue to be more comfortable with the stability of gold and the U.S. dollar. Unless they have been specifically targeted by financial sanctions, dictators have an easy time holding cash in the international financial system with shell companies.

2. Seizure Resistant

Thesis: Bitcoin allows civilians to more easily withhold wealth from rapacious governments. Fleeing a totalitarian regime with your family's wealth used to mean concealing gold or diamonds, and praying that a greedy border guard didn't find your stash. With bitcoin, you could memorize 24 words that store an arbitrary amount of value. Abusive seizures of wealth are not limited to totalitarian regimes, the United States government takes $5 billion per year with a process called civil asset forfeiture that assumes "guilty until proven innocent". Additionally, a United States federal district court judge can freeze supposedly tainted assets before a criminal trial happens, which could prevent you from hiring the lawyer you want. Having a secret stash of bitcoins could secure criminal defendants' due process rights.

Anti-thesis: Governments will still be able to identify who owns bitcoins due to the public blockchain and seizing records from exchanges and brokerages. This would allow them to imprison and torture bitcoiners until they divulge their private key. While it is not criminal for an attorney to accept a tainted asset as payment, they may still refuse to do so to avoid the risk of themselves being subject to civil asset forfeiture.

3. Judgement Resistant

Thesis: The successful party in civil litigation can have a right to recover money or property from the unsuccessful party, in which case the successful party is a judgement creditor. Judgement creditors can freeze a bank account with a court order, called a garnishment or attachment. Bitcoin can be used to illegally hide

value from judgement creditors. More interestingly, holding bitcoins with multi-signature technology in one or more foreign jurisdictions can be part of a legal strategy to frustrate or prevent the recognition and enforcement of a just or unjust judgement. Even before a party succeeds and obtains a judgement, they could freeze an individual or business bank account with a pre-judgement attachment. This can be an economic hardship, regardless of whether the trial lasts weeks, months, or years. This is especially problematic for large multinationals which operate in jurisdictions with dysfunctional or abusive judiciary systems. International banks currently provide a similar service with judgement resistant trusts, but these are expensive and cumbersome compared to a Bitcoin solution. This thesis was formulated by Ari Paul.

Anti-thesis: We don't have any examples of Bitcoin's judgement resistance being tested. We don't know how judges will respond to the complexity of an asset being in multiple foreign jurisdictions simultaneously. Judgement-resistant does not mean judgement-proof, it may just take longer and be more expensive but lawyers will get to the bitcoins eventually. We may see treaties or case law emerge to prevent bitcoin multi-sig jurisdictional "abuse".

3. Banking crisis hedge

Thesis: In 2008, WaMu experienced two bank runs. Even with FDIC insurance, if this were to happen to several major international banks simultaneously it would be disruptive enough to freeze the banking services of many businesses and individuals. Bitcoin's layer 1 and layer 2 payments systems are decentralized and 100% reserve, thus immune to bank runs, they would continue to process payments seamlessly in a crisis. Bitcoin has no bank holidays. For this payments system hedge to work, the hedger has to be holding bitcoins ahead of the crisis, otherwise fiat payments to exchanges and OTC brokers would get caught up in the fiat freeze. Worse than a temporary payments freeze would be a bank bail-in, for example in 2013 Cypriot banks' depositors were subjected a one-off 9.9% levy for any deposits above €100,000. Bitcoin is an insurance policy for both individuals and corporate treasuries and should be a part of business continuity planning.

Anti-thesis: Governments would just bail out "too big to fail" financial institutions to keep fiat payment systems from freezing up. The hedge does not work if retail stores, vendors, suppliers, employees, business owners, etcetera are unable or unwilling to accept bitcoins as payment even in a crisis.

4. Inflation hedge

Thesis: Central banks are engaging in unorthodox monetary experiments to stabilize financial systems and economies after the 2008 crisis. These experiments will

eventually result in uncontrolled inflation. Countries with failing governmental institutions, like Venezuela, are currently suffering from hyperinflation. Bitcoin's ultra-orthodox monetary policy of targeting a fixed money supply, with 80% of the total 21 million bitcoins already in circulation, is the ideal hedge for fiat money printing.

Anti-thesis: People have been predicting fiat hyperinflation since quantitative easing started a decade ago, and yet inflation is still very low in developed countries. Owning stocks, real estate, commodities, or precious metals is a better long-term inflation hedge than Bitcoin, which has a very short track-record. Bitcoin's track-record indicates that its value is not tied to expected inflation.

5. Uncorrelated returns

Thesis: Bitcoin's returns are uncorrelated or weakly correlated with other asset classes. This makes it ideal for diversifying a portfolio. The optimal allocation to Bitcoin has been estimated to be 1.3%.

Anti-thesis: Bitcoin is increasingly correlated with the stock market. It is widely viewed as a "risk-on" asset that is being inflated by easy money going into the broader tech ecosystem. Past lack of correlation was just due to how small bitcoin was relative to other asset classes.

6. Intergenerational timelocking

Thesis: OP_CHECKLOCKTIMEVERIFY could be used to lock up bitcoins for several centuries. This could help overcome what's called the rule against perpetuities which prevents the deceased from affecting the ownership of property long after they have died.

Anti-thesis: Time-locked bitcoins will end up trading in a secondary market at a discount.

7. Holders of last resort

Thesis: Fractional-reserve monetary systems require lenders of last resort to stop debt-deflation from causing the economy to collapse. An emerging 100% reserve monetary system like Bitcoin requires holders, and buyers, of last resort to stop a crisis of confidence from causing the value of bitcoins to collapse. This is functionally similar to a central bank using its reserves to buy the domestic currency, fighting off speculators who are betting on devaluation. Holders of last resort are intransigent advocates for Bitcoin's economics and technology.

Anti-thesis: Not enough people are interested in Bitcoin maximalism's ideology to form a set of holders of last resort with enough capital to defend bitcoin from a catastrophic and final loss of value. Holders of last resort are delusional and will end up just holding a worthless bag of buttcoins.

8. Destroyed coins

Thesis: Many bitcoins have been destroyed, accidentally or deliberately. This permanently removes them from the market. When a bitcoin is destroyed this makes all other bitcoins proportionately scarcer, and thus presumably more valuable.

Part 3 coming soon!

If you have any ideas for investment theses, feel free to reach out! I'm on Twitter @pierre_rochard, DMs are open.

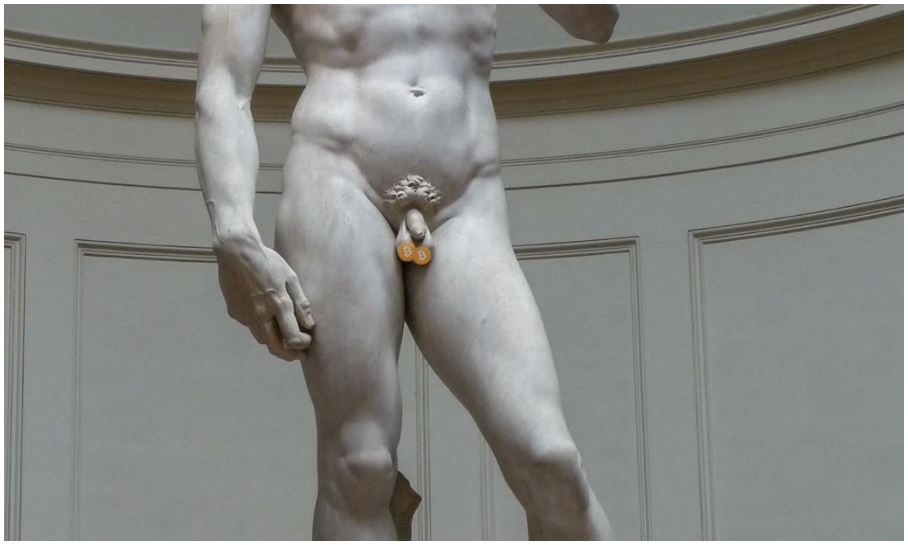
Did you disagree or agree with any of the above? Leave a comment below!

Bitcoin's Energy Consumption

A shift in perspective

By Gigi

June 10, 2018



You might have heard that Bitcoin wastes a tremendous amount of energy. You might also have heard that Bitcoin will use half a percent of the world's electric energy by the end of the year, the computations used for mining don't do anything useful, and if the current rate of growth continues it will suck up all the energy and we are all going to die.

I don't want to dispute the numbers or compare Bitcoin's energy usage to the current banking system. I simply want to offer a shift in perspective.

Bitcoin is Offensive

Bitcoin is a global, permission-less, censorship-resistant network. Its nature is inherently offensive. It offends governments, bankers, and central authorities alike. Hell, offending banks was the whole point of this experiment in the first place.

At first glance, Bitcoin is the worst database ever devised by mankind. In addition to being seemingly inefficient and slow, it is eating up computational resources at a mad pace and consumes as much energy as a small country.

"In comparison to modern distributed databases, blockchains are slow, ponderous, unnecessarily redundant and overly paranoid."*Dhruv Bansal*

As Nick Szabo so succinctly put it: "Bitcoin offends the sensibilities of resource-conscious and performance-measure-maximizing engineers and businessmen alike." It also offends our globally shared understanding that wasting energy is bad, and energy-efficiency is always good.

According to a recent paper "the Bitcoin network can be estimated to consume at least 2.55 gigawatts of electricity currently, and potentially 7.67 gigawatts in the future, making it comparable with countries such as Ireland (3.1 gigawatts) and Austria (8.2 gigawatts)."

It's easy to be concerned, outraged or offended. *"Did you know Bitcoin uses as much energy as Austria? Baby cows are dying because of Bitcoin!"*

What-what the hell is a gigawatt?

To understand why all these gigawatts are necessary for the Bitcoin network to function properly and securely, we will have to take a closer look at the nuances of mining.

Mining Blocks and Coins

The name "mining" stems from the proposition that bitcoin has more in common with gold and other precious metals than paper money. Satoshi made this clear in one of his posts.

"In this sense, it's more typical of a precious metal. Instead of the supply changing to keep the value the same, the supply is predetermined and the value changes."*Satoshi Nakamoto*

Hence bitcoins are not printed, they are mined. Even though we talk about "mining bitcoins" all the time, keep in mind that it isn't bitcoins which are mined. Blocks are mined, and miners are currently rewarded with *new* bitcoins if they find a valid block. Miners are rewarded because finding new blocks is inherently difficult. The system is set up in a way that the difficulty of finding a new block is adjusted automatically so that a new block is found every 10 minutes on average. Differentiating between "mining bitcoins" and "mining blocks" helps to point out a couple of things:

First, that the rate at which bitcoins are mined is decoupled from Bitcoin's energy use. If everyone would decide to double the energy spent on mining, the number of bitcoins mined would *not* double as a consequence. The rate of supply is fixed, no matter how much energy you choose to expend for mining.

Second, that miners do a lot more than bringing new bitcoins into existence: maintaining the security and continuity of the network, confirming transactions, and signaling their support or rejection of network changes, to name a few. Not all of these require an excessive amount of energy, which is one of the reasons why running a full node is important.

Third, that mining is not a fixed process. Both the mining reward and the mining difficulty are dynamic and thus will necessarily change over time.

Fourth, that mining is *supposed* to cost a lot of energy. It is computationally expensive by design, which is why Satoshi chose to reward people *extra* for expending this energy. It is the main ingredient of the Nakamoto Consensus. It is the work in proof-of-work. It is absolutely essential.

Without a closer look at the mining process, it is easy to confuse the energy-intensive process of finding valid blocks with "finding new bitcoins". From this perspective, it seems like all this electrical energy is transmuted into new bitcoins.

This is wrong.

The energy expended acts as a barrier which protects the public ledger. The creation of new bitcoins is just a side-effect.

Cryptographic Walls

Until very recently, securing something meant building a thick wall around whatever is deemed valuable. We all know how to do this, and we all agree that this is a sensible thing to do.

The new world of cryptocurrencies is unintuitive and weird. There are no physical walls to protect our money, no doors to access our vaults. Bitcoin's public ledger is secured by its collective hashing power: the sum of all energy expended to do the work in its proof-of-work chain.

Thus, we can think of Bitcoin's energy usage like a giant wall—a sort of electrical force-field—which secures all bitcoin balances of all users, now, and in the future.

It is hard to say how much energy has to be expended building these cryptographic walls. Financial systems are critical infrastructure, which is why most engineers in this space rightfully argue that security and stability are paramount. If Bitcoin will be the money of the future, it better be prepared to withstand high-impact, low-probability events.

How thick will these cryptographic walls need to be? Only time will tell. If Bitcoin is able to survive coordinated attacks by multiple state-level attackers, the walls were thick enough.

The End of Mining New Bitcoins

Bootstrapping a new network is difficult. It's like trying to convince everyone to buy a fax machine if you are the only guy in the world with a fax machine. It's really, *really* hard. As outlined above, Satoshi solved this problem by adding a block reward mechanism, which acts as (a) the controlled currency supply of Bitcoin and (b) an incentive for people to participate in the network to expand and secure the public ledger.

Expending energy is essential to provide security for this new financial network.

The current phase of "mining bitcoins", where miners are incentivized with a high reward, is a clever way to get the network started. In other words: everyone who is greedily mining bitcoins today is helping to bootstrap this new financial system, whether they realize it or not.

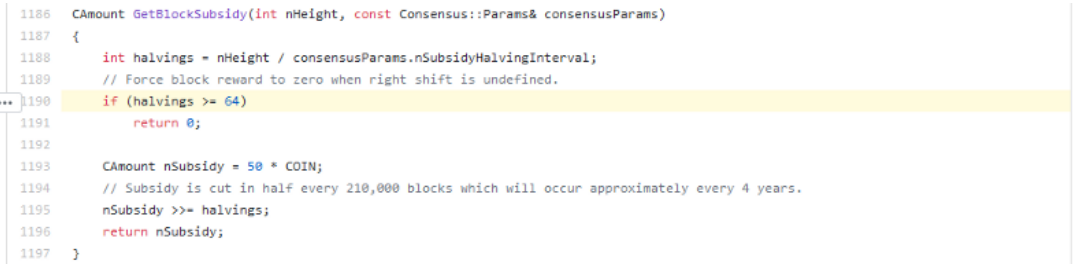
John Nash commenting on the game theoretical aspect of Satoshi's invention.

As mentioned above, Bitcoin's mining difficulty adjusts automatically, leading to a dynamic, self-correcting system. If mining—for whatever reason—gets more expensive, fewer people will mine at a profit, resulting in fewer people mining, lowering the mining difficulty. This, in turn, will make mining easier again and thus cheaper, which will incentivize more people to mine.

Over time, the financial incentive of running a mining operation will change. It follows that Bitcoin's energy consumption will change as well. The reason why change is inevitable is Bitcoin's block reward function which ensures a controlled, limited supply.

The block reward is halving every 210.000 blocks and will eventually reach zero, after 64 halvings. After the last of these halvings, miners will be left with transaction fees as the only financial reward for mining a new block.

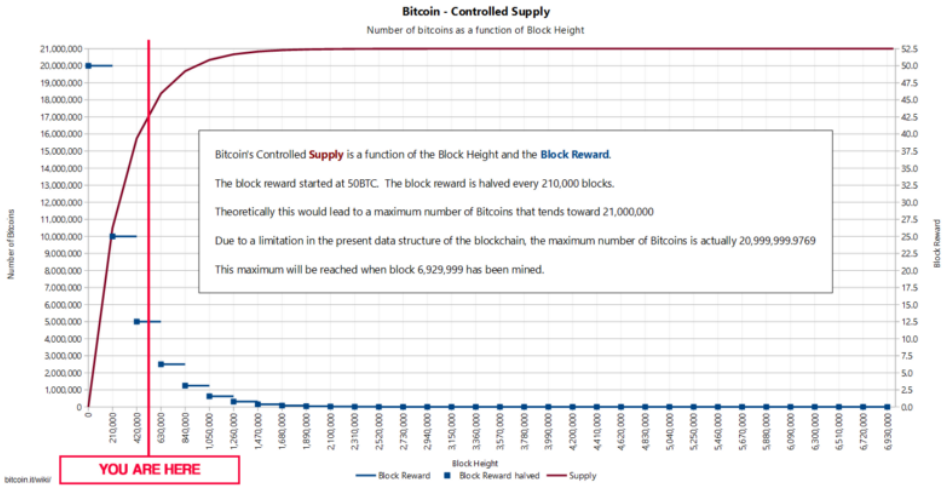
In other words: The "mining of new bitcoins" will eventually stop. The mining of valid blocks will continue after that.



```
1186  CAmount GetBlockSubsidy(int nHeight, const Consensus::Params& consensusParams)
1187  {
1188      int halvings = nHeight / consensusParams.nSubsidyHalvingInterval;
1189      // Force block reward to zero when right shift is undefined.
1190      if (halvings >= 64)
1191          return 0;
1192
1193      CAmount nSubsidy = 50 * COIN;
1194      // Subsidy is cut in half every 210,000 blocks which will occur approximately every 4 years.
1195      nSubsidy >>= halvings;
1196      return nSubsidy;
1197  }
```

In Bitcoin, code truly is law.

One could argue that we are currently in the bitcoin equivalent of the Gold Rush, where the reward for mining as well as the future projected reward far outstrips the investment and energy costs. While it is hard to estimate how much security is enough security, a case could be made that the Bitcoin network is currently "hypersecured" as a side-effect of this Gold Rush.



Bitcoin's controlled supply and block reward over time.

We are still in the early phases of Bitcoin's block reward phase, as the above graph shows.

Whether the adaption of bitcoin as a currency will be slow and steady, or exponential and parabolic, a continued exponential growth of energy consumption is very questionable. I would argue that excessive growth will give way to a somewhat sensible balance between security and energy consumption as the block reward approaches zero. Depending on the future value of bitcoin and the willingness of people to pay transaction fees, this balance might be leaning more towards security or more towards conservative use of energy.

Modern Blocks of Marble

Once you wrap your head around proof-of-work, it becomes more and more clear that the energy consumption of the Bitcoin network is not a bug, it's a feature. As far as we know, you can't cheat the laws of thermodynamics. Given that we don't have any world-shattering breakthroughs in physics, mathematics and/or quantum computing, expending energy is the only way to flip bits, and flipping bits is the only way to mine new blocks.

Unfortunately, we don't have an intuitive understanding of this new cryptographic world (yet). Fully grasping the importance of proof-of-work requires a deep-dive into a multitude of topics. We lack concise, easy, elegant explanations and metaphors. Hugo Nguyen did a great job explaining how proof-of-work links the abstract, digital world of bitcoin to our physical world:

"By attaching energy to a block, we give it "form", allowing it to have real weight & consequences in the physical world."*Hugo Nguyen*

Proof-of-work is essentially a mechanism to easily check the truthfulness of the statement "I worked really hard to create this thing". From that perspective, our new and fancy computational blocks are a bit like blocks of marble, and proof-of-work is a bit like looking at a beautiful marble statue. It is immediately obvious that a lot of work went into creating the statue. Cheating is extremely hard, because creating such a glorious statue without actually doing the work is pretty much impossible. You can't throw a block of marble against a wall and everything which is not David will fall off. It's not impossible, but it is very, very, *very* unlikely. Instead, you have to chisel away at the marble, and you have to do it properly and with care. One might argue that this is one of the reasons why great artworks are so valuable: a lot of thought, care and work was expended to create them.

Oldschool proof-of-work by Michelangelo. Photo by Jörg Bittner Unna

It is similarly unlikely to find valid blocks without actually doing the work. Like an ugly half-haphazardly chiseled statue, an invalid block can be simply thrown away. When you see a *valid* block, however, you immediately *know* a lot of work went into it.

In both cases, the artifacts themselves, the statue and the valid block, are in itself the proof of work.

My point is that understanding the nature of proof-of-work and the incentives of mining valid blocks, as well as the security properties and thus the value of proof-of-work, might help to shift the perspective from "energy wasted" to "energy used for creating something valuable". Most people value beautiful marble statues. A rising number of people value a chain of valid blocks.

Security Through Purity

Another feature disguised as a bug is the randomness of bitcoin's proof-of-work. A common suggestion for improvement is that we could use all this electricity to do something else, something *truly* useful, like finding prime numbers or compute protein foldings, in addition to securing the network.

Again, this objection to Bitcoin's proof-of-work algorithm is rooted in the assumption that finding valid blocks is inherently useless. It is not.

While introducing a secondary reward for doing the work might seem like a good idea, it actually introduces a security risk.

The problem with doing something else—something that other people might consider useful—is that that splits the reward. It means that miners have two reasons for which they are mining.*Andreas M. Antonopoulos*

Splitting the reward can lead to a situation where "it's more worthwhile to do the secondary function that it is to do the primary function". Bitcoin will never have this problem. Bitcoin guarantees its security by the purity of its proof-of-work algorithm.

If someone figures out a more energy-efficient way to secure an open, decentralized, censorship-resistant, permission- and trustless network for value exchange—without compromising one of these qualities—this hypothetical future network will eventually dethrone Bitcoin, solving this supposed energy problem. And no, proof-of-stake is probably not the answer.

In the future, we might find something which is even *more* suited to be an anchor for truth than energy. Until we do, we should stick to something we are extremely confident in: the laws of thermodynamics; the energy required to do the work in proof-of-work.

Conclusion

I hope to have planted the seed for a shift in perspective: that spending energy on proof-of-work is not a waste, but a worthwhile endeavor.

Understanding mining and proof-of-work in more detail might help to convince some of Bitcoin's critics and shift the perspective from "inefficient and wasteful" to "secure and censorship-resistant". Pointing out these nuances might also be helpful to understand that Bitcoin's energy consumption most strongly correlates with the network's security, and not with the adoption, usage, or utility of bitcoin. Even if the utility of the network and the price of bitcoin continues to increase exponentially, the energy consumption does not necessarily need to follow the same exponential trend. Gaining a better understanding of the Bitcoin network might also help to understand where other solutions fall short.

Satoshi's genius was to combine a bunch of clever tricks into a new economic game which creates a digital, scarce artifact, without central issuance. This artifact is backed by computation, and computation requires energy.

The current economic game is a game of walls and vaults, closed systems and centralized power. The new economic game is a game of hashes and blocks, public keys and private keys, based on mathematical proofs and physical reality. A game without gatekeepers, without central authorities, without censorship or discrimination.

The old rules have led to a system where money is valuable "because I say so", leading to magic tricks like fractional reserve banking, inflation to stimulate excessive consumption, and even hyperinflation because the temptation to print ever more money is simply irresistible.

The new rules might not be easy to understand. They might, however, lead to a new financial reality: a new economy based on sound money. We will all have to adapt to these rules and become familiar with the nuances of this new game. And we will have to come to terms with the fact that a finite resource has to be used to secure this new, decentralized economy. In the case of Bitcoin, this resource is energy.

The Bitcoin Lightning Network: A Technical Primer

By Joe Kendzicky

Posted June 5, 2018

TL;DR:

The Lightning Network is a protocol layer that seeks to provide instantaneous, trustless Bitcoin payments. In this article, I walk through the construction process for Lightning Channels and illustrate how multi-hop transfers are initiated. This article is the third piece in a multi-part series where I attempt to deep dive into notable cryptoasset projects.

Background

The Lightning Network is Layer 2 infrastructure built on top of the Bitcoin protocol, and hopes to increase transactional throughput. Bitcoin has a hardcoded upper bound limit on the number of transactions it can process. In traditional payment rails, ledgers are updated every few seconds and can achieve high degrees of scalability. These systems reach finality quickly and efficiently due to their centralized structure: *clients_communicate directly with the _master* server, who make ledger alterations in real time as notice is provided.

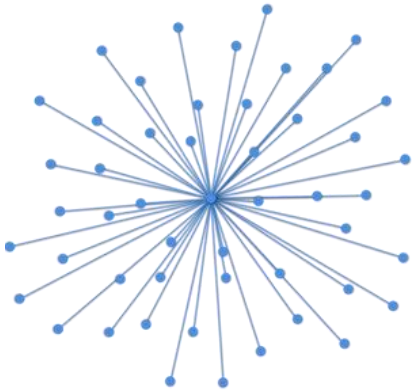


Image Source

Bitcoin faces inherent challenges since the system utilizes distributed architecture. When new information needs to be appended to the ledger, that information must be redundantly pushed across every participating server inside the network. These servers must parse through the data and reach consensual agreement on which transactions they intend to accept and write to database, and which to reject. The difficulty in this scenario arises when multiple servers have conflicting views on

transactional sequencing. Each node in the ecosystem maintains equivalent weight, so without top-down authority to establish a canonical vision, the system would eventually stall out if participating validators are unable to reach consensus.

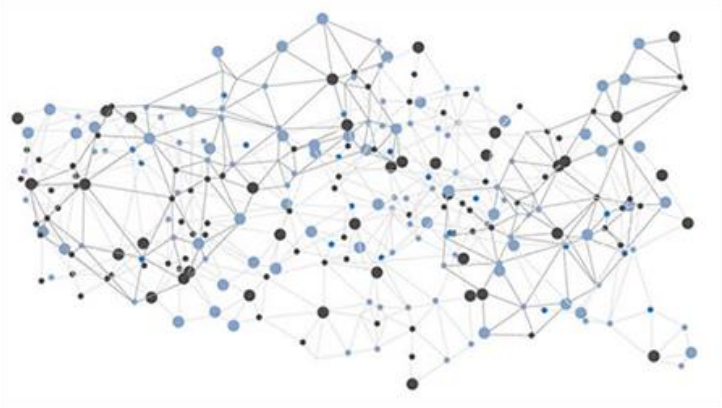


Image Source

Bitcoin introduces the concept of mining to guarantee network progression and prevent ledger fragmentation. Miners contribute computational power from specialized hardware to earn the right to propose ledger alterations during iteration rounds which occur roughly every 10 minutes. A mathematical challenge is included in each round. If a miner is able to find a solution, they earn the right to establish canonical vision of the ledger, which the rest of the network accepts based off protocol rules. When a claimant proposes a solution, other nodes can verify integrity of the solution. Peers will only recognize the claimant's ledger version if the solution is valid.

When we talk about "vision" of the ledger, we are referring to the construction of blocks. Blocks are aggregations of transactions compressed into a singular file unit. When a miner "solves" a block, they earn the right to inscribe their view of the ledger to the blockchain, an immutable database containing an archive of previous network transactions. Transactions are simply lines of code, so they have deterministic size. With the blocks having an upper bound limit at 1MB, the system can process ~7 transactions per second (tps). In contrast, networks like VISA can support ~50,000 tps.

Overview

The Lightning Network utilizes the concept of payment channels to provide bi-directional monetary transfers, and envisions a network with near-instantaneous speed, zero counterparty risk, and low fees. In doing so, the Lightning Network aims to alleviate scalability concerns surrounding the Bitcoin protocol. The system routes around the bottlenecks of universal consensus by settling transactions off chain,

avoiding latency and computational redundancies that plague blockchains. Lightning claims transactional processing capabilities in the millions of tps.

Funding Payment Channel

The first step involves an initial funding transaction where each party deposits BTC into a 2-of-2 multisignature address. Once deposited, each participant has full guarantee of security, since any forward movement of funds will require signature authentication from both parties. But what if the channel is unable to progress forward after the funding transaction? **If the opposing party becomes unresponsive or loses their private key, any balance locked up in that channel is permanently lost.** Thus, both sides of the agreement need insurance against counterparty risk that may ensue.

To solve this dilemma, users draft refund transactions and have their counterparty sign. These transactions are constructed before either individual deposit to the multisignature address, and allows for revocation of the original funds back to channel depositors. Bob asks Alice to draft a settlement transaction that refunds his deposit back to himself. Alice complies with the request, drafts the message, and signs it with her key. She then returns it to Bob. In the process, she also includes a similar refund script for her bitcoins. Bob reviews the transaction, and if the outputs align with his specifications, attaches his signature to the message, relaying it back to Alice. Both members now possess a symmetric transaction which they tuck away as leverage for a future mishap. In the event either party becomes unresponsive, the counterparty can simply broadcast the transaction to the network, creating an escape route to withdrawal their balance from the multisig. Both individuals are now protected and can deposit to the channel with full reassurance.

Commitment Advances

With funds locked up in the multisig account, a "channel" is now created. Participants can issue fully valid transaction scripts to one another via private medium, and both parties can accept these instruments of payment as valid without having to broadcast the payment on-chain. **In doing so, these commitments act as a form of *promissory note* with enforceable guarantees backed by the Bitcoin blockchain, all while avoiding the bottlenecks and costs of universal consensus**. If circumstance requires, either party can push the latest commitment version to the blockchain and close out the channel without requiring approval from their counterparty.

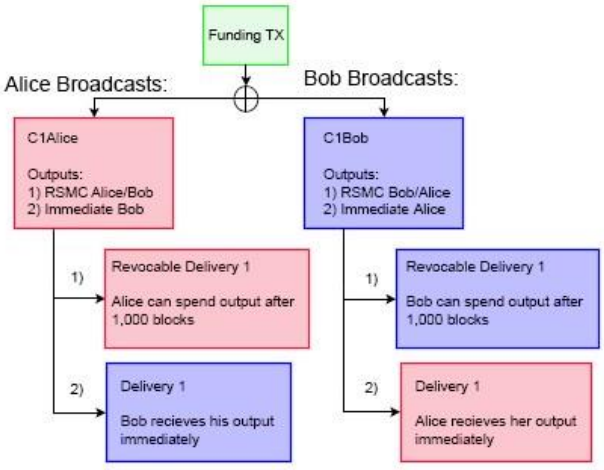
Problems arise when it becomes economically advantageous for a participant to push a previous commitment to the blockchain. Returning to our example, after both depositing a 1 BTC balance, Bob sends 0.5 BTC to Alice inside the channel. His

balance will now show 0.5 BTC, and Alice's will read 1.5 BTC. But remember, Bob has his initial refund TX, signed by Alice, that allocates 1 BTC back to himself. Bob is now incentivized to push this outdated transaction to the network and make off with Alice's money. Thus, we need some method to invalidate previous commitments.

Commitment Transactions

When Bob and Alice want to advance the state of the channel, they need a way to autonomously enforce their contracts. This is done through commitment transactions. Suppose Bob wishes to send Alice 0.5 BTC. Each party creates two near-identical transactions spending the same input values. These transactions operate similar to a RBF or a Doublespend- if both transactions are pushed to the blockchain, only one of them will ultimately confirm and be appended to the ledger since they reference the same input values. Bob and Alice carefully construct these transactions in a manner that makes it deterministically provable which will be included into a block first.

Bob creates a transaction by referencing a set of outputs, and signs with his key. We call this transaction C1Bob (Commitment1Bob), which he forwards to Alice. Alice mirrors this action, creating C1Alice and forwards to Bob. Because these transactions are originating from the 2-of-2 multisig, neither party's script is valid until *both* signatures are transcribed. Once Bob and Alice put their stamp of approval on each other's commitments, they are voluntarily accepting the potential of their counterparty broadcast the transaction at any point in the future (thereby closing the channel). Bob cannot push the transaction he constructed to the network, since he doesn't possess Alice's private key. Bob can only broadcast Alice's version, and Alice can only broadcast Bob's.



The above illustration describes the redemption paths if a commitment were broadcast on-chain. If Alice were to push her transaction to the network, she would

initiate two events. The first would immediately unlock Bob's balance, allowing him to transfer his funds. The second would trigger a countdown on her funds. Alice will have to wait 1,000 blocks in order for her outputs to unlock. Once this timespan has elapsed, her funds will become available for redemption. This process is mirrored on Bob's commitment. If he pushes his version to the network, Alice's funds are immediately unlocked, while he has to wait 1,000 blocks. These lockup intervals are set to mitigate counterparty risk.

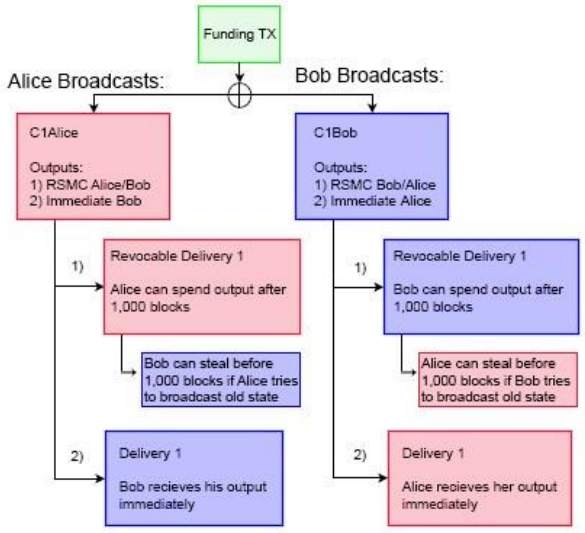
We introduce the concept of Revocable Sequence Maturity Contracts (RSMC) as a means to invalidate previous commitments. This occurs via the scripting flag CHECKSEQUENCEVERIFY (CSV). CSV's are a way to dynamically lock up bitcoins over a predefined time interval, and is enforced by the Bitcoin blockchain rather than users themselves. CSV checks for the current block height (aka the *sequence*) from the moment the transaction is included in a block, and *verifies_that the encumbrance scripts are met. In the example above, it is the CSV encumbrance in the transaction that forces Alice/Bob to wait 1,000 blocks for their funds to become redeemable. This creates a _bonded deposit* window where a plaintiff can present a breached remedy tool in the event the counterparty tries to broadcast an outdated commitment.

Creating Breached Remedy Commitments

When Bob and Alice want to advance the state of the channel, they need a way to invalidate previous commitments. Bob and Alice repeat the commitment process by constructing a new 2-of-2 multisig account (aka C2Bob, C2Alice) with a fresh set of keys. They reference their outputs, enact similar 1,000 block CSV scripts, sign the transaction with their own keys and pass along to their counterparty. Their counterparty tucks this transaction away. **However, before finalizing the new C2Bob/C2Alice commitment schemes, both parties disclose their private keys used in C1Bob/C1Alice.** Once this occurs, each party is protected from publication of outdated commitments.

As mentioned earlier, if Bob closes out the channel, Alice's funds are immediately spendable. Bob's money on the other hand is locked up for 1,000 blocks by the CSV encumbrance. If Bob tries to cheat the system by broadcasting an outdated commitment whenever financially incentivizing to do so, those funds are not immediately accessible. Alice will see that Bob is trying to cheat her, and use her breach remedy "tool". This tool allows Alice to spend the 1,000 block encumbered funds *immediately* if she can provide Bob's private key. Alice is capable of fulfilling this obligation now that the channel state has advanced, because Bob has voluntarily relinquished the key to her in the last round. Thus, Alice can not only ensure that she won't be cheated out of the BTC she is owed, but will be able to walk away with the entirety of Bob's balance, making additional money. Thus, Bob is

highly incentivized not to try and cheat the system by publishing outdated commitments, since Alice will be able to walk with his entire deposit. Conversely, if Alice tries to pull a similar trick on Bob, he can walk with the entirety of her deposit. This creates incentive models where both parties are highly incentivized to act altruistically.



Cooperative Channel Closeout

When either party wants to close out the channel, they can do so cooperatively by disregarding all outstanding *promissory notes* and constructing a normal transaction from the original 2-of-2 escrow. This transaction would pay out the respective balance to each member, based off the most recent commitments. **Because the outstanding *promissory notes* are backed with full guarantee by the blockchain, both parties have an incentive to collaborate**. Neither individual has to go through the frictionary process of paying additional on-chain fees, nor lose out on opportunity costs of time having their BTC locked up by the CSV encumbrances for 1,000 blocks.

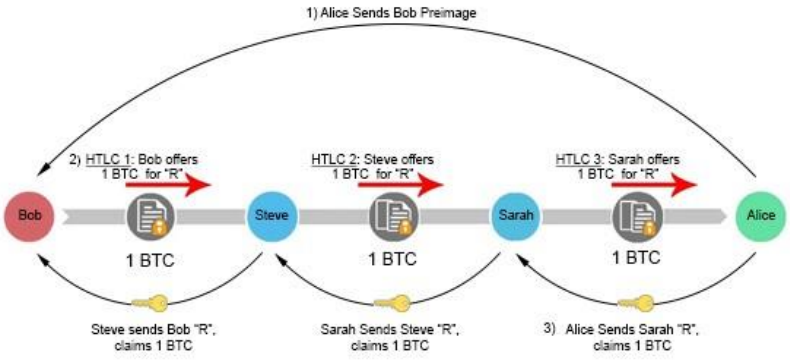
Hashed Timelock Contracts (HTLC's) and Multi-hop Transfers

HTLC's are forms of transactional encumbrances which use hashlocks (locking scripts that ensure certain data is known) and timelocks (restricts future spending of outputs until a predetermined date) as a way to enforce provisions on a transaction. Both types of encumbrances are enforced by the blockchain rather than channel counterparties. The concept is fairly simple, and serves as a way to extend payment channels beyond a bi-directional state. Lightning Network will have the ability to route channels deterministically through multiple parties through a process called multi-hop transfers. At first, Lightning might not be very appealing unless two

participants plan to remunerate very frequently, since opening a new channel requires locking up assets via an on-chain broadcasted transaction. Bob having unique channels with many participants means less money in his wallet for discretionary spending, significantly reducing the versatility of his funds. Lightning alleviates these concerns by introducing an effective path finding algorithm between network participants, and linking their channels together via HTLC's. Bob and Alice are two individuals who want to transact, but don't have an existing channel open. If both parties have a mutual channel connection with Steve, they can still route the transaction with full guarantee of atomic settlement. This works by Bob paying Steve, who in turn pays Alice. Bob has now trustlessly paid Alice without needing to open a channel with her. If the relationships between participants are extremely isolated, we can keep introducing more intermediaries to form a lineage robust enough to facilitate payments.

Bob(the sender) initiates the multi-hop process by communicating directly with Alice(the beneficiary). Bobs asks Alice to create a randomly generated secret *R*, which remains private to Alice. Bob asks Alice for a hash of *R*, called the preimage, but not the plaintext version of *R* itself. Bob subsequently specifies only to disclose *R* to an intermediary party, Steve, in exchange for 1 BTC.

So, Alice hashes *R*, and sends a copy of the preimage to Bob. Bob takes this preimage to Steve, and offers a 1 BTC bounty if he can produce the hash's plaintext version, *R*. Steve accepts the offer, and goes to Alice with an offering of 1 BTC in exchange for the secret value. Note that in this situation, Steve front runs his own capital to make this exchange with Alice. Alice, seeing this offer of 1 BTC in exchange for an arbitrary secret *R*, accepts the proposition and gives the value of *R* to Steve, just as she was instructed earlier by Bob. Steve then hands *R* to Bob in order to claim his bounty. In this example, Bob has found a trustless way to pay Alice, without having to go through the burden of opening a channel with her. If Bob and Alice lack a mutual contact to route the channel through, we can keep introducing more intermediary liquidity providers until a connection is made. For example, if Bob has an open channel with Steve, and Alice has an open channel with Sarah, and Sarah and Steve have a channel together, a payment can be initiated.



CHECKLOCKTIMEVERIFY (CLTV) vs. CHECKSEQUENCEVERIFY (CSV)

What is the difference between a CLTV and a CSV? Both are examples of timelock encumbrances, and are used to accomplish similar goals.

Suppose a CLTV encumbrance is placed on an output for 10 blocks. The current BTC block height is b=500,000. Once the blockchain hits b=500,010 the outputs unlock and become spendable. The time at which the original transaction gets a confirmation is irrelevant to the spender.

In contrast, a CSV script is based entirely on the time the original transaction is included into a block. Suppose a CSV script is placed on an output for 10 blocks. The current BTC block is b= 500,000. Once this transaction is broadcast, it sits unconfirmed for 5 blocks. After 5 blocks ensue, it finally gets picked up and included at b=500,005. In this scenario, the timer begins once that transaction gets its first confirmation. The CSV encumbered output doesn't become spendable until 10 subsequent blocks at b=500,015. Conversely, if the original transaction receives its first confirmation at b=500,003 then the outputs becomes spendable at b=500,013.

In summary, a CSV sets a dynamic encumbrance that makes an output spendable after a specified number of confirmations once the original transaction is included in a block. In contrast, with CLTV you are specifying when the output will become spendable based off block height. This means that the output's encumbrance status is completely independent of the mining process.

Constructing Hashed Timelock Contracts

In our previous example, we presented a basic overview of how a multihop transfer can occur, but failed to articulate how to create an enforceable contract on the blockchain to facilitate those functions. For example, what if Alice fails to produce the secret value after Bob transfers her the bitcoin? Or what if Bob revokes his

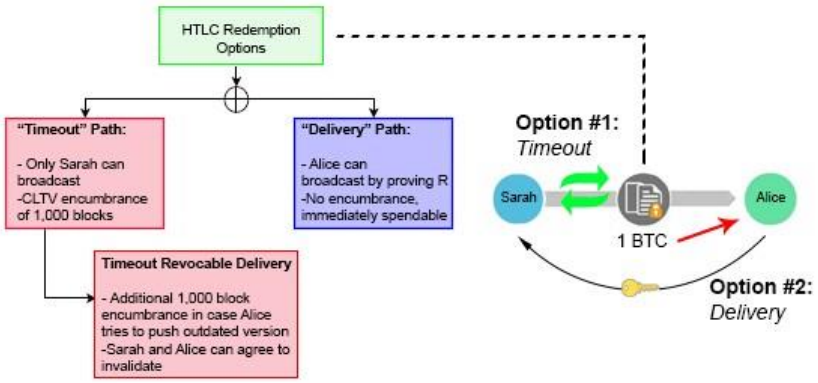
bounty commitment to Steve after acquiring the secret from Alice? In both scenarios, Steve has lost money.

In order to create a trustless layer of commitments, we build off similar RSMC properties outlined in earlier sections, but add a few twists. After Bob communicates directly with Alice and receives a copy of her preimage, he constructs a hashed-timelock contract (HTLC) transaction with Steve. This contract has two paths for output redemption. The first is a "delivery" path which sends Steve 1 BTC immediately if he can produce the secret *R*. The second is a "timeout" path which allows Bob to refund himself in the event Steve cannot produce the secret. This is accomplished using a CLTV flag instead of the CSV as in previous examples.

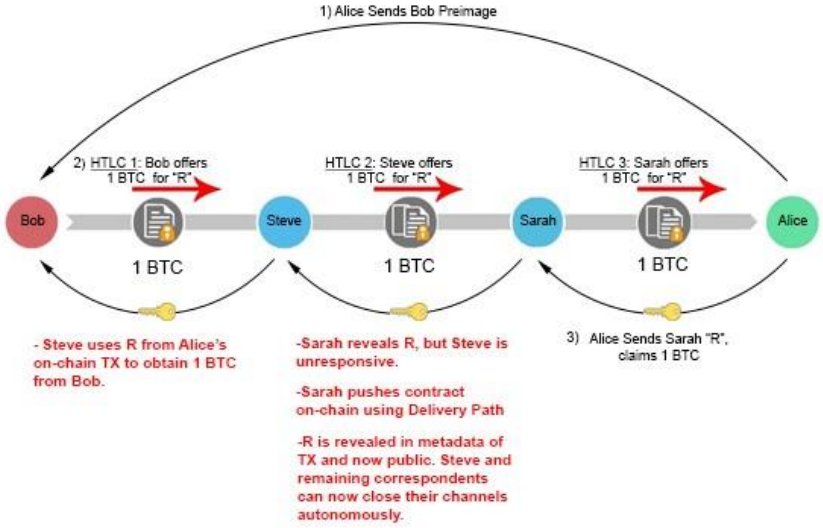
In the transactional script, Bob sets the timeout length of the CTLV to 1,000 blocks. This means Steve essentially has 1,000 blocks to obtain *R* from Alice and claim the 1 BTC bounty via the "delivery" path. If he waits longer than this time, he loses guaranteed insurance that he can claim the bounty safely. Steve mirrors this same transactional script with Alice, front running his own personal capital in the process. If Alice wants to claim the 1 BTC sitting in escrow, all she needs to do is reveal the secret *R*. Once Steve has *R*, he can turn around and use it to pull the 1 BTC out of escrow sitting between him and Bob. Everyone gets paid.

Importantly though, these "timeout" intervals must decrease in length as the chain progresses right to left. The timeout between Alice and Steve must expire earlier than the timeout between Steve and Bob. If they expire simultaneously, Bob runs the risk of transferring his funds to Alice near the end of expiration, and then having Bob's "timeout" unlocking before he has time to grab his funds out of escrow. In this scenario, Steve would be left doing the bagholding, since he front ran capital to Alice but was not able to collect from Bob. To make matters even more challenging, blocks are solved in random 10-minute intervals. There is no inherent guarantee that a subsequent block will be solved 10 minutes after a previous. It could happen 1 second afterward. This is why CLTVs are used instead of CSVs. Thus, it is imperative that participants provide ample blocks between channel "timeouts" to prevent loss of funds.

If Steve cannot obtain *R* from Alice (she is a fraudulent actor, becomes unresponsive etc.), nothing is hurt. He simply lets the channel expire and revokes his money out of the escrow by using the "timeout" path. This will set off a chain reaction, where Bob will revoke his funds out of escrow once they timeout. Though the parties may experience opportunity costs of locked-up capital, they have full reassurance that they can ultimately reclaim those escrowed funds.



Interestingly, disruption of the channel somewhere along the line does not destroy payment guarantee, but actually strengthens it. Suppose Sarah fulfills her end of the obligation and provides Steve with *R*, but Steve remains unresponsive and does not update their channel balance. In such a situation, Sarah is still capable of obtaining the 1 BTC she is owed through the HTLC contract. If Sarah uses the "Delivery" Path, *R* becomes publicly available on the blockchain; she has to disclose it in the metadata of the transaction to unlock the encumbrance and receive her BTC. Intermediary liquidity providers can extract this information off the blockchain and use it to unlock their escrow channels immediately, without ever having to wait for their correspondent to reveal *R* to them. This structure provides cryptographic certainty that each claimant will be able to receive their capital, so long as they push the TX before the CLTV encumbrance expires.



Recap

C2Bob is Broadcast (Only Bob can broadcast):

1. Immediate transfer of outstanding balance to Alice
2. 1,000 block redeemable lockup to Bob for his outstanding balance
    a. If Bob tries to cheat, Alice can steal his entire deposit
3. HTLC commitment redemption by whatever party is front running capital for the counterparty
    a. If Bob is front running for Alice, Bob can capture the bounty by immediately publishing *R* via the "delivery" path (and vice versa).
    b. Alice can refund herself the escrowed bounty after 1,000 blocks if Bob cannot publish *R*. She does this using the "timeout" path. This route will include an additional 1,000 block lockup period, so Bob can punish Alice if she tries to cheat by publishing an outdated commitment.

***At this point, the HTLC needs to be terminated. If they want the channel to remain open, then they will construct a new C3Bob/C3Alice displaying the updated balances. If Bob can prove *R*, then Alice will reflect this in the new state C3Alice. If Bob cannot produce *R*, then it will not be updated in the new C3Alice. As always, Bob and Alice will use the breach remedy "tool" outlined earlier to protect themselves before signing C3-Commitments.

Sequence of events for a C2Bob broadcast

C2Alice is Broadcast (Only Alice can broadcast):

1. Immediate transfer of outstanding balance to Bob
2. 1,000 block redeemable lockup to Alice for her outstanding balance
    a. If Alice tries to cheat, Bob can steal her entire deposit
3. HTLC commitment redemption by whatever party is front running capital for the counterparty
    a. If Alice is front running for Bob, Alice can capture the bounty by immediately publishing *R* via the "delivery" path (and vice versa).
    b. Bob can refund himself the escrowed bounty after 1,000 blocks if Alice cannot publish *R*. He does this using the "timeout" path. This route will include an additional 1,000 block lockup period, so Alice can punish Bob if he tries to cheat by publishing an outdated commitment.

***At this point, the HTLC needs to be terminated. If they want the channel to remain open, then they will construct a new C3Bob/C3Alice displaying the updated balances. If Alice can prove R, then Bob will reflect this in the new state C3Bob. If Alice cannot produce R, then it will not be updated in the new C3Bob. As always, Bob and Alice will use the breach remedy "tool" outlined earlier to protect themselves before signing C3-Commitments.

Sequence of events for a C2Alice broadcast

Final Closeout

The beautiful thing about Lightning Network is that all these described provisions will rarely take place on-chain. **Participants can avoid broadcast of all these intermediary steps and simply pay one another out at the conclusion of the channel using traditional payment terms.** These intermediary technicalities exist for the sole purpose of protection. Participants essentially load a gun, then handing it over to the opposing channel member with instructions to shoot if they act dishonestly. Incentives are aligned to follow the rules by constructing channel operations in such a manner. Thus, altruistic behavior is a rational assumption. If participants act dishonestly or become disconnected for extended periods, the Bitcoin blockchain acts as an enforcement mechanism to ensure integrity of commitment balances.

Follow me on twitter for more Crypto insight!

On Schelling points, network effects and Lindy: Inherent properties of communication

Willem Van Den Bergh

June 29, 2018

The above mentioned phenomena are widely known among Maximalists and although they seem to apply to Bitcoin on an intuitive level, I wanted to define these principles on a higher resolution. Only after establishing this framework in detail can we better understand why these effects make Bitcoin such an all-consuming force to contend with. Furthermore, it will become evident why "successful" alternative blockchains like Ethereum cannot compete with Bitcoin. (Disclaimer: this article presumes a basic understanding of the above mentioned effects).

What really got me puzzled at first was the insight of Giacomo Zucco during episode 0.14.0 of the Noded podcast (hosted by Pierre Rochard and Michael Goldstein). There he elaborated on his insightful observation that although capitalism is an immensely powerful tool for the advancement of society, there are some anomalies that do not abide by these traditional properties of free market capitalism.

Unlike all other products, protocols do not benefit from the perpetual struggle of competing markets as one would assume to be the case in a healthy capitalist environment. Rather the opposite is true; **protocols tend to converge to one sole victor over time** who subsequently becomes the dominant monopoly player within its respective market. But what do we mean exactly by protocols? Is it constrained to computer protocols like HTML, HTTP and TCP/IP? All proven to be monopoly king within their respective markets. Or, just as Zucco suggested by referring to the English language as a protocol we all concede to in this globalized world, is there a bigger picture? Let us investigate a good example of a market that has benefited from this tendency towards monopoly to illustrate the point.

Video tape format war:

In the early seventies the time and technology was getting ripe for the conquest of the home cinema market. For the first time in history it would be possible for millions of households to enjoy the full scope of movies from the comfort of their own houses while at the same time also making it possible to record public TV broadcasts. The battle for the consumer was commencing and what ensued was a 10 year death struggle between the 2 predominant market leaders; JVC's VHS

cassette (video home system) and Sony's Betamax. Both products hit the market in 1975 with very similar features. Though most people only remember the two mentioned above, the late seventies offered a wide variety of alternatives (for example Avco's cartrivision). All of whom were destined for a quick demise.

The advantages of both competitors became clear, once the market started to develop. VHS had a slightly lower retail price and offered a recording time of 120 minutes, while Betamax was putting emphasis on video quality but only allowed for 60 minutes of recording. The battle for the US consumer was gathering steam but over the coming years it proved to be easier for JVC to enhance the product quality while Sony was struggling to increase its recording time. The Americans started to favour VHS and by the end of the 1970's JVC controlled 70% of the US market. In 1980 Europe started to warm up to this new medium and families all over the continent started to buy into the video recorder. Though by this point both availability and a better optimized economy of scale led a lot of households to adopt VHS over Betamax. **VHS was the emerging Schelling point in the space of home cinema**. Betamax kept competing during the early 80's but its success continued to dwindle and by 1986 its global market share had dropped to only 7.5%. Shortly after Sony threw in the towel and VHS became the monopoly brand in the sector. Any competition thereafter proved futile as **VHS now enjoyed the fully fledged benefits of the Lindy Effect.**

Other examples, all with equally fascinating origin stories, that enjoy the **network monopoly effect**include: Facebook, Amazon, PostgreSQL, the English language, the dollar, google, USB ports, CD, HTML, Windows, bit torrent, YouTube, the metric system, TCP/IP, HTTP, Binary code, Wikipedia..

There is one binding factor that this broad collection of networks all share in common: They all belong to the sphere of communication. Whether it's VHS recorders that provide an analogue interface model to communicate movies from tape to screen, TCP/IP that makes it possible for all email clients to send content to each other or USB ports that allow multimedia devices to have a direct line of information exchange. **Communication is their core function.**In any other sphere you can name, whether it be entertainment, sports, consumable or durable good, services, arts etc, there is no inherent tendency towards monoculture. Rather the opposite is true, when one of these spheres tends towards monopoly, the product quality becomes increasingly stale and the market starts to collapse due to falling revenue and lack of diversity. People only buy out of pure necessity or lack of alternatives. These markets cannot function without the essential stimulus of competition. **Communication truly seems to be the only sphere that successfully escapes the beneficial dance of perpetual competing capitalist markets.**It's even worse than that, if there is choice within a certain communication protocol market, it seems to diminish cooperation and efficiency rather than enhancing it. To be clear, in the early stages, fierce competition is more than welcome; it's the only way to

arrive at a broad consensus among all market participants. The statement above just highlights the outcome, not the initial selection process. Note that for this thesis hardware communication is defined as equipment that interacts in a physical manner, mainly this interaction happens between a media carrier (for example a DVD) and a media decoder (DVD player). This definition allows us to make a clear distinction between communication hardware that evolves towards a monopoly (CD, DVD etc.) and communication hardware that does not evolve towards a monopoly (Personal Computer, Smartphone etc.)

The case for monopoly:

So we've established that communication protocols in general tend towards monopoly. This definitely doesn't need to be a bad thing, quite the opposite. There are three main reasons why I think communication is antithetical to market competition in the long run.

A new form of communication requires a considerable adaptation period; it needs to be learned in the case of humans, developed in the case of software or designed in the case of hardware. These adaptations represent the **sunken cost** on behalf of all participants in that specific communication network. This considerable sunken cost entrenches the user of that network and makes them unwilling to change to a different protocol on the basis of some arbitrary additions or improvements. This is what you might call protocol loyalty. It signifies the inefficiency of repeatedly switching between different communication networks.

Furthermore, the division of the market between several competing protocols represents a **problem of compatibility**. Choosing one communication model over the other immediately connects you to all individuals within that group but at the same time prevents you from having any communication to people who prefer another model. The different protocols become isolated from each other and all networks start to form closed-off parallel communities. This unavoidably leads to the fragmentation of knowledge and information, which in turn results in less optimal use of time and resources. **Division of labor cannot express itself to its fullest in a fragmented society.**This compatibility problem only occurs in the sphere of communication. All the other spheres do not suffer from a diminished potential of collaboration as a result of having several competing products. We don't all need the same brand of car in order to get along in traffic, we don't all need to wear the same brand of clothes in order to fulfill the socially acceptable standard of appearance, we don't all need to watch the same sport in order to have entertaining high level competition etc.

Finally I would add that protocols are not static but organic of nature. They can **adapt** to new circumstances or implement solutions when confronted with

previously unknown flaws. Without this ability to adapt or evolve, communication networks would not be able to persist long enough to amortize sunken costs.

Money as communication

Money is one of the most effective forms of communication known to mankind. As Nick Szabo defines it in "Shelling out": "Money converts the division of labor problem from a prisoner's dilemma into a simple swap". It is the communication tool that allowed us to scale up from barter based tribes no larger than the Dunbar number into thriving societies and civilizations with millions of people cooperating in peace. **Money is the language in which we communicate value to one another**. Since humans are social beings and we have a proclivity to create value systems as a tool to make sense out of our environment and the world, despite what some utopians might claim, **there will always be a need for money,** no matter how advanced or altruistic the society. Because money is a form of communication we can therefor assume that it will act as any other communication protocol; it will converge to a single protocol (in Austrian economics this market chosen protocol is called the most saleable commodity). This is also proven by history, which again and again converges to gold.

It is through this reference frame that we can understand precisely how the following three effects synergistically feed into all forms of communication (money being one of the most important):

Network effect:

This is the driving force behind any emerging form of communication. As famous network effect pioneer W. Brian Arthur puts it "Modern, complex technologies often display increasing returns to adoption in that the more they are adopted, the more experience is gained with them, and the more they are improved" (from his famous paper "Competing technologies, increasing returns, and lock-in by historical events"). This of course implies there is to some degree a randomness effect at play because early on small events can sway the adopters in one direction or the other creating a feedback loop which can lead to the lesser protocol becoming the monopoly (VHS was considered inferior to Betamax in the seventies). Although the best protocol doesn't necessarily win, it's important to point out that there is only room for very little variation between competing candidates. **There is an infinite amount of possible formats that can exist as a protocol within a specific communication domain, but there is only a very tiny amount of viable formats that can pass the test of the free market within that domain.**Despite the fact that viable contenders always try to promote themselves by accentuating how different they are from one another, in essence they only diverge in the details. From a broader perspective, VHS and Betamax are almost identical. The whole video cassette competition took place within a very narrow set of logistical and

technological boundaries. It was the details and minor price differences that proved pivotal. As a comparison; the differences between Ethereum and Bitcoin are more substantial than those of VHS and Betamax ever were. Claiming that Ethereum competes with Bitcoin is absolutely preposterous. It's like saying Atari Pong was competing with VHS, a straight out idiotic proposition (more on this later).

Betamax and VHS (left) Atari Pong (right)

Hardware communication networks also have another factor at work, the economy of scale. Creating another layer of feedback loops for the protocol in the lead. This is less of an aspect in software technologies, though open source projects have incremental advantages with growing adoption as a consequence of Linus's Law; "given enough eyeballs, all bugs are shallow".

And then there is the most important factor of the network effect, Metcalfe's law. This is a well documented and well known aspect of networks. So without going into too much details: Metcalfe's law states that a network becomes proportionally more valuable the more users it has. The relationship between the network value and amount of users is n^2. Where n is the amount of users and n^2 is the value of the network. This makes sense at an intuitive level as the larger the group of users gets the more unique possible connections can be formed which in turn increases the functionality of the network. But the theory also holds up in practice when examining the vast amount of data we now have available since the mainstream adoption of the internet (see "Empirical validation of Metcalfe's law: How Internet usage patterns have changed over time" by António Madureira).

Both the Schelling point and the Lindy effect can be considered a subcategory of the network effect.

Schelling point:

"A Schelling point is a solution that people will tend to use in the absence of communication, because it seems natural, special, or relevant to them". The classic definition of the term Schelling point does not directly indicate it has special relevance to emerging communication technologies, but in my honest opinion, it does. The description bellow is a generalization of the mechanism that takes place when the market is sorting out who will become the monopoly.

During the first years of a new emerging technology, people mainly show interest in it due to its novelty. People didn't really care if that new gray box underneath their TV was compatible with VHS or Betamax, they just wanted that home cinema experience. It's hard enough already to figure out how this new technology can even possibly record live broadcasts! Even more problematic, they had no reference point or experience to properly asses the quality of the products being offered. **The Schelling point had not revealed itself yet.** But as the market matures, stakes rose and the consumer got smarter and more informed, people wanted their specific choice of movies and they wanted one universal recorder to play them all. So they were forced to make strategic decisions, they wanted to be on the side of the winner! Will my local store offer mainly VHS or Betamax? And in 5 years, will I still be able to use my recorder? So to the best of their incomplete information, they tried to pick the network which would survive in the long run. They actively attempted to select the Schelling point product. A maturing market can stay in this period of flux for quite some time, but once a Schelling point starts to gather steam, things can move quickly and a **lock-in**is imminent. Again bear in mind that the Schelling point can only shift between different protocols that are almost identical, the free market is very intolerant of protocols that stray too far from the narrow viable format formula.

Lindy effect:

The Lindy effect is the concept that the future life expectancy of a technology is in proportion to its current age. It is the final stage of a communication technology and comes into full effect once lock-in is established. Let me use the metaphor of W. Brian Arthur to explain: Imagine an infinitely long bowling lane. When you make a near perfect throw, the bowling ball can stay in the middle for an extensive amount of time, but at some point a divergence has to take place towards the gutter one way or the other. From that moment on the direction is virtually irreversible and the Schelling point has revealed itself, once the ball hits the gutter it is locked-in and the Lindy effect reaches maximum enforcement. In this case the emerging communication market is the bowling ball and the gutters resemble competing protocols. This is also what happened in the VHS-Betamax feud. For some years it

could have gone either way, predicting the outcome at this point was pure speculation. But then VHS started to take the upper hand in Europe and all of a sudden the **lock-in**happened, sealing the fate of Betamax. I believe the main power of the Lindy effect lies in the irreversibility of acquired monopolies through lock-in. **It transforms the sunken costs of all participants in aggregate into an intolerant and permanent status quo established by free market consensus making**. Especially good examples of protocols that benefitted from the Lindy effect are TCP/IP, HTML and HTTP.

Next generation technology: Lindy cycles

All the above sounds really nice, but if the story ends here then we would have no way to break through any Lindy effect ever, including that of the dollar. Monopolies would stay monopolies and that's that. So let us once again revisit our video recorder example. No story truly lasts forever, and VHS had a long and dominant run. But times change, and technologies change even faster. When the DVD came along, a major transformation had taken place in society. Computers slowly but surely started to compete with the classical TV set in our living rooms. The world was moving from an analogue society to a digital one. And with a digital world came digital media. The Lindy Cycle of analogue video recording had come to an end.

It's not that the VHS Lindy effect became obsolete for some random reason. But the DVD was a totally different and improved experience altogether. **DVD is the next generation technology in the video communication market.**Where VHS was the undisputed king in the realm of analogue video, the DVD represented an improvement of several orders of magnitude because of its digital nature. Vastly better video quality, longer play times, easy scene selection (no more rewinding), great interface possibilities, multiple audio tracks, deleted scenes… It is this kind of innovation that breaks open the Lindy effect. Only a paradigm shift justifies the time and energy expenditure needed to make the long and burdensome transition from one protocol to another. During this transition period a lot of logistical, cognitive and financial sacrifices have to be made on behalf of the network users. The DVD passed this test with flying colours, it justified the abandonment of sunken costs that VHS represented. It is also worth mentioning that you can be the holder of the Lindy effect of a next generation technology even before you have broken up the previous generation Lindy effect. Lindy Cycle's of succeeding technologies can temporarily overlap during the adoption phase of the next generation technology. For example: VCD was defeated by DVD in the US markets well before VHS dominance in the video space had ended.

The case for Bitcoin

I believe Bitcoin is the seminal improvement in the money technology language that will lead to the breakup of the current Lindy effect enjoyed by our current

money protocol monopoly aka the dollar.I understand that there is a huge amount of alternative currencies but since the dollar is the world reserve currency it effectively functions as the global monopoly of money. I am not going to lay out the full history of money and its many transitions from protocol to protocol through time, but please do check out Nick Szabo's "Shelling out" and "Collecting metal" as they make a great summary of our early monetary history. The period that is relevant to this discussion is the last ~ 150 years.

The gold standard:

Though a lot of empires and tribes have used gold in one way or another as a monetary standard throughout history (and consequently met their demise after abandoning it), the most recent and globally implemented example of this is La Belle Époque, spanning from 1871 to 1913.

Considered by many as the pinnacle of human endeavour and prosperity, the latter half of the nineteenth century up until World War 1 was an era of unprecedented sound money. During this economic and technological boom the US and all the prominent European countries worked together under this standard. A further improvement was made on top of this communication protocol by issuing 100% redeemable bank notes. These were a lot easier to carry around and allowed for smaller purchases, thus greatly improving the portability and divisibility of gold. They started out as a great second layer solution to the limitations of gold but little did we know how much these bank notes were going to be abused and exploited by nation states in the coming century, ultimately leading to the demise of the gold standard. The more these notes were adopted by the general public, the less need there was to hold physical gold. As a consequence gold became more and more centralized at the banks due to the logistical benefits this entailed (less and less settlement costs). Over time this process put the responsibility of maintaining the gold protocol in the hands of less and less actors, who subsequently gained increasing amounts of power. Generation after generation the general populace became more disenfranchised from the superior proposition that sound money can offer society, it was a slow collective amnesia event. Money became easy, and debasement became the norm. **Over time, gold always consolidates under the control of the few, be it emperors or central banks. This is the quintessential flaw of gold and it has been exploited many times in the course of history.**A famous example is the debasement of the Aureus golden coin issued by Julius Caesar. Over the centuries it got continuously debased (same is true for the silver Denarius) until finally leading to the collapse of the Western Roman empire. For this reason I do not consider the dollar as a separate Lindy effect holder as compared to the gold standard Lindy effect. It doesn't matter that the dollar is completely fiat and without gold backing, it is rooted in the gold standard and could never have existed without this prehistory. The dollar is simply the contemporary representative of a gold standard in its final stage of decay. There have been many of these gold standard

iterations before, and if Bitcoin fails for whatever reason, there will surely be many iterations of the gold standard in the future. Without ever achieving a different final resolution.

The next generation of the money protocol: Breaking open Lindy

This limitation of the current money Lindy Cycle is exactly the problem that Bitcoin is trying to address. Due to the invention of the blockchain technology, it is now possible to effectively isolate monetary policy from any human interference while at the same time avoiding the centralization mechanisms inherent to gold. It allows us to create a non-sovereign money in the digital space, a truly groundbreaking achievement (to understand how Bitcoin accomplishes this, read Bitcoin: A Peer-to-Peer Electronic Cash System by Satoshi Nakomoto). This quality is so unique and mind boggling that there isn't anything yet that comes close. Furthermore, Bitcoin has an even scarcer supply then gold. It is what Saifedean Ammous likes to call *absolute scarcity*(for more information read The Bitcoin Standard: The Decentralized Alternative to Central Banking). For these reasons I believe that Bitcoin is the next generation technology for money, it has what it takes to break open the prevailing Lindy effect!

This rational also completely demolishes the "blockchain not Bitcoin" mantra as the Schelling point is purely based on bitcoin the money, not blockchain the technology. Blockchain is just a tool, a very sophisticated but narrow tool, specifically designed to allow Bitcoin to have monetary properties that were unthinkable before. A blockchain without similar monetary properties than Bitcoin is like a computer in the middle of the jungle without any access to electricity, a useless piece of junk.

Bitcoin the Schelling point, Bitcoin the Lindy effect holder

The transition towards the next generation money protocol has been going on for well over 9 years now and there are undoubtedly a lot more years of adaptation to come. But by this point it's becoming increasingly clear that Bitcoin is the undisputed Schelling point.

The main reason being that for all this time Bitcoin really hasn't gotten any decent competition. Very few altcoins seem to focus on an immutable monetary policy, and the ones that act as if they do (for example BCash, Litecoin) completely neglect the centralization problem that got us into this financial mess in the first place! So for whatever reason, 99.9% of all altcoins totally abandon BOTH preconditions to be able to compete with Bitcoin as a next generation technology of money. Off course competitors being so naive and horrendously awful at design and game theory doesn't go unpunished. Fact is that by this time Bitcoin has been able to build up such a considerable lead (Hash rate, developer community, decentralization, code quality, reputation of extreme security, liquidity, amount of users and nodes,

ossification of its core principles…) that is seems virtually impossible to break its Lindy effect. If the bowling ball isn't in the gutter already, it's so close that you would need a damn miracle to prevent it from locking in!

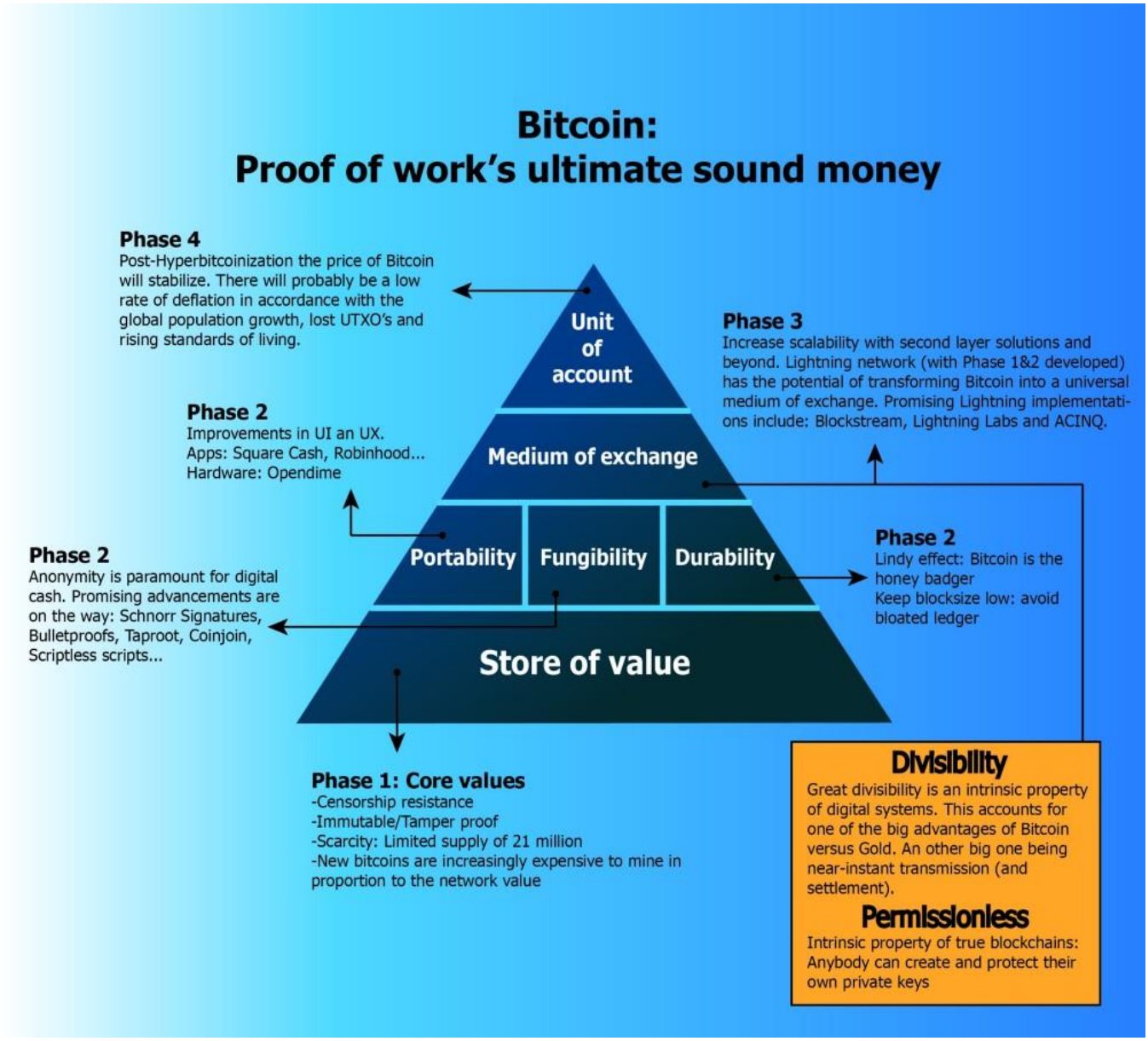
As discussed earlier in this article it is not necessarily the best protocol that wins. But the margins that competitors inevitably have to compete within, in order to qualify as a viable format, are extremely narrow. I believe that in order to take over the Schelling point of Bitcoin (as unlikely as it is at this point) there are some indisputable principles an altcoin has to adhere to.

1. Proof of work:

POW is the key to unlock the solution to the double-spending conundrum. It is a vital cornerstone to build a secure and trustless money protocol. **Despite what some altcoin hucksters might claim, it is the only consensus algorithm that actually works.** The best analogy comes from Tuur Demeester; alternative consensus algorithms are the modern day alchemy, they try to create something of value out of thin air. A delusion that will probably be propagated for many years to come. Furthermore, whether you like it or not, ASICs are an inevitability in this business. Nothing is ASIC resistant; the best you can hope for is ASIC tolerance that lasts a year or maybe two. If someone wants to compete with Bitcoin they better embrace ASICs, the alternative is constant danger of 51% attacks.

2. Heavy emphasis on store of value:

As Nick Szabo illustrates in Shelling out, proto-money emerges as a store of value and a medium of wealth transfer. These proto-moneys are selected on the basis of their unforgeable costliness. Bitcoin is strictly scarce, making it the hardest money in existence. For another blockchain to compete, the same strictness or more will have to be applied.



The Bitcoin utility stack, everything has to be built on top of the store of value bedrock

SoV can function as a basis and other utilities can then be built on top of this bedrock. It absolutely does not mean that medium of exchange is not a vital part of money. But the reality is that creating a medium of exchange is fairly simple, creating of store of value on the other hand is something never attempted before in the digital space and probably needs decades to mature and cultivate.

3. Heavy emphasis on decentralization:

This is by far the hardest concept and it can express itself in many different forms. Centralization is a constant threat. It can manifest itself in governance for example. The only way to limit this flaw is by keeping the governance strictly off-chain as Bitcoin does. On-chain governance will inevitably lead to the loss of sovereignty of

its users. The UASF of 2017 was a great example and the undisputed proof that off-chain governance is the only way to preserve decentralization of decision making, once and for all debunking the myth that miners have all the power. Another centralization threat is node deficiency, a danger that Bcashers cannot grasp for some reason. Fewer nodes greatly reduces the ability of users to exert influence on governance and selection of the valid chain. Centralization can also manifest itself in miner cartels, probably the biggest threat to Bitcoin right now but improvement might be on the horizon (Matt Corallo's BetterHash, Sony entering the ASIC market). Many other forms of centralization exist but they go beyond the scope of this article.

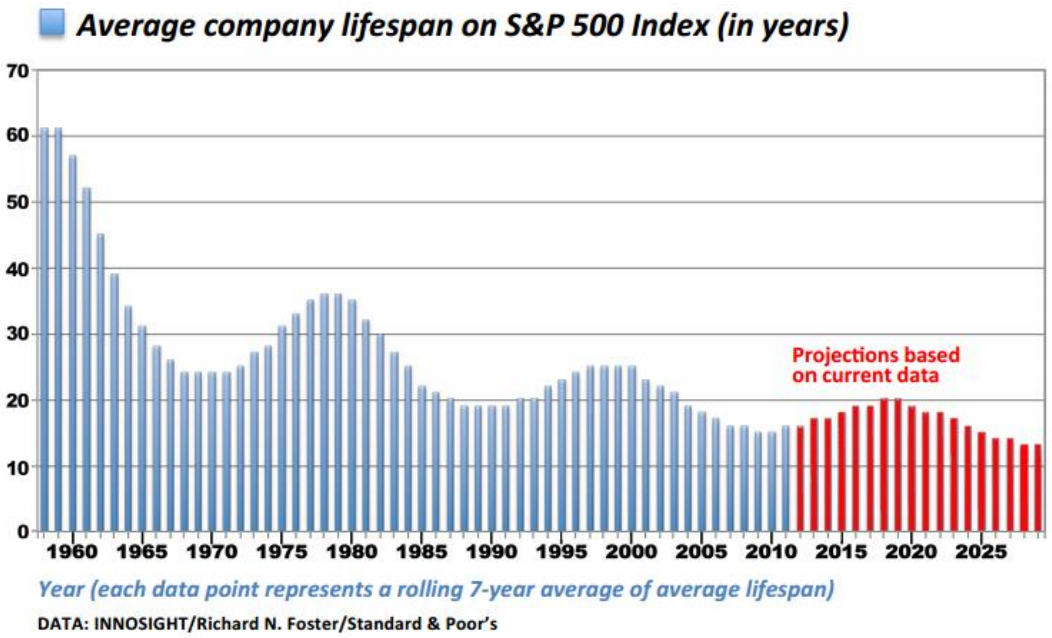
I could easily write another 20 minute long article just to discuss these 3 fundamentals of Bitcoin in more detail .But the bottom line is that from an objective perspective, **there is not one single altcoin that comes even close to the high standards of Bitcoin concerning these 3 principles.**This framework makes it abundantly clear that Ethereum cannot be compared to Bitcoin as it does not even compete it the same communication market. Ethereum doesn't want to be a money, it wants to be a decentralized application platform (and a very bad one at that).

Top down Schelling points, false lock-ins and open source

There is one last important topic we need to address in order to understand Bitcoin; the relevance of its open source nature. Through history many communication protocols emerged and vanished. And beside money itself, it is only in recent times that companies or third parties were able to monetize them. Before analogue and digital media, our societies only had access to a small number of communication markets, for example language itself. You could posit that the English language was and still is an open source project created by society at large. In our modern age we have grown used to companies being the patent holders of communication protocols (Facebook, YouTube, Blu-ray etc.). This is an unnatural state of affairs because communication networks spontaneously evolve towards monopoly, and putting a small group of people or a company in control of the whole market is the equivalent of central planning. There are two big problems with communication markets that are not open source:

Firstly, all companies grow and behave in a predictable manner (To learn more about this read "Scale: The Universal Laws of Growth" by Santa Fe Institute professor Geoffrey West, or watch his TED talk). Geoffrey West makes the point that growing bureaucracy and administration in big firms contribute to its unavoidable demise. Humans make the architecture of a corporation increasingly vulnerable over time. The vertical hierarchy that defines firms lends itself to all sorts of rent-seeking, abuse and miscommunication. The result is that companies all follow the same life trajectory. They grow up (hockey stick), they bend over (plateau), and then they all die. All companies have a limited life expectancy and Microsoft, YouTube or

Facebook are in no way an exception to this rule. An average S&P 500 company today has a life expectancy of just under 20 years. **This inherent instability poses a big problem because they limit the degree to which company protocols can enjoy the Lindy effect**. Open source does not have this vertical hierarchy problem, as it is a permissionless meritocracy. The administrative and managerial costs are stripped to the bone due to the horizontal and open approach. Anybody can work on any problem at any given time, and the most interesting improvements will be picked up and integrated into the source code.



As our economy deteriorates under Keynesian impulses, the average company lifespan decreases

Secondly, communication protocol companies do not wish to share the burden of maintaining and improving their product with the general public because that means they would have to share the profits. **You can sustain this creative input asymmetry for a reasonable amount of time but in the long run open source always wins out on closed source.**It is a mathematical certainty, proven over and over again, that the joint efforts of passionate volunteers out-compete the highly paid corporate methodology. In the nineties for example, intranets jumped out of the ground like mushrooms. Firms were not convinced of the internet as a whole and thought they would be better off using their own closed off intranet infrastructure. Over time it has become evident that intranets become stale rather quickly. Despite still being used today they are a fascinating illustration of how the quality of open source and closed source projects diverge over time. The evolution of a communication protocol is an organic process that can only be improved on by trial and error of society as a whole. Assuming that a small group of people in a

corporation can perfectly predict the needs of an entire market is naive, a communication protocol cannot function properly under central planning. A single company that controls a communication protocol is the exact antithesis of capitalism, it completely undermines the competition of ideas. Open source on the other hand thrives on the competition of ideas due to its uncompromising meritocratic nature. **Open source is the perfect solution to this communication monopoly conundrum as it transfers the free market of ideas from the inter-protocol domain to the intra-protocol domain.** In the long run I think it is inevitable that all forms of communication migrate to open source. The days of companies like Facebook, Amazon and google are numbered.

Thankfully Bitcoin is completely open source, probably the only one in the whole crypto space. **Altcoins simply cannot compete with Bitcoin because fundamentally they are companies, not protocols.**

Conclusion:

The Network effect, Lindy effect and Schelling point are facets of one overarching phenomenon i.e. the adoption of one monopoly communication protocol through free market competition over time. The communication monopoly effect if you will. With the emergence of Bitcoin it is becoming increasingly clear that the Lindy Cycle of the dollar is coming to an end. We must be thankful for the timing of this event because I believe it is still possible to transition to Bitcoin before the complete collapse of the current late stage gold standard iteration. Bitcoin is the pinnacle of what human endeavour and technological progress is capable of as it brings together a large variety of fields including cryptography, politics, distributed systems, economics, game theory etc. It took us thousands of years to come up with a worthy successor of gold as our money protocol and therefor I think it is reasonable to assume that the Lindy cycle of Bitcoin will rule for at least hundreds of years to come.

- *Many thanks to Dirk vandekerkhove for the comments and feedback*

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