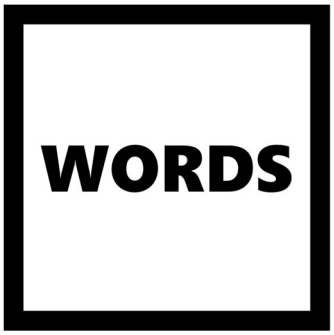
CRYPTO WORDS

CY19 July

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

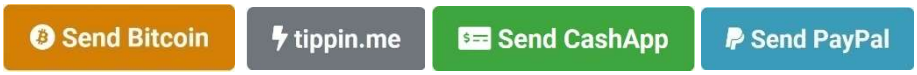
There exists a gap in Bitcoin publishing. For authors with commentary and scholarly papers on topic, the choice of publication outlets is relatively limited. The number of journals that serve as outlets for crypto research is in any event too small, as the number of crypto thinkers continues to grow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

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.



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:

Subscribe to our newsletter

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

Our pledge

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

Bitcoin's Department of Defense: The Case For A Global Reserve Currency With No Guns

By Anthony Pompliano

Posted July 1, 2019

The country with the strongest military has historically implemented their national monetary system as the global reserve currency. This started with the Silver Drachma of ancient Athens during the 5th century BC. Next up was Rome when they issued the Gold Aureus (from 1st century BC to 4th century AD) and then replaced it with the Silver Denarius coin in the year 312 AD.

As the Western Roman Empire fell and the Eastern Roman Empire (Byzantine Empire) survived/thrived, the Silver Denarius was replaced by "Byzantine coins" or a "Gold Solidus" which was an evolved variation of the Western Roman Empire's coinage. During the early 1000s AD, the Gold Solidus was gradually debased and eventually Emperor Alexios I Komnenos replaced it with the "hyperpyron," a refined gold coin that had ~ 20% less gold.

Toward the end of the 7th century, we saw the rise of the Islamic Dinar. It wasn't until the 13th century that the Florence Fiorino became globally dominant, which was followed in the 15th century by the Venice Ducato. Then in the 17th century, the Dutch Guilder took over as the world currency, before the 19th century ushered in the British Pound Sterling as the most important currency in the world. And the British Pound Sterling remained the global reserve currency until World War II.

It was at this time that the US dollar become the global reserve currency and it has defended that position since World War II. As I mentioned at the start of this letter, the global reserve currency was under the control of whoever was the global superpower at any given time.

This trend is about to change though.

Previously, the country with superior military firepower and tactics prevailed. It mattered who had the upper hand on land, sea, or air. But given where we are going, the bombs, bullets, tanks, ships, and fighter jets aren't going to be nearly as important as they once were. We are moving from physical warfare to cyber warfare.

We no longer need to send troops to combat if we can attack a country's critical infrastructure (ex: electrical grid, banking system, media publications, etc). War becomes even less necessary when we can weaponize the US dollar and cut off

entire countries from the international financial system (ex: Venezuela, Iran, North Korea, etc).

There is one problem with this military, economic, and cyber strategy though — what happens if we can't attack a country through military firepower, economic sanctions, or cyber warfare?

This may initially sound like a ridiculous question, but it isn't. Whether we like it or not, there is a group of people (the Internet) that has created a new currency (Bitcoin) that is slowly vying for global reserve currency status. And this group of people did something counterintuitive that is currently misunderstood.

The creators of Bitcoin focused on defense, rather than offense. Instead of conceiving a plan to gain superiority by attacking other countries or currencies, Bitcoin is designed in a way to survive any known attack. You could say this strategy falls in line with the belief that "the best offense is a great defense."

Lets look at the three main threats to a currency's global reserve status:

1. **Military superiority** — If you control the global reserve currency and your superpower status is revoked, you have historically lost global reserve status. No matter how hard nation states try, there are no individuals, companies, or physical locations to attack. No one person or group controls Bitcoin. If a nation state was to capture or kill an individual, nothing would change. If a nation state was to blow up all the mining facilities in their country, nothing would change. Simply, the decentralized nature of Bitcoin renders military superiority irrelevant.
2. **Economic sanctions** — The US has done a great job defending its global reserve status by weaponizing the US dollar. Unfortunately for the world's leading currency, there is no individual, company, or country to sanction in an effort to stop Bitcoin. No one is in control, therefore the economic sanctions are rendered irrelevant.
3. **Cyber warfare** — Over the last 10 years, Bitcoin has become the most secure computing network in the world. There are hundreds of billions of dollars in incentives for someone to successfully attack the system, but no one has succeeded yet. Additionally, the network continues to get stronger every day (up 10x in hash rate over the last 2.5 years), which widens the moat of security. Because of Bitcoin's decentralized nature, cyber warfare tactics are rendered irrelevant.

So what exactly does this mean?

Bitcoin is the first world currency that is (1) not backed by a nation-state and (2) has the ability to withstand any and all attacks by every nation-state in the world. Quite literally, the "defense first" approach to Bitcoin's design is likely to have led us to a

world where currency dominance shifts from military/economic/cyber superiority to anti-fragile superiority.

Bitcoin's Department of Defense has no bullets, no bombs, no ships, no fighter jets, and no soldiers. It has thousands of volunteers and millions of computers around the world that are cooperating to ensure there is no single point of failure.

The world is changing quickly. Nation-states are behind the curve. And Bitcoin is the sleeping giant that is well-positioned to be the first currency to achieve global reserve status without ever having to engage in conflict.

-Pomp

Bitcoin, The Dollar And Facebook's Cryptocurrency: Price Volatility Versus Systemic Volatility

By Caitlin Long

Posted July 1, 2019

Bitcoin has a systemic-stability mechanism built into it, but not a price-stability mechanism built into it.

Bitcoin's price swung wildly this week, causing many to conclude bitcoin is unstable. But this conclusion misses a key nuance: Bitcoin was designed for *systemic stability*, not for *price stability*. Indeed, as a system Bitcoin is highly stable even though its price may not be. Bitcoin is the opposite of fiat currencies, which generally exhibit price-stability but are susceptible to periodic bouts of financial system instability. By extension, stablecoins that track fiat currencies, such as Facebook's new cryptocurrency (Libra), fall into the same category as fiat currencies—they're designed for price stability, not systemic stability, and are exposed to the same risk of periodic instability of traditional financial systems. Can a monetary system be both price-stable and systemically-stable? Probably not, and here's why.

The real world isn't stable. Unpredictable events happen. Consequently, demand for money is inherently unstable too, influenced by factors such as earthquakes, droughts, hurricanes, technology break-throughs, the sudden discovery of large oil/mineral reserves, tax/tariff/regulatory changes, population trends and even simple seasonality. To cajole price stability within fiat currency systems, central bankers counteract these demand fluctuations by intervening in markets—in an attempt to steer the economy to perform within a target rate of price inflation, a currency peg or interest rates.

But remember—demand for money isn't stable. Central bankers manufacture the price stability of fiat currencies by interfering with natural market processes. Their actions can eventually lead to systemic instability. But hold that thought.

Bitcoin as a System: Designed for Systemic Stability, Not Price Stability

Bitcoin, by contrast, is a system that prioritizes security over price stability. Bitcoin's systemic stability stems from the security of its network. This week, as bitcoin's price volatility was capturing headlines, I was watching core bitcoiners get excited about something else entirely—the network's hash power hit an all-time high, and its "difficulty" also adjusted to an all-time high.

Translation: Bitcoin's network security hit at an all-time high.

Hash power is defined as the processing power of the Bitcoin network to perform calculations necessary to confirm transactions. The higher the hash power, the more secure Bitcoin becomes—i.e., the more immune it is to attack, simply because (by design) the cost to amass enough hash power to attack the network far exceeds the gain from doing so. Bitcoin is almost certainly the most secure computer system ever created, mostly due to the staggering size of its hash power. The Bitcoin network hit a high of 66.7 quintillion hashes per second (66.7 exahashes/second) on June 22—it's hard to convey just how powerful that is because it's not directly comparable to supercomputers, owing to the specialized nature of chips used in the Bitcoin network, but it's safe to conclude it still dwarfs the world's top 500 supercomputers, combined. The size of Bitcoin's hash power is one reason why it has survived every attack thrown at it to date, and its hash power continues to grow. What happens when additional hash power is added to the Bitcoin network? Answer: the network becomes more secure. That's it. Adding more resources does not—cannot—create more bitcoin. Why? Because (1) bitcoin's supply is fixed by algorithm and (2) the protocol's " **difficulty adjustment** " automatically kicks in when more hash power enters the network, to ensure that a new block is added to the blockchain every 10 minutes, on average.

"Difficulty adjustment is the most reliable technology for making hard money and limiting the stock-to-flow ratio from rising, and it makes Bitcoin fundamentally different from every other money(emphasis added)," wrote Saifedean Ammous wrote in his book,The Bitcoin Standard.

While investing more resources in gold mining causes more supply of gold to come online, that's not the case with Bitcoin. More computer resources simply create more security, not more supply.

So, Bitcoin has a virtuous cycle that fiat currencies don't have. As bitcoin's price goes up, more hash power joins the network. As more hash power joins the network, the

network's security hardens. Bitcoin becomes more immune to attack—more systemically stable. (Of course, the reverse is true as well—a vicious cycle could occur whereby Bitcoin becomes less secure as hash power exits the network. But even though the Bitcoin network lost hash power during the "crypto winter" of 2018-19, the loss of hash power negated only the prior four months of hash power growth and didn't remotely come close to rendering Bitcoin systemically insecure. When hash power leaves the network, the difficulty adjustment adjusts downward until the cycle turns virtuous again. It's a self-correcting system.)

To summarize, Bitcoin has a systemic-stability mechanism built into it, but not a price-stability mechanism built into it. Bitcoin's supply is fixed, so its price will fluctuate directly as demand for it fluctuates.

Fiat Currency Systems: Designed for Price Stability, Not Systemic Stability

Fiat currency systems, by contrast, are designed to have "stability mechanisms"—they're called central banks—which cajole short-term price stability by intervening in markets to keep a targeted metric within range. Why the quotation marks around "stability mechanisms"? Because by intervening in markets, central banks distort natural market signals (namely, interest rates) and thereby prevent accurate economic calculation by businesses—fomenting the next round of systemic instability when cash flows don't materialize to service the debt. Indeed, as central banks became more activist in the early 1980s, traditional financial markets have ping-ponged within a crisis/stability/crisis cycle.

Nassim Nicholas Taleb provides an apt analogy for this process in his book,Antifragile: forest fires. Artificial suppression of natural volatility (by suppressing small fires) creates false stability that can last short-term, but it builds long-term risk by letting an enormous amount of tinder build up. When the fires eventually come, they're more devastating.

By analogy, central banks have successfully suppressed market volatility in the short-term. Yet, clear signs of underlying systemic instability are again showing up—because central bank actions not only interfere with price signals in markets, thereby causing investors to misallocate capital unintentionally, but they also gut balance sheets. We can see signs of systemic instability brewing yet again in esoteric but critical corners of money markets, which is usually where the next round of systemic instability shows up first. Jeff Snider at Alhambra Investments chronicles on a daily basis the dozens and dozens of indicators showing that the financial system is well into its fourth systemic "disturbance" since the 2008 financial crisis (e.g., the LIBOR curve just inverted for the first time since February 2008, swap spreads just turned uniformly negative in key parts of the swap curve and repo fails are growing again, among the many, many other indicators also confirming another round of systemic

instability is underway). As Snider points out, this fourth episode is shaping up to be particularly nasty—maybe not as nasty as 2008, he says, but nastier than the prior three episodes. Time will tell. Despite all the warning signs, incredulously, on Thursday the Fed approved stock buyback plans submitted by 18 big banks, saying "The nation's largest banks have strong capital levels and virtually all are now meeting supervisory expectations for capital planning." I suspect the Fed's decision won't age well, but I digress...

The takeaway here is that systemic stability concerns have not been solved in traditional financial markets—and they won't be, owing to the inherent design of fiat currency systems that favor short-term price stability at the expense of periodic episodes of systemic instability.

Summary—And What This Means for Facebook Libra

Here's what it all means: traditional financial markets may be more price-stable than Bitcoin short-term, but will periodically face systemic crises. Bitcoin as a system is far more stable, even though its price may not be.

How does Facebook's Libra fit into this picture? Libra is a system designed to track a basket of fiat currencies—a "stablecoin," in the parlance. In other words, Libra is designed for price-stability but will inherit the same periodic instability faced by fiat currency systems—that is, assuming that the Libra Association keeps the basket allocated to fiat currencies. But Libra's basket is not set in stone. Over time, the Libra Association has the opportunity to invest the basket in bitcoin and other assets that are more systemically stable than fiat currencies. It will be fascinating to watch.

The real beauty of Bitcoin is that it offers each of us a choice to own financial assets outside of the traditional fiat-currency system, if we choose to. From a system design perspective, Bitcoin and fiat currencies are fundamentally different. One way to ponder that choice is to ask yourself how much you value price stability, and whether the systemic stability of Bitcoin is valuable to you as an insurance policy. Only in retrospect will it become clear how valuable that choice turns out to be.

Tweetstorm:SIDECHAINS ARE NOT LAYER 2

By Georgios Konstantopoulos

Posted July 4, 2019

Let's put a myth to bed.

Thread on the history of sidechains, their security properites, concluded by their differences to Layer 2 solutions.

(there's a lot of resources, feel free to skip/bookmark for later!)

👇

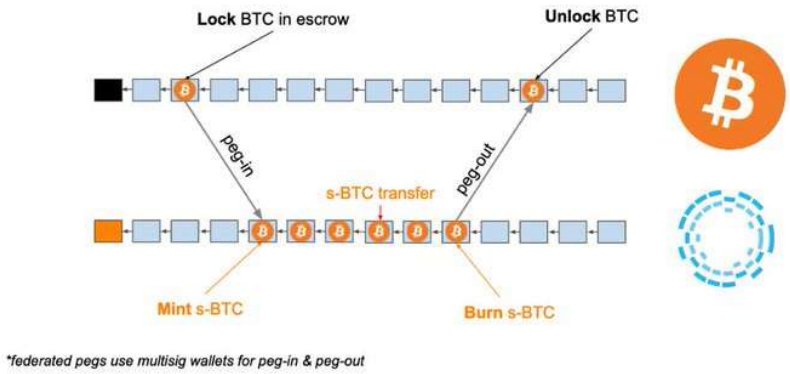
– History of Sidechains –

"Sidechains" is a term coined in [1] by @Blockstream, as a way to access innovative blockchain features which are too risky to try on Bitcoin.

This is done by enabling the transfer of BTC between chains w/ varying feature sets

[1] blockstream.com/sidechains.pdf They introduced the "two-way-peg" (2WP) for PoW blockchains.

To transfer assets from the "sending chain" (SC) to the "receiving chain" (RC), you lock them on the SC, and mint an equivalent amount on RC by providing a proof of ownership on SC along with a DMMS* with enough work.



- DMMS: Dynamic Membership Multi-party Signature. In the PoW case, that's an SPV proof. Screenshots from [1].

We observe that Bitcoin's blockheaders can be regarded as an example of a *dynamic-membership multi-party signature* (or *DMMS*), which we consider to be of independent interest as a new type of group signature. Bitcoin provides the first embodiment of such a signature, although this has not appeared in the literature until now. A DMMS is a digital signature formed by a set of signers which has no fixed size. Bitcoin's blockheaders are DMMSes because their proof-of-work has the property that anyone can contribute with no enrolment process. Further, contribution is weighted by computational power rather than one threshold signature contribution per party, which allows anonymous membership without risk of a *Sybil attack* (when one party joins many times and has disproportionate input into the signature). For this reason, the DMMS has also been described as a solution to the Byzantine Generals Problem[AJK05].

Because the blocks are chained together, Bitcoin's DMMS is cumulative: any chain (or chain fragment) of blockheaders is also a DMMS on its first block, with computational strength equal to the sum of the strengths of the DMMSes it is composed of. Nakamoto's key innovation is the aforementioned use of a DMMS as a signature of *computational power* rather than a signature of *knowledge*. Because signers prove computational work, rather than proving secret knowledge as is typical for digital signatures, we refer to them as *miners*. To achieve stable consensus on the blockchain history, economic incentives are provided where miners are rewarded with fees and subsidies in the form of coins that are valuable only if the miners form a shared valid history, incentivising them to behave honestly. Because the strength of Bitcoin's cumulative DMMS is directly proportional to the total computational power contributed by all miners[Poe14a], it becomes

Note that the 2WP between PoW chains requires each chain be able to verify the other chain's Proof of Work algo.

Blockstream's Liquid uses a multisig federation and doesn't need SPV proofs for peg-in/out (more on that later on PoS sidechains).

– PoW Sidechains –

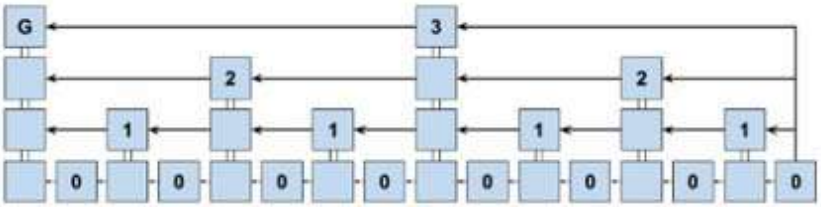
A few years later @sol3gga, @socrates1024 and @dionyziz came up with NiPoPoWs [2], a succinct SPV proof technique where the main insight is that some blocks have a better mining target than others.

[2] nipopows.com

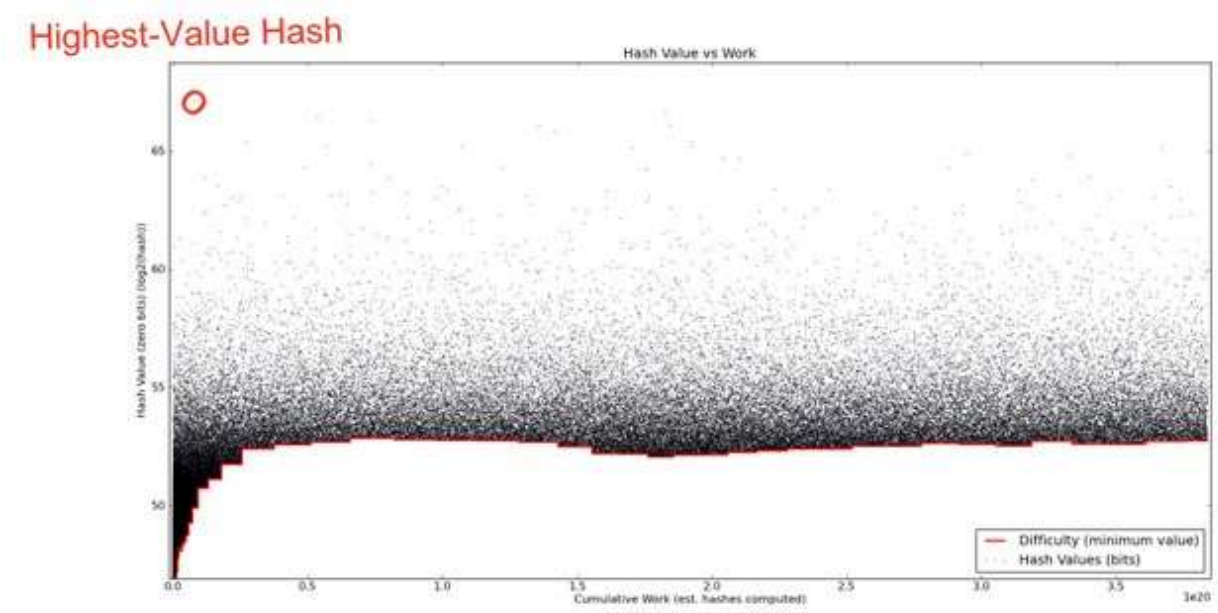
HOW DO THEY WORK?

Proofs of Proof-of-Work are based on the simple observation that some blocks achieve a better mining target than others. For example, the current difficulty may require that a block hash needs to start with 10 zeroes, but it so happens that some block hashes start with 15. These **superblocks** are rare and happen randomly. The idea with NIPoPoWs is that the whole list of block headers doesn't need to be presented to the network, as these blocks capture cumulative difficulty on average. If a blockchain portion has 128 blocks, then on average half of them (64) will have an extra zero in the binary representation of their hashes, a quarter (32) will have two zeroes, and so on. A blockchain can therefore be "compressed" by only sending these blocks on the network.

The average distribution of blocks is illustrated in the following figure. The bottom part shows the regular blockchain. Higher levels show blocks with 1, 2, or 3 extra zeroes in their hashes. Taking only these blocks, one can form a **superchain**.



(obviously, @socrates1024 talked about this in bitcoin talk in 2012 bitcointalk.org/index.php?topi...)

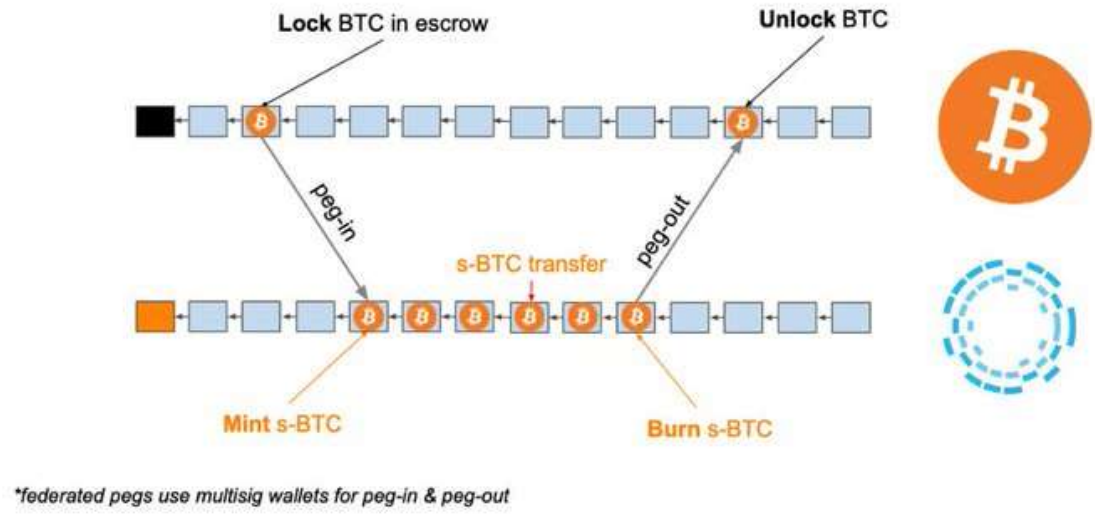


This works only for constant difficulty PoW, so is still not practical, and is vulnerable to block withholding/bribing! @gtklocker implemented a NiPoPoWs velvet fork and interlinker for Bitcoin Cash which he writes about in his thesis [3].

[3] arctan.gtklocker.com/thesis.pdf FlyClient [4] by @benediktbuenz utilizes @peterktodd 's MMRs* [5] to succinctly commit to the chain history. Combined with probabilistic sampling** has better performance than NiPoPoWs and works for varying PoW difficulty.

[4] eprint.iacr.org/2019/226 [5]**proofchains/python-proofmarshal** Contribute to proofchains/python-proofmarshal development by creating an account on GitHub. https://github.com/proofchains/python-proofmarshal/blob/master/proofmarshal/mmr.py

We recently wrote a ZIP with @*prestwich* and @therealyingtong to add MMRs in ZCash's blockheaders. Full FlyClient ZIP soon?



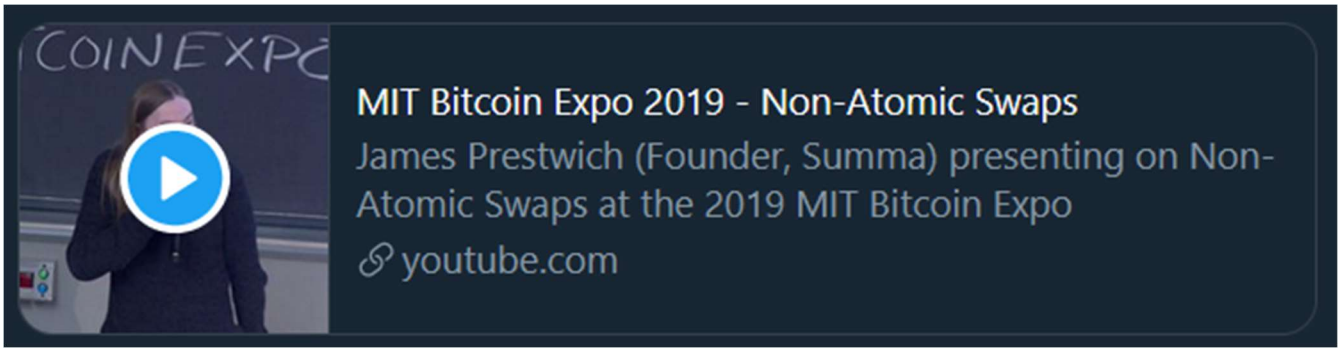
Link to tweet

**the light client repeatedly asks a full node about random parts of the chain history until they're convinced that the chain being shown to them is correct. This is made non interactive via the Fiat Shamir Heuristic

Short discussion on FlyClient vs NiPoPoWs:

@summa_one's stateless SPV proofs [6] can also be used for pegs, but are 'cryptoeconomic': the more work inside the provided headers the more confident you can be about the transaction being part of the heaviest chain

[6]

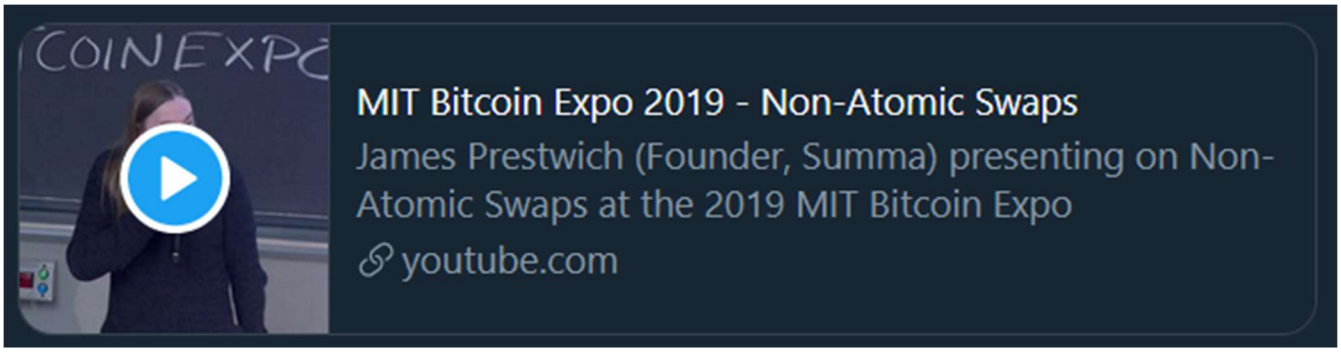


link

All PoW sidechain schemes assume that each chain is independently secure. That is a BIG assumption, as argued by Peter against Dionysis: .

Constructing PoW sidechains is also described in [7].

[7] eprint.iacr.org/2018/1048.pdf



link

TAKEAWAY:

The moment your bitcoins move to an output that is spendable based on an event that happens on a chain with less hashrate than the bitcoin chain, you're exposing yourself to counterparty risk (the miners of the other chain, or the validators if PoS) I like to think of crosschain assets as alloys.

BTC on the bitcoin chain is BTC-100. It is pure, inefficient, boring; but it is the most sovereign asset that has ever existed.

BTC-X would explore a different tradeoff space, as envisioned by the original @blockstream paper

Enabling Blockchain Innovations with Pegged Sidechains

Adam Back, Matt Corallo, Luke Dashjr,
Mark Friedenbach, Gregory Maxwell,
Andrew Miller, Andrew Poelstra,
Jorge Timón, and Pieter Wuille*†

2014-10-22 (commit 5620e43)

Based on that thought, @ethereum 's or @binance 's WBTC would be BTC-X, where X is (cost of corrupting the federation) / (cost of attacking bitcoin). It's easy to see how the fraction's value could become 0 on regulatory pressure.

Bitcoin Alloy	Use Cases	Security Assumption
BTC-100 (native chain)	Store of Value	Honest Majority of miners
BTC-30 (other PoW chain)	Daily Transacting	Honest Majority of miners (less than BTC-100)
BTC-X (WBTC?)	DeFi	Honest Federation (subject to KYC, regulation etc.)

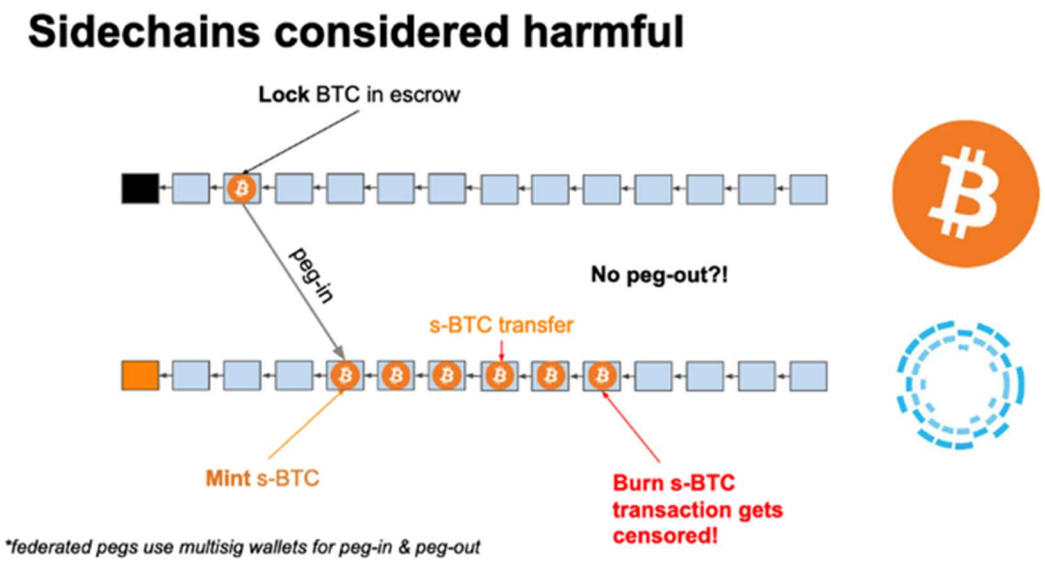
Aluminum alloy	K [MPa]	n	Ultimate stress, σ_u [MPa]
AA6082 T6	588.7	0.205	290
AA2024 T4[a]	806	0.200	476
AA6111[b]	504	0.270	272

*Source: [a]Dowling [18]; [b]Han and Kim [6].

(iii) the yield stress varied from 217.4 MPa to 261.4 MPa, consistent with the real value of 250 MPa; also, these values agree with the results obtained by Hopperstad et al. [1];

What if the receiving chain's consensus halts (i.e., no blocks are produced)? What if the miners refuse to include your locking transaction?

WORST CASE SCENARIO: YOU LOSE ALL YOUR MONEY



What is the point of gambling your BTC with WBTC in the #DeFi casino if you cannot cash out? It's as if as the casino shut down with all your money inside. Remember Mt. Gox?

– PoS sidechains –

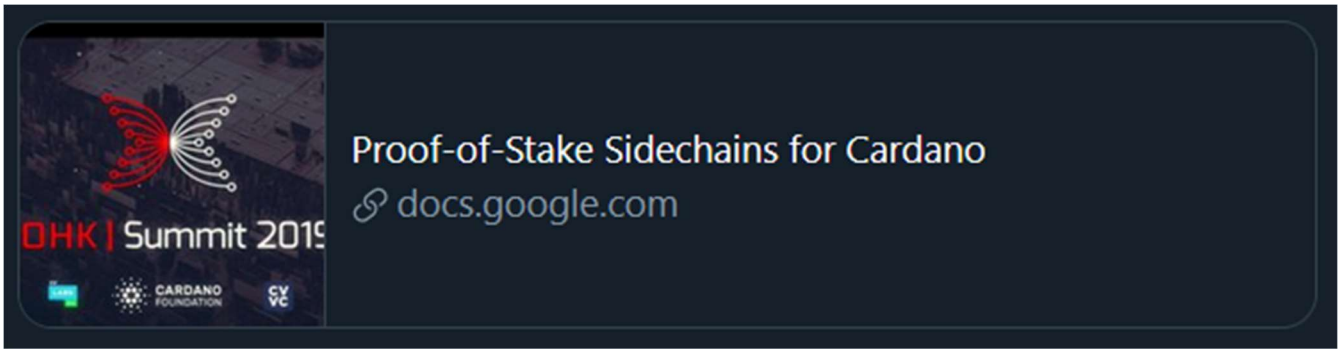
In [8], Andrew Poelstra formalizes DMMS security, and argues that a properly implemented PoS with long/short-range attacks protection can be DMMS-like, but has different security from Bitcoin's DMMS.

Maybe that's BTC-99.99?

[8] download.wpsoftware.net/bitcoin/pos.pdf (my favorite PoS paper) Since there's no notion of "work", can we construct a secure DMMS that can convince us that an asset was locked on another chain?

Dionysis' work [9], [10] covers this area extensively

[9] eprint.iacr.org/2018/1239.pdf [10] **Proof-of-Stake Sidechains for Cardano** https://docs.google.com/presentation/d/17x25AfvnMOpmXFO7wqs5q0AtW4yrYJeVPS2Lb22thyo/edit?usp=sharing



link

– Crosschain communication in practice (follow IBC for standardization) –

Deposit from sending PoW chain to receiving PoS chain:

1. Send asset to special output on sending chain
2. Validator listens for deposit *with a light client* and signs it
3. If 2/3rds of validators weighted by stake signed, the asset gets minted on the receiving chain

Withdraw from sending PoS chain to receiving PoW chain:

1. Burn on sending chain
2. Make withdrawal request to validators with proof of burn
3. Validators signs on the withdrawal request
4. Output on receiving chain gets unlocked if signatures with 2/3rds of stake are shown

I hope that I have convinced you that there is counterparty risk in moving assets from a PoW chain to a sidechain with less hashrate, or a PoS chain.

There may be feature tradeoffs which justify that move, but the extra risk must be part of your security model.

Sidechains:

- **interoperability** solution
- **NOT** a **scalability** solution
- **independent** security model
- consist of their own **L1 that talks with other L1s**

What makes Layer 2 special?

L2 security == L1 security

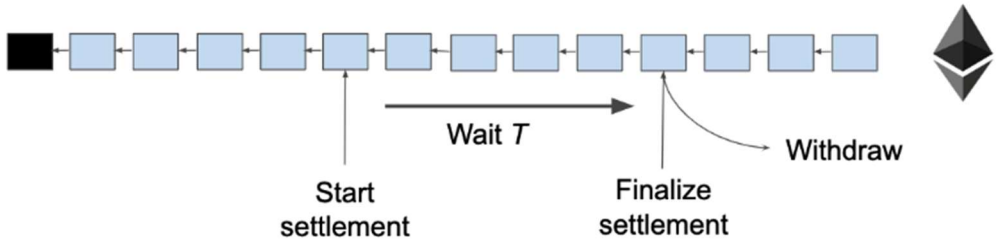
A L1 smart contract acts as an escrow. Unlocking the assets relies on:

1. Playing a fixed duration game where honest players are guaranteed to win, OR
2. Cryptographically proving ownership with a ZKP.

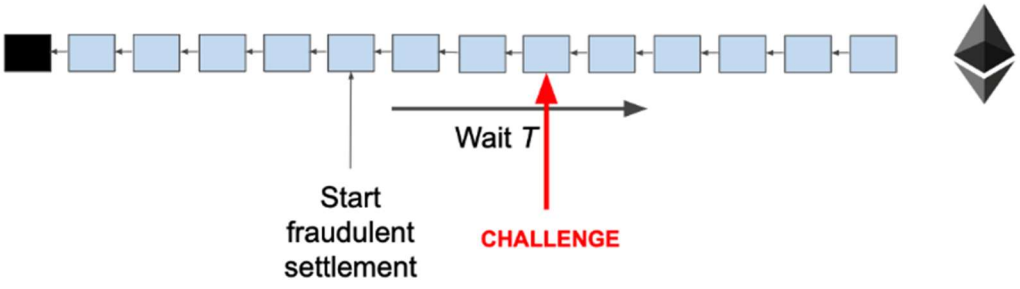
In detail: Fraud proofs:

Client side validation with an L1 smart contract as adjudicator. Withdrawal requests take time T, after which you can unlock the claimed asset. If another user comes online and submits a fraud proof, the request is cancelled. (add slashing for incentives). Assumptions: user comes online, L1 is not congested

Example: Lightning Network, Plasma, State Channels



Unlock assets by **proving ownership** on a **smart contract on L1**

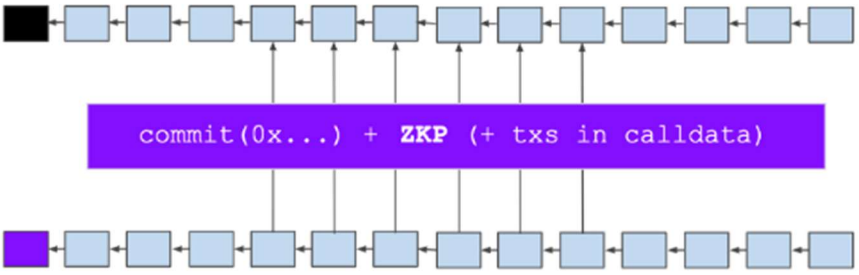


Challenged settlement requests get cancelled.

Validity Proofs:

- L1 smart contract stores hash of state.
- Aggregator gathers state updates, generates & submits ZKP.
- Update contract hash If proof is valid.
- Supports instant withdrawals
- Has no liveness assumption Assumptions: fancy crypto doesn't break, data availability (sort of)

Examples: ZkRollup, StarkDEX, Loopring



Fraud is prevented by the validity proof.
Validity Proof caveat: expensive, slow, maybe trusted setup

The above was a quick summary of L2 techniques. The biggest issue with L2 that's not state channels is the data availability problem, but that's a separate discussion.

More about Fraud vs Validity Proofs in @StarkWareLtd 's blog post:

Validity Proofs vs. Fraud Proofs - StarkWare - Medium Validity Proofs and Fraud proofs are both used in different L2 scalability solutions. In this post we analyze and compare them. https://medium.com/starkware/validity-proofs-vs-fraud-proofs-4ef8b4d3d87a

This was my longest thread! I hope I got my point across, and maybe you, dear reader, are now less confused.

I am considering doing "Drivechains & Statechains are not Layer 2" & "Plasma & Rollup is Layer 2" threads, let me know on your thoughts.

{fin}

Tweetstorm: The Founders and Cryptocurrency

By Jake Chervinsky

Posted July 4, 2019

0/ Happy Fourth of July!

Have you ever wondered what the founders of the United States would say about cryptocurrency? Given their views on paper money, I get the sense they'd be hodling bitcoin.

Warning: 🔥 takes from the Early Republic below.

1/ First, a brief history lesson.

Before the American Revolution, the colonies used many different forms of money, including European specie (money in the form of metal coins), personal lines of credit, IOUs, and paper bills issued by banks and governments.

2/ During the war, Congress (both Continental and Confederation) and the states didn't have enough specie to cover their rising costs.

To address the shortfall, they printed paper money backed by loans from individuals, banks, and foreign nations.

3/ But, they printed way more paper bills than the value of those loans and far outspent their actual worth. This resulted in rapid inflation and caused government debt to skyrocket.

Thus, the saying: "not worth a Continental."

After the war, the US had to repay its debts.

4/ Problem was, Congress couldn't force the states to contribute to the national debt, and citizens didn't have enough cold, hard specie to pay taxes.

So, Congress and many states started experimenting even more with paper money.

Here's what a few of the founders had to say:

5/ Alexander Hamilton, June 1783:

"To emit an unfunded paper as the sign of value ought not to continue a formal part in the Constitution, nor ever here after to be employed;..."

6/ "...being in its nature pregnant with abuses and liable to be made the engine of imposition and fraud; holding out temptations equally pernicious to the integrity of government and to the morals of the people."

7/ George Washington, 1785:

"I never have heard, and I hope I never shall hear, any serious mention of a paper emission in this state. Yet ignorance is the tool of design and is often set to work suddenly and unexpectedly."

8/ George Mason, 1785:

"[T]hey may pass a law to issue paper money, but twenty laws will not make the people receive it. Paper money is founded upon fraud and knavery."

9/ James Madison, 1786:

"Paper money is unjust; to creditors, if a legal tender; to debtors, if not legal tender, by increasing the difficulty of getting specie. It is unconstitutional, for it affects the rights of property, as much as taking away equal value in land...."

10/ "...It is pernicious, destroying confidence between individuals; discouraging commerce;...reversing the end of government, and conspiring with the examples of other states to disgrace republican government in the eyes of mankind."

11/ George Washington, January 9, 1787:

"Paper money has had the effect in your state that it will ever have, to ruin commerce, oppress the honest, and open the door to every species of fraud and injustice."

12/ Oliver Ellsworth, August 16, 1787:

"This is a favorable moment to shut and bar the door against paper money. The mischiefs of the various experiments...are now fresh in the public mind, and have excited the disgust of all the respectable part of America."

13/ George Washington, February 16, 1787:

"[I]f I had a voice in your Legislature, it would have been given decidedly against a paper emission.... I contend that it is by the substance, not with the shadow of a thing, we are to be benefited...."

14/ "...The wisdom of man, in my humble opinion, cannot at this time devise a plan by which the credit of paper money would be long supported; consequently depreciation keeps pace with the quantum of the emission; and articles for which it is exchanged..."

15/ "...rise in a greater ratio than the sinking value of the money.

"I shall therefore only observe...that so many people have suffered by former emissions, that, like a burnt child who dreads the fire, no person will touch it who can possibly avoid it."

16/ Charles Pinckney, May 1788:

"[T]hese general reasons will be found true with respect to paper money; that experience has shown that in every state where it has been practiced since the Revolution, it always carries the gold and silver out of the country and impoverishes it."

17/ Thomas Jefferson, November 6, 1813:

"[T]he trifling economy of paper as a cheaper medium, or its convenience for transmission weigh nothing in opposition to the advantages of the precious metals; that it is liable to be abused..."

18/ "...has been, is, and forever will be abused in every country in which it is permitted. [W]e are already at 10 or 20 times the due quantity of medium, insomuch that no man knows what his property is now worth, because it is bloating while he is calculating[.]"

19/ Before anyone drags me into politics twitter (please no), it's worth pointing out that the founders had diverse views on many issues. They'd probably end up arguing as passionately as we do today.

Still, as they intended, it often feels as if they're talking to us directly:

20/ Thomas Jefferson, May 28, 1816:

"I sincerely believe, with you, that banking establishments are more dangerous than standing armies; and that the principle of spending money to be paid by posterity, under the name of funding, is but swindling futurity on a large scale."

21/ We're still working on a problem that Jefferson identified 200 years ago. Maybe, just maybe, we finally have the technology to solve it.

I'd like to think Jefferson, an inventor, would approve.

So let's all enjoy the holiday, and then let's get back to work!

PS/ Thanks to @lmchervinsky, my brilliant wife and PhD-holding historian of the American Revolution and Early Republic, for helping me understand 18th century fiscal policy.

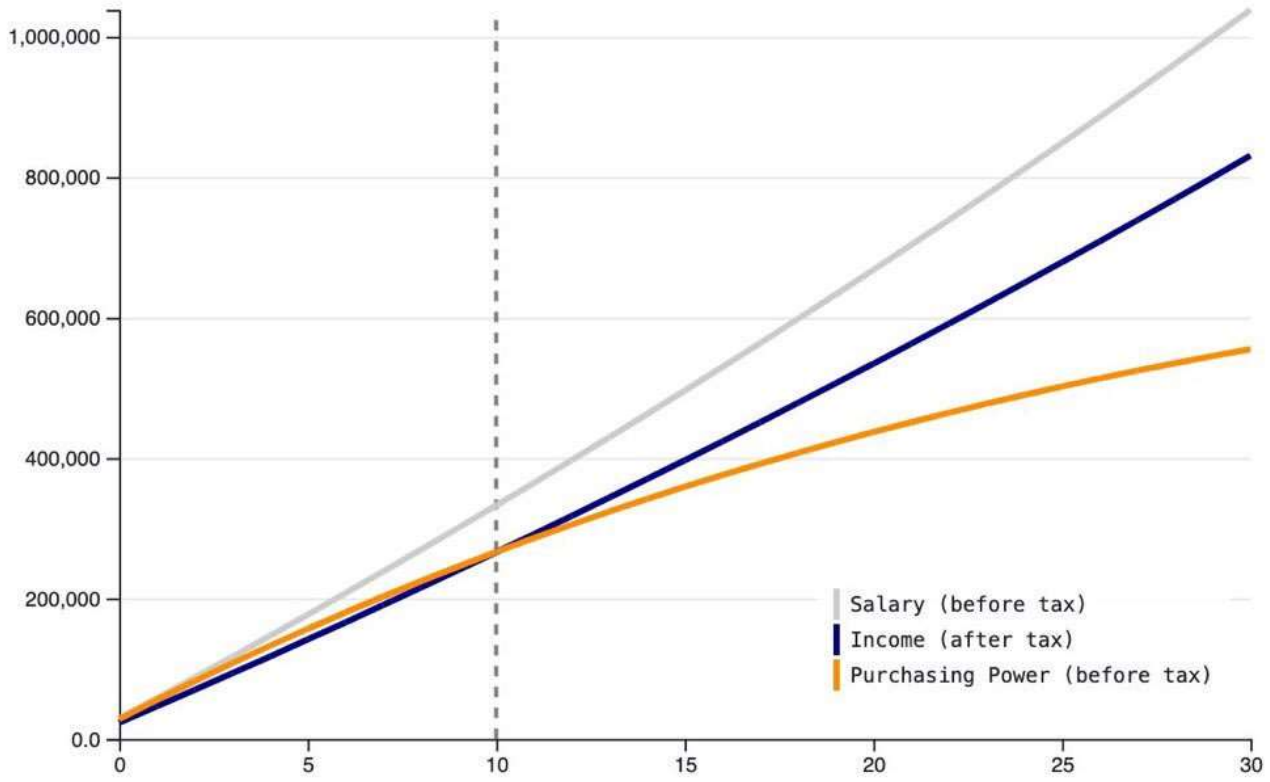
She says historians will accuse me of taking these quotes out of context, but I think I can handle it. 🚀

Tweetstorm: Inflation is Cruel

By Ben Prentice

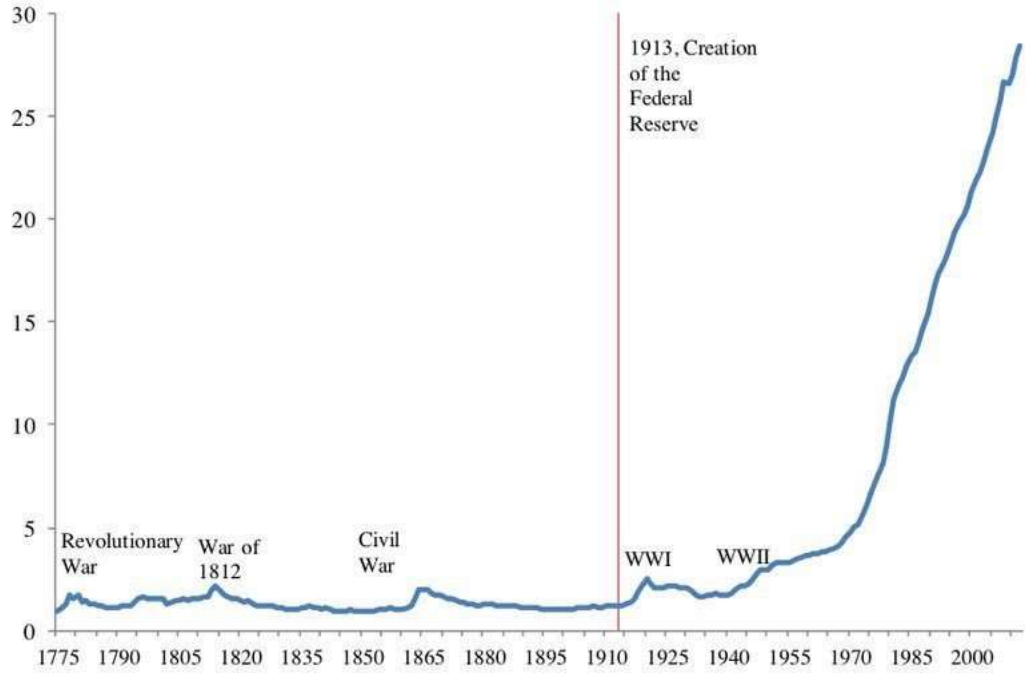
Posted July 6, 2019

Inflation is a cruel clandestine method of stealing wealth, unlike tax which is at least knowable, inflation destroys savings, wages, and economic calculations.



Zoom out to see what establishing the federal reserve has done to the price system, the integral component of economic coordination. When prices are distorted, our coordination with each other, our time-preference in saving/spending, and our very culture is being corrupted.

Figure 1. Consumer Price Index, United States, 1775-2012
(level, 1775=1)



Sources: Bureau of Labor Statistics, Historical Statistics of the United States, and Reinhart and Rogoff (2009).

To understand the miracle of the price system, one must simply ask: "who knows how to make a pencil?"

When prices are distorted, prices that we understand are set in aggregate by the market, the signals used by savers, spenders, and producers are manipulated, and the miracle is destroyed.

The temptation to print money is not to be underestimated. In the past, rulers were caught red-handed debasing their currencies, and at great cost of minting new coins.

The tyranny of the status quo is that we've all been convinced 2% inflation is necessary for growth.

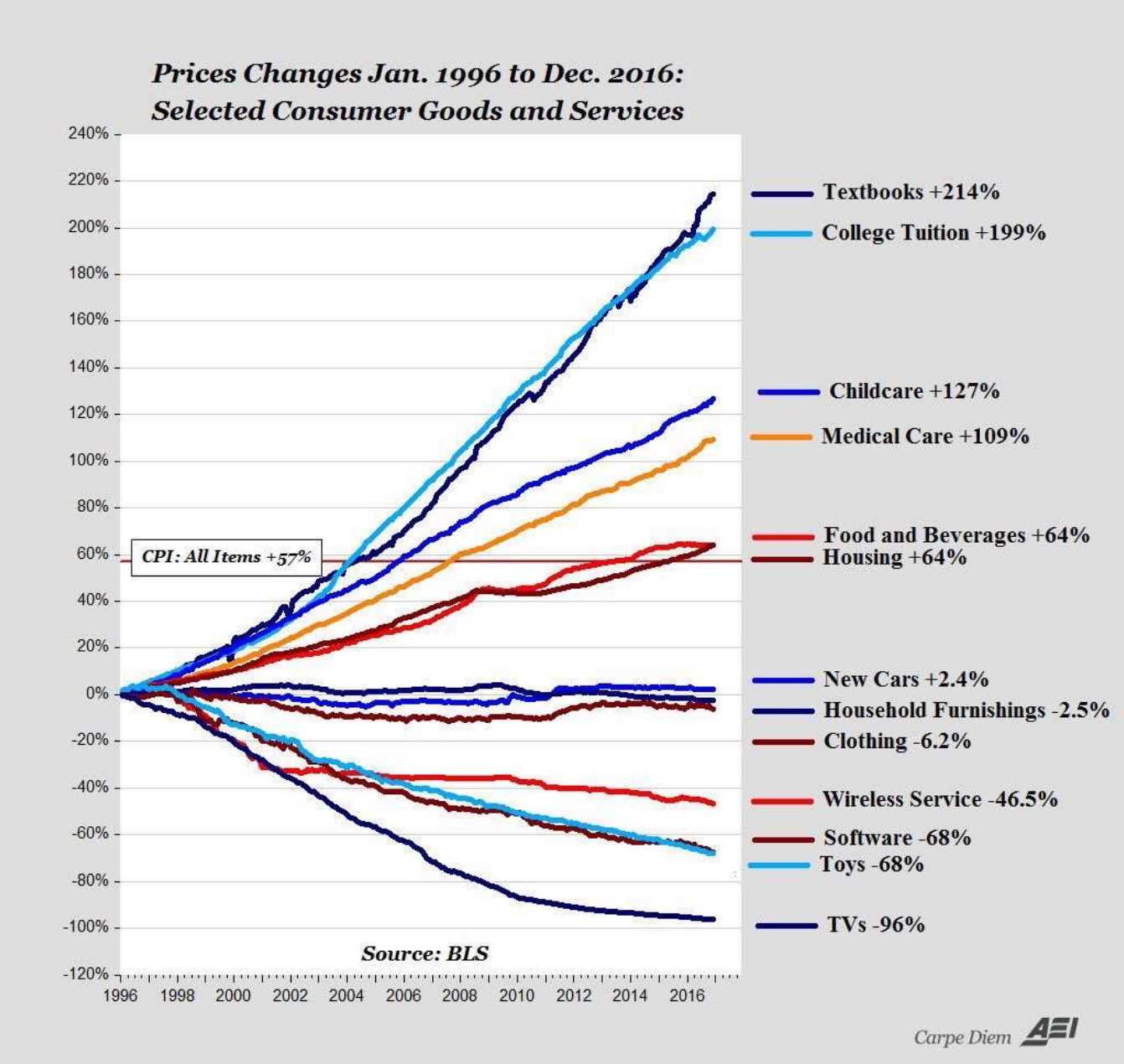
i.e. "Debasing our currency is necessary for progress. If we don't devalue your money, you might actually save some!"

No surprise, savings are at all time lows.

This lie, taught to us by the Keynesians, fed to us by the govt-funded schools, perpetuated by the Fed-endorsed banking system where money is created to enrich

the banking class, and risks and losses are laid on the populace, maybe the the greatest lie ever told.

The only economic progress we have seen in the past century is due to deflation. Electronics and technology, the exponential revolution, is progressing so rapidly, only prices tied to this phenomenon are falling, in spite of inflation.



So before you point to all the “progress” we have seen in increasing standards of living, ask if it is due to inflation manipulating people into investing in stocks, or due to falling prices of technology.

What could possibly dismantle this global tyranny of lies distorting economic progress to protect big govt and enrich the rich? Could we “end the Fed” with legislation? Protest? Discourse? I have doubts.

What if we could create a new system of money, outside the control of govt, backed by raw energy and mathematics, secured by hundreds of thousands of rule-enforcers, promulgated by a social contract to preserve liberty and protect wealth?

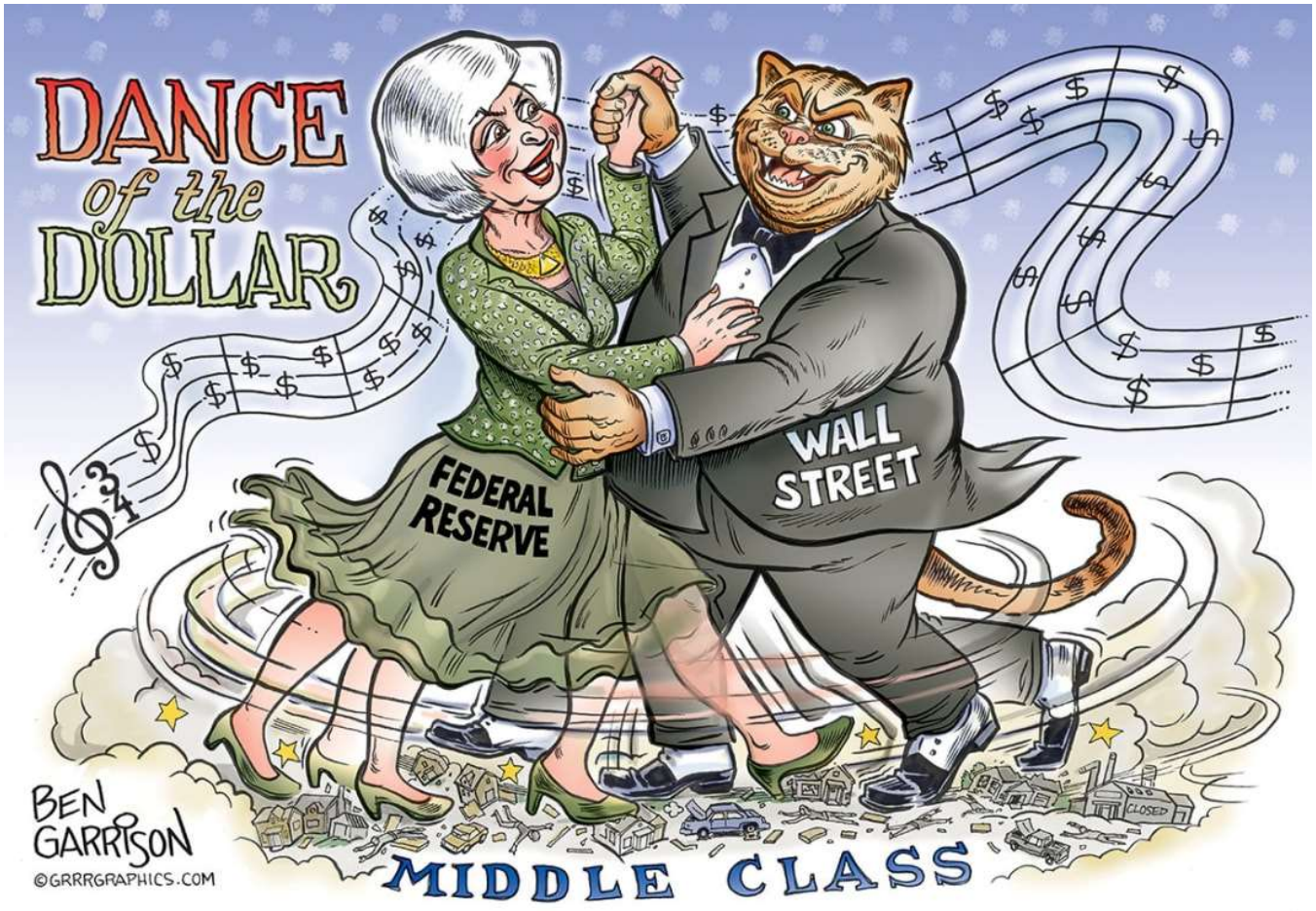
What if the incentives were so aligned that everyone was incentivized to secure the system, to profit from its adoption, to slowly and voluntarily exit the hegemony of govt money? What if #Bitcoin is a global peaceful #revolution that secures wealth and protects individuals?

Bitcoin Is Smarter Than Politicians And Central Bankers

By Antony Pompliano

Posted July 8, 2019

Don't look now, but the global economy is becoming unstable and uncertain. Each individual, regardless of geographic location, is increasingly being asked to trust the expertise and experience of politicians, economists, central bankers, and the leaders of legacy financial institutions.



While this would historically seem like a reasonable ask, these "experts" have proven time and again that they are ill-equipped to handle the complexities of many situations that we face today. The confluence of events playing out at the moment are incredibly bullish for Bitcoin, but before I explain why, here is an overview of the current headwinds facing currencies and economies:

- **Trade wars** — The two largest economies in the world, the United States and China, are locked in a trade war that continues to escalate aggressively. The US has hit China with a 25% tariff on approximately $250 billion of Chinese products, while China has ratcheted up their response with increasing tariffs on billions of dollars of American products. This is all happening while the US barely avoided a trade war with Mexico and is currently threatening the EU with new tariffs that would hit $4+ billion of EU products. If the ramifications of these trade wars weren't so serious, we would all be laughing at the fact that a material amount of this nonsense is playing out on Twitter (see here,here, and here for examples).
- **Recessions are upon us** — The US Treasury yield curve officially closed the second quarter of 2019 inverted. This means that for an entire quarter, investors were given higher returns on short term bonds, rather than long term bonds. As many have explained, this has been the leading indicator of an impending recession over the last 50 years (has happened 7 times) and there has not been a false positive over that time period. The US isn't the only economy in trouble though, especially when you consider Raoul Pal's recent argument that the EU is already in a mild recession.
- **European banks are failing** — Deutsche Bank is dominating headlines for their ineptitude over the last decade, which has culminated in a recent announcement of ~ 20,000 job cuts and a complete restructuring of the bank. They aren't the only banks struggling though. Others like UBS,Credit Suisse,Société Générale,BBVA, and Barclays appear to be facing major issues that could quickly turn into a domino effect that ends in a widespread financial crisis.
- **Loss of Federal Reserve Independence** — According to the Federal Reserve website, " *the Federal Reserve, like many other central banks, is an independent government agency but also one that is ultimately accountable to the public and the Congress. The Congress established maximum employment and stable prices as the key macroeconomic objectives for the Federal Reserve in its conduct of monetary policy. The Congress also structured the Federal Reserve to ensure that its monetary policy decisions focus on achieving these long-run goals and do not become subject to political pressures that could lead to undesirable outcomes.*" This independence is being tested as President Trump continues to publicly apply pressure to the Federal Reserve on currency manipulation, while openly critiquing the organization's decision making.
- **Low Interest Rate Environment** — In the last two economic recessions, central banks were able to cut interest rates an average of 5.0% or more in an attempt to combat headwinds. Given the current 2-2.5% interest rates in the US, and negative interest rates in Japan and Europe, these institutions won't have the same severity of aggression available to them this time around.
- **High Levels of Debt** — We are currently experiencing record levels of debt around the world, including US corporate debt as a percent of GDP over 70%

and China holding strong around 150%. The last time this US metric was so high was during the Global Financial Crisis and China hasn't ever seen levels this high before. To put this all in context, there is 3X+ more debt than GDP in the world today.

- **Slowing Global Growth** — The World Bank continues to slash global growth forecasts. They cut " *2019 global growth forecast to 2.6% from 2.9% and cut its forecast for growth in trade to 2.6% from 3.6%. The World Bank had already forecast the US to slow to 2.5% in 2019 from 2.9% in 2018 and for China to slow to 6.2% from 6.6%.*" Additionally, when World Bank President David Malpass was asked for the reasoning behind these cuts, he cited falling business confidence, the slowest pace of global trade growth since 2008 and sluggish growth in emerging and developing economies.

The outlook for the global economy is currently bleak, with numerous signals indicating an impending recession. Whether we like it or not, markets can't go up and to the right forever.

Unfortunately, investors don't have very many options in this scenario. They are being asked to trust the expertise and experience of politicians, economists, central bankers, and the leaders of legacy financial institutions. Not exactly something that many people are comfortable doing.

The global uncertainty, and increasing likelihood for instability, is leading investors to look for alternative options. This brings me to the argument of why Bitcoin is poised to greatly benefit from the perfect storm of events that are unfolding.

Bitcoin is a decentralized, digital asset that is built in a way that prevents any individual or organization from manipulating key components of the asset (monetary policy, security, transaction history, etc). In effect, Bitcoin as a system can not be manipulated by any government, central bank, financial institution, or politician.

And to make things even more compelling, the monetary policy decisions have already been decided for the next ~ 120 years, along with a feature where anyone in the world can publicly audit the execution of this monetary policy plan as it plays out. Think about that for a second….there is more uncertainty in the global financial system, than in the structure, operation, and governance of Bitcoin.

As we know, investors find comfort in decreased uncertainty. This is exactly why we are seeing Bitcoin become more and more attractive as global instability and uncertainty increases. Don't believe me? Here are some interesting facts:

- During the month of May, the US was actively ratcheting up the trade war with China, along with threatening Mexico, Europe, Iran, etc with trade wars as well.

Many of the issues outlined in the bullet points above were also increasing in severity during that time.

- Bitcoin's price appreciated 55% during May, but more interestingly, the asset had a negative correlation to the S&P 500 (-0.9%) and gold (-0.8%). That means that as stocks and gold became less attractive, Bitcoin was becoming more attractive.

Obviously, one month of data is not enough to make a compelling argument with, but it is worth watching this trend as we move forward. There is a good chance that we are on the cusp of a monumental shift in global economies — a shift from trusting humans to one of trusting algorithms and machines.

This shift has already happened in other aspects of our lives, so it makes sense that it would eventually happen in economics as well. We trust algorithms over humans to give us driving directions, music recommendations, or search results, but for some reason continue to believe that humans are better than machines at synthesizing financial and economic data to produce decisions on highly complex economic issues.

Obviously, this is going to change and I'm betting that it will happen sooner rather than later. While the humans are struggling to figure out how to manipulate currencies and economies to keep the bull market raging on, Bitcoin continues to produce block after block completely unmanipulated by any outside force.

As Villeroy de Galhau, a member of the Governing Council at the European Central Bank (ECB), recently said " *the [ECB] priority is to reduce this uncertainty and here we will do our duty as central bankers, but monetary policy cannot do everything. Monetary policy has no magic wand, it cannot make miracles. And it's up to political leaders to reduce these uncertainties, sometimes self-created.* "

I, for one, don't find it comforting to rely on the bias, greed, fear, and general emotion of politicians and central bankers. The machines are smarter, more disciplined, and better decision makers than us, so the sooner we admit that, the better off we will be.

-Pomp

[The differences between Bitcoin and Libra should matter to policymakers]

By [Peter Van Valkenburgh]

Posted July 8, 2019

The two have different design goals, work in different ways, and raise different regulatory questions.

Recently Congress has taken a strong interest in the newly announced Libra digital currency. We have been getting many questions from policymakers and the media about how Libra (as described in its white paper and accompanying materials) compares to Bitcoin and other cryptocurrencies. We thought we'd share our thinking on this here.

Our answer is that Bitcoin and Libra are very different projects that use very different technologies and, as a consequence, each project faces different regulatory and legal challenges. It's important that policymakers understand these differences so that they may appropriately tailor any necessary policy response. If they overlook these differences, policymakers risk adopting a one-size-fits-all response that would inevitably result in unintended consequences to the detriment of the public. So, we want to make sure policymakers don't confuse Libra with Bitcoin and similar

cryptocurrencies. Let's look at the design goals of each project, the technologies they use, and conclude with a high-level comparison of the relevant laws and regulations.

Different Design Goals and Priorities

To get a sense of their respective goals and priorities, it's instructive to compare the first sentence of each project's white paper. **Bitcoin:** *"A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution."*

Take note that the same thing is being said four different ways. The key message is "money without trusted intermediaries." Bitcoin is peer-to-peer, cash, direct, and without institutions. The design goals of Bitcoin prioritize building a payments network without trusted intermediaries over the network's ease of use, stability, or scalability. The Bitcoin white paper says that people should have access to an efficient and fast online payment technology, but also that it's more important for those payments to work person-to-person without reliance on any corporation or government than it is for those payments to be easy to perform. Bitcoin is a technological response to distrust in corporations and nation states, and was designed to work for a nation's citizens even if that nation's government became tyrannical, and even if that nation's businesses and corporations were untrustworthy or monopolistic.

Libra: *"The goal of the Libra Blockchain is to serve as a solid foundation for financial services, including a new global currency, which could meet the daily financial needs of billions of people."*

Take note that this sentence is all about scale and access. Libra should "meet the needs of billions"; it should be a "solid foundation" for a variety of "financial services," not just cash-like payments; and it should be "global." The design goals of Libra prioritize scale and inclusivity over the need to avoid reliance on trusted intermediaries.

Both projects take for granted that something is wrong with the current global financial system. The problem that Bitcoin seeks to address is the consolidated power of intermediaries in that system and the danger that such power poses: corporations and governments can arbitrarily block people from participating in the economy. The problem that Libra seeks to address is the inefficiency of intermediaries in that system and their disinterest in providing services to persons who are insignificant to their bottom line.

Different Technologies Employed

Bitcoin and Libra both use distributed ledgers (loosely called blockchains) to record payment transactions between users. In short, both projects intend to create money by sharing data over the internet. That's generally where the similarities end.

Bitcoin is the first of a now broad class of innovations often called cryptocurrencies. It is money **based on economic scarcity** with transactions recorded on a censorship-resistant ledger that any anyone can both access (read data from) and append to (write data to). In other words, the Bitcoin ledger is **public and permissionless**. Libra is the latest of an older class of technologies often called digital currencies. It is money **based on trust in an issuer** with transactions recorded on a ledger that anyone can access and view, but only an authorized set of corporations can amend. In other words the ledger is **public and permissioned**.

Cryptocurrencies are defined by their lack of reliance on trusted intermediaries. While none of these terms are official or uncontroversial, we believe that Libra is not a cryptocurrency because of its use of a permissioned ledger and its reliance on a trusted issuer to hold and manage a fund of assets that back the currency. Libra is still part of the broader category of digital currencies along with airline miles, World of Warcraft gold, or Liberty Reserve Dollars.

Here's a chart reiterating these fundamental differences in architecture:

	Basis of Value	Read access to ledger	Write access to ledger
Bitcoin	**Economic Scarcity** Supply is fixed. Demand sets price. Mathematically verifiable scarcity of units on ledger creates fixed supply.	**Public** Anyone can download the blockchain and see transactions. Transactions use random but unique numbers to identify sender and recipient on the ledger.	**Permissionless** Anyone with commonly available hardware, an internet connection, and free software can add transactions to the ledger.
Libra	**Trust in Issuer** Supply is adjusted by a consortium of corporations to match a quantity of other assets held in reserve and maintain stable value even if demand shifts.	**Public** Same as above.	**Permissioned** Only authorized members of a consortium of corporations can add transactions to the ledger.

These varying architectural choices are not arbitrary. Bitcoin's primary goal is to obviate the need for trusted intermediaries in online payments while Libra's goal is to make online payments easier, more inclusive, and scalable. If you are willing to trust an issuer, then you can likely have a digital currency with less price volatility (because

supply can be adjusted in response to shifts in demand). If you are willing to rely on a permissioned set of transaction validators, then you can likely get transactions validated faster and at a greater scale because fewer parties need to reach consensus. These are the assumptions inherent in Libra's design. Bitcoin's design is largely indifferent to these goals; its singular priority is to be resilient and unreliant on any such trusted intermediary. If that means that bitcoins will be more volatile in price, or that it will be more difficult to scale the Bitcoin ledger to several thousand transactions per second, so be it.

These choices also have consequences for how each project's asset functions. Bitcoin ends up working like a bearer instrument: anyone who has the bitcoin automatically has the value. Libra ends up working like a registered instrument: the holder of a Libra really only has the value of that Libra if the official registrar, the Libra Association, says that they do and maintains the underlying reserve assets. Bitcoin, therefore, is censorship-resistant and functions like gold coins or any other valuable commodity. Libra transactions can be censored and the asset functions like a bank note or stock certificate.

Here's another chart to illustrate how bitcoins and libras differ as assets:

	Censorship Resistant?	Analogous Assets
Bitcoin	**Yes.** A person wishing to censor Bitcoin transactions would need to spend more computing resources than the rest of the network combined.	**Gold or other valuable and scarce commodities.** Mere possession of the thing conveys value. Can be traded from person-to-person.
Libra	**No.** A person wishing to censor Libra transactions can persuade or compel the Libra Association and its member corporations to do so.	**Banknotes or securities.** Value is dependent on an intermediary that backs the value of the thing with other assets and the wise management of those assets. Can only be traded from person to person if the official registrar of transactions adds the trade to the official ledger.

Different Regulatory Consequences

Broadly speaking, financial regulations are in place to ensure that persons performing trusted roles within the financial system do not betray that trust. For example, if you are trusted with holding or managing someone's wealth you should honor that trust and not enrich yourself at the expense of your customer. Bitcoin and similar cryptocurrencies are not designed to avoid regulation, but they are designed to minimize the number of trusted parties in an economic transaction. This is because the fewer the number of trusted parties, the fewer the number of parties that can pose a risk to users. A system without intermediaries is a system without

intermediary risk, and thus no need for regulation aimed at safeguarding against the types of risk presented by intermediaries.

It stands to reason, therefore, that a true cryptocurrency will involve fewer regulated parties than a traditional financial service. Fewer but not none. Miners and software developers are not trusted custodians of people's value, so it makes no sense to regulate them as we would regulate a bank or a money transmitter. Exchanges and custodial wallet providers, however, are indeed trusted by Bitcoin users, and therefore consumer protection and anti-money laundering regulation does apply to them.

Even miners and software developers may be subject to some regulations. While they have no more reason to know their customers than a safe manufacturer or a gold miner would have reason to know the people who store gold in safes, they may make warranties or other promises about the products they put into the world. Rather than subjecting these persons to ex-ante prudential regulations like bank chartering or licensing, regulations and laws create ex-post enforced obligations for them not to engage in fraud, breach of contract, theft, and unfair or deceptive acts and practices.

Securities laws exist to address information asymmetries between investors and persons trusted by investors to earn financial returns or manage a fund. Anti-money laundering regulations and sanctions laws exist because financial institutions establish customer relationships and can block the illicit flows of funds through their networks. While these regulations often apply to persons using Bitcoin to raise money (ICOs) or to offer exchange services (exchanges), there are obvious reasons why these regulations don't apply to Bitcoin as a network writ large: Bitcoin doesn't have a trusted institution minting it or a fund that backs its value. Bitcoin miners validate transactions but don't establish customer relationships, and they don't have the power to reliably block specific persons from sending money through the network.

Libra, on the other hand, is not designed to minimize the number of trusted parties in an economic transaction. Quite the opposite. Libra is designed to maintain a stable value and users trust the Libra Association's management of a reserve fund to achieve that goal. Users also rely on the permissioned validators to add transactions to the ledger, and but for their participation a transaction would not go through. It's still too early to say whether these trusted parties should or would be subject to securities or anti-money laundering law, but it might be hard to argue that they should not since with trust comes responsibility.

Pathways for DeFi on Bitcoin

By Mohamed Fouda

Posted July 10, 2019

	Centralized	Decentralized Efforts			
		Cross chain swaps	Federated Sidechains	Using other blockchains	Native Bitcoin/ Layers on Bitcoin
Exchanges	coinbase, kraken	ARWEN, SUMMA		WBTC, Cosmos Zones	
Derivatives	CME Group, Bakkt			WBTC, Cosmos Zones	Discreet Log Contracts, TRADELAYER
Lending	GENESIS CAPITAL, BlockFi			WBTC, Cosmos Zones	Discreet Log Contracts, MAST
Stable coins				WBTC	TRADELAYER

Decentralized Finance (read **DeFi)**has been a popular narrative for many crypto investors and enthusiasts. DeFi builds upon the promise that several critical financial services are cheaper and more efficient when the role of intermediaries is downsized or eliminated altogether. Theoretically, it also makes online financial services more inclusive since it transcends artificial barriers like different geographic boundaries or jurisdictions.

DeFi products and protocols are made possible by allowing us to code the rules (and consequences) of our financial interactions into permissionless blockchains. Consequently, it comes as no surprise that almost all current DeFi projects have been developed on Ethereum to leverage its smart contract functionality.

DeFi movement is rapidly growing

However, Bitcoin is still the most liquid, familiar, and decentralized cryptocurrency in the world (with dominance exceeding 60% at time of writing). This obviously positions bitcoin as a strong competitor for financial products that can benefit from trustlessness and decentralization. ***However, just because it is obvious does not mean it is easy.***

Bitcoiners want to preserve the *hardness* of Bitcoin at all costs and are not willing to radically change the monetary policy for any reason, DeFi or not. There is no chance smart contract functionality would be added to the Bitcoin protocol to allow for the implementation of DeFi products, though sidechain solutions like RSK exist.

But, that does not mean Bitcoin DeFi could never happen.

Many individuals and teams are striving to use Bitcoin, *with its current structure*, in financial products ranging from centralized to almost completely decentralized.

In this article, I discuss how Bitcoin DeFi can be made possible. The different technological approaches are explained along with the different use cases that they target.

But First, What Do We Mean by DeFi?

Decentralized Finance or **DeFi** is an umbrella term for all the financial services that can be performed without a central authority or when the mechanism to control the financial product is decentralized between different entities. DeFi products include decentralized lending, decentralized exchanges, decentralized derivatives or even

decentralized issuance of stable coins. Many argue that ***decentralized payments on their own are DeFi products.*** I happen to agree with this argument. In this regard, BTC is the cryptocurrency with most merchant adoption. Services like BTCPay Server even allow merchants to receive BTC directly without a third-party payment processor. Therefore, this article is mainly about how Bitcoin can *expand* its DeFi footprint beyond decentralized payments.

Overview of Bitcoin Centralized Financial Products

Before diving into the pathways for DeFi on Bitcoin, let's start with some of the "centralized" financial services currently using Bitcoin. These will be prime targets for decentralization once DeFi can be efficiently executed on Bitcoin.

Bitcoin Lending

One of the most popular financial services built on Bitcoin is lending. We can categorize companies in this area into two buckets. First, are the companies that allow investors to borrow Bitcoin and other cryptocurrencies for trading or market making purposes; the most well-known company in this sector is Genesis Capital. Genesis Capital has reportedly processed $1.1B of crypto loans in 2018, ending the year with ~ 75% of these loans in BTC.

The other line of lending businesses are the companies that offer BTC-collateralized loans such as BlockFi and Unchained Capital. To protect against collateral value volatility, these companies only issue over-collateralized loans with loan-to-value ratios of 20–50%.

Margin Lending

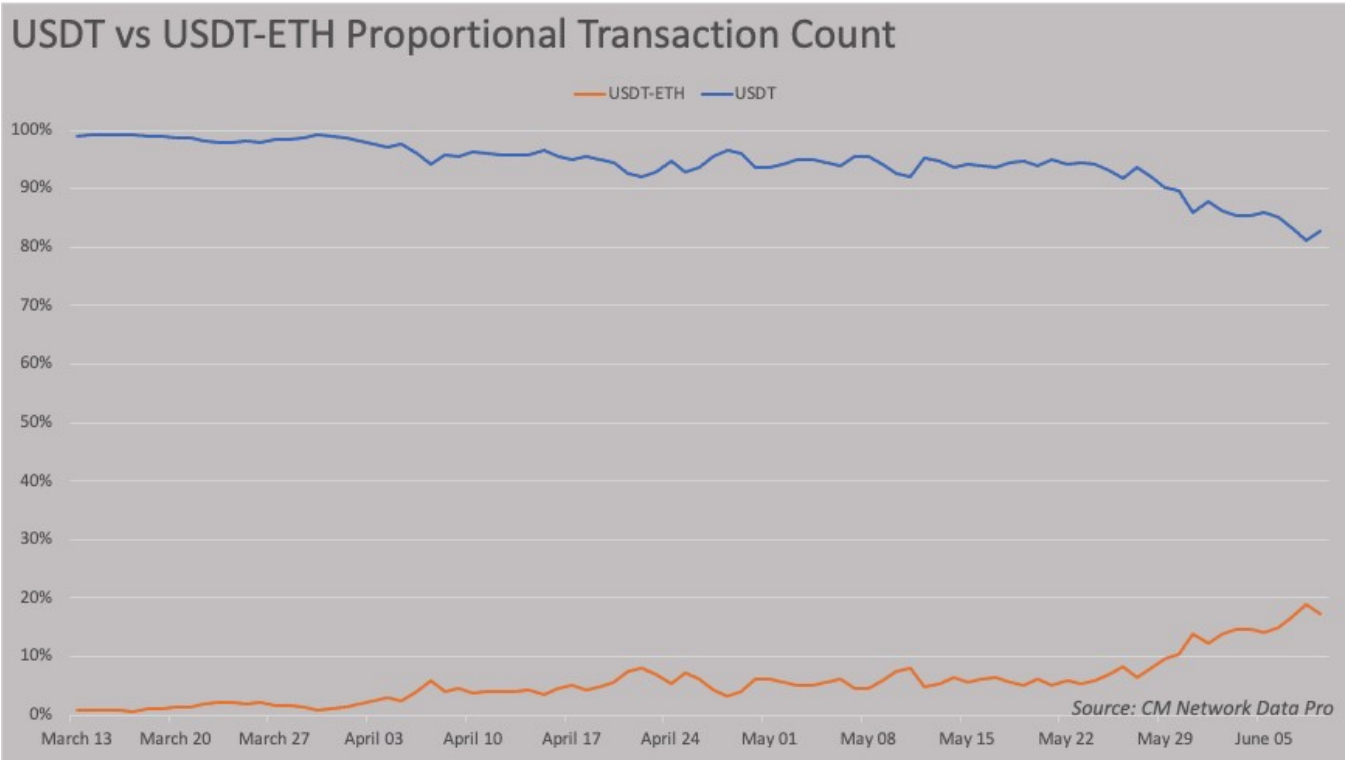
Margin lending is a special case of collateral-based lending used for leveraged trading. In such scenarios, the borrowed funds are not allowed to leave the lending platform. Instead, if the trade loss is equal or below the collateral value, the margin position is liquidated to return the funds to the lender. Exchanges, such as BitMex, Kraken, Bitfinex, and Poloniex, are the major players in margin trading field. However, most of these products are not available for US customers because of regulatory uncertainty.

Stablecoins

Stablecoins that can be transferred easily with low fees have specifically been of interest to traders who want to benefit from volatility but keep a stable value when they are not in active positions. Tether (USDT) was one of the earliest stablecoins

offered to address this issue. It was completely built on Bitcoin using the OmniLayer protocol. OmniLayer allows the creation and transfer of assets using Bitcoin transaction's opcode space.

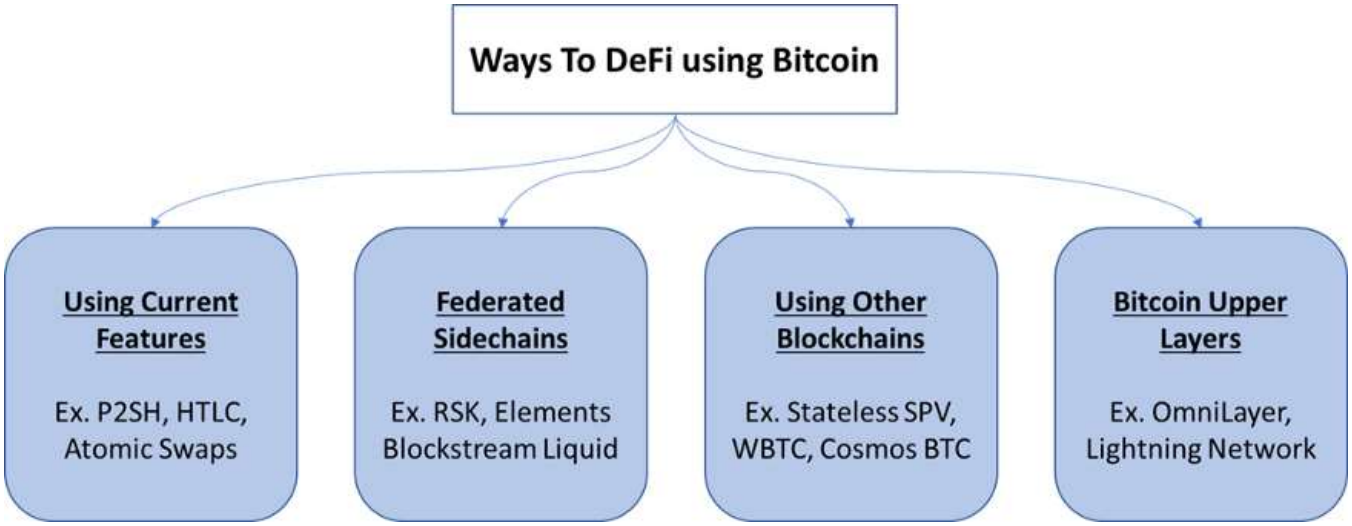
USDT was created as a stablecoin pegged to the dollar with the promise that the USDT tokens are only minted when corresponding USD deposits are credited to the Tether company and burnt when the USDT tokens are redeemed back to USD. Although Tether can be transacted in a decentralized way, it is centralized in the most important aspects: reserves and control. The Tether company holds and controls all the USD reserve for the issued USDT tokens in its bank account which regularly puts them in legal headwinds.



USDT usage on Ethereum is stealing activity away from USDT Omni activity. Source: CoinMetrics

Recently, Tether started to reduce its dependence on the Bitcoin network by issuing USDT on other blockchains like Ethereum and EOS, which has been taking activity away from the Bitcoin blockchain.

Decentralized Finance in Bitcoin



Possible technological approaches to use Bitcoin for DeFi

Now let's look into how DeFi products can be used with Bitcoin and list a few use cases and projects in that area. The possible use cases include decentralized exchanges (DEXs), decentralized lending, decentralized stablecoins, and decentralized derivatives. The technological approaches to implement Bitcoin DeFi include

1. Using Bitcoin current capabilities such as Hash Time Locked Contracts (HTLCs) to facilitate direct cross-chain atomic swaps to build decentralized exchanges with other cryptocurrencies.
2. Federated sidechains to Bitcoin such as Blockstream's Liquid. These sidechains use two-way pegs to the Bitcoin blockchain and allow the use of pegged BTC in various financial activities.
3. Using Bitcoin within other protocols such as Ethereum or Cosmos to interact with DeFi products.
4. Using layers on top of Bitcoin like OmniLayer or Lightning Network.

These technologies differ in capabilities and the range of DeFi applications they can support. In addition, most of these technologies are work in progress. In the following, we explore these technologies and the use cases they target.

Cross-chain Swaps For Decentralized Exchanges

The simple premise of DEXs is to execute trades between Bitcoin and fiat or between Bitcoin and other cryptocurrencies while keeping custody of your coins until the trade is completed. In other words, trading without the need to deposit your valuable bitcoins into a centralized exchange wallet and be subjected to the exchange security risks.

While such trades can be performed using platforms like LocalBitcoins or OpenBazaar, these platforms are only suitable for once-in-a-while slow trading and are not suitable for fast or frequent trading that allows efficient price discovery. For the latter, a centralized order book along with the ability to quickly settle trades is needed. Practically speaking, building a truly decentralized exchange is one of the hardest challenges in DeFi. As long as you have centralized servers keeping or even displaying the order book, you still have centralized components. However, our focus here is mainly around keeping custody of coins until trades are settled. In this domain, we believe a small number of companies are developing the technology needed to achieve that. The ones that we feel at the leading the pack are Arwen and Summa.

Arwenuses the concepts of trustless on-chain escrows and cross-chain atomic swaps to allow non-custodial access to centralized exchanges order books. In that sense, it is possible to trade efficiently on a centralized order book while maintaining custody of the asset until the trade is executed. Currently, the product only supports cryptocurrencies that use the same codebase as Bitcoin such as Litecoin and Bitcoin Cash. They are working on implementing cross-chain atomic swaps between Bitcoins and Ethereum and ERC-20 tokens. Arwen can currently be used (in beta) on Kucoin exchange.

Summahas invented the Stateless SPV technology to allow for trustless financial services for Bitcoin and other blockchains. Stateless SPV allows for validating Bitcoin transactions using an Ethereum smart contract making it possible to perform a wide range of financial transactions using Bitcoin. Using that technology, Summa's team performed an auction using bitcoin bidding for Ethereum-issued tokens. The team is working on generalized cross-chain exchanges between Bitcoin and Ethereum and ERC-20 tokens.

Bitcoin DeFi Using Federated Sidechains

Bitcoin sidechain is a concept that was proposed by Blockstream in 2014 to introduce new features to Bitcoin without changing the protocol base layer. Since then the concept has developed significantly. The simple idea of sidechains is to create a separate chain with a small number of validators (called a federation) and use a token in that chain that is a pegged to BTC through a two-way peg. The benefits can include faster transaction confirmation or implementing features that may be controversial such as confidential transaction, tokenization of other assets or smart contracts. The main drawback of sidechains is the need to trust a small federation to operate the sidechain and keep it running. There is also a risk of losing money by using sidechains if, for any reason, sidechain validators decided to abandon the chain. In those situations, pegged assets would get stuck and cannot be redeemed back to BTC.

A notable sidechain working to bring smart contract functionality to Bitcoin is RSK. It supports Solidity smart contracts making it easy to migrate Ethereum DeFi protocols to RSK. In addition to RSK, Blockstream has commercially launched its Liquid sidechain product in 2018. However, Blockstream's initial focus is around the tokenization of assets and faster transaction but the concept could be expanded later to support DeFi applications.

Decentralized Derivatives Using Bitcoin Layers

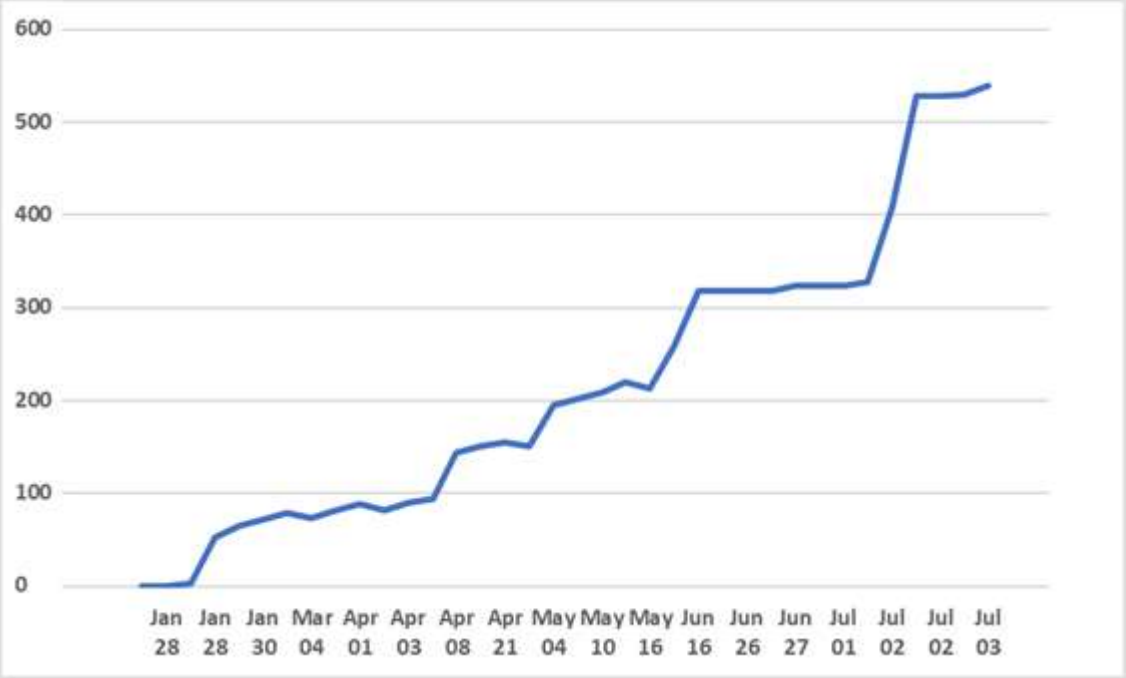
A third approach to implement Bitcoin DeFi products is to utilize intermediate layers built on top of Bitcoin such as Lightning Network or OnmiLayer. As LN is a relatively new Bitcoin development, building complex DeFi products using LN is a topic of research. The most notable effort there is Discreet Log Contracts which are discussed in some detail at the end of this article.

The other option is using OmniLayer. One of the interesting projects in this regard is Tradelayer, which is trying to implement decentralized derivative markets on Bitcoin. The project aims to extend the OmniLayer protocol with multisig channels to allow for using Bitcoin, or other tokens issued on Bitcoin, as collateral for peer-to-peer derivative trades. A possible scenario is to have traders pledging capital to multisig addresses and co-sign transactions and trade updates to settle the derivative trade. In this sense, users can take leverage natively and get fast-execution by co-signing trade transactions. Using the same methodology, another possible use case could be the issuance of stable coins using Bitcoin as collateral the same way Ether is used to collateralize DAI issuance on MakerDao.

Bitcoin DeFi With External Help

Wrapped BTC on Ethereum

A completely different approach to allow using Bitcoin in DeFi is to leverage other networks like Ethereum or Cosmos. As most DeFi projects now work on Ethereum, it seemed logical to try to find ways to use BTC on Ethereum. The simplest idea is to issue a BTC-backed ERC20 token (WBTC) that can be traded on any Ethereum DEX or used in various Ethereum DeFi projects. The BTC used to mint WBTC are secured in mutisig wallets maintained by the project custody providers. As of early July 2019, only ~ 540 WBTC were minted is a tiny fraction of the BTC circulating supply.

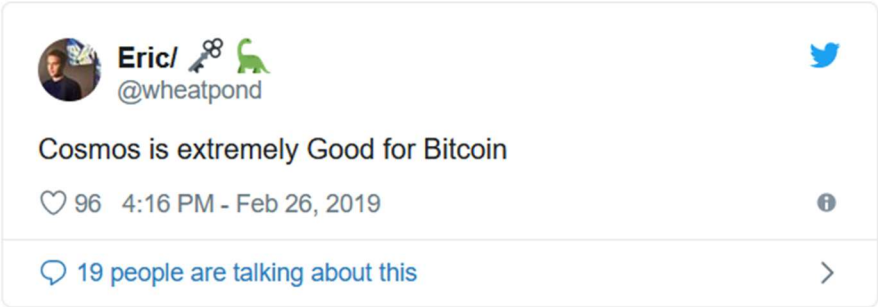


Growth of the Wrapped BTC (WBTC) supply over time

While WBTC may facilitate using BTC in DeFi, it suffers a few important drawbacks. The first and most important is counterparty risk. The BTC used to collateralize WBTC is maintained by centralized parties that might be hacked. Secondly, introducing intermediate entities to custody the assets (BTC) to some extent kills the point of the DeFi movement. Finally, to use BTC/WBTC in DeFi, users have to pay fees in ETH, which is something many Bitcoin fans are not willing to do.

Cosmos Zones

Interoperability blockchain projects, such as Cosmos, opened new opportunities to bring DeFi to assets like Bitcoin. For example, Cosmos protocol defines Peg Zones where assets (issued on Cosmos) can be pegged to other blockchain assets like Bitcoin. In these zones, it is possible to add smart contract functionality to the pegged asset and benefit from faster finality. This approach has garnered the support of some hardcore Bitcoin supporters like Eric Meltzer for one specific reason: in this approach, Bitcoin will remain the native currency to pay fees and use the peg zone. Bitcoiners can stake their pegged bitcoins in the zone to process the zone transactions and claim the zone fees. In that sense, Bitcoin will benefit from the new tech without depending on a different asset. This comes in stark contrast to WBTC, which requires using ETH to pay for fees or interact with DeFi protocols.



It is worth mentioning that using Cosmos zones for Bitcoin DeFi is still work under development and there is a number of stealth projects that are building it. It is not clear yet how the two-way peg between Bitcoin and Cosmos would work. The implementation of the Cosmos Inter-Blockchain Communication (IBC) is not yet finalized. If the two-way peg requires custodial services, like WBTC, or a few validators to execute the peg, like federated sidechains, the Bitcoin zone on Cosmos will not offer much differentiation to other solutions.

In addition to the projects that are building such systems for Bitcoin, we are seeing a lot of interest in using Cosmos for bringing DeFi to other assets such as Kava Labs. If these efforts deemed successful, barriers for Bitcoin use in DeFi would significantly diminish. Success in this regard is to be able to attract sufficient liquidity to the peg zone and to maintain a reasonable level of decentralization by attracting a large enough number of validators.

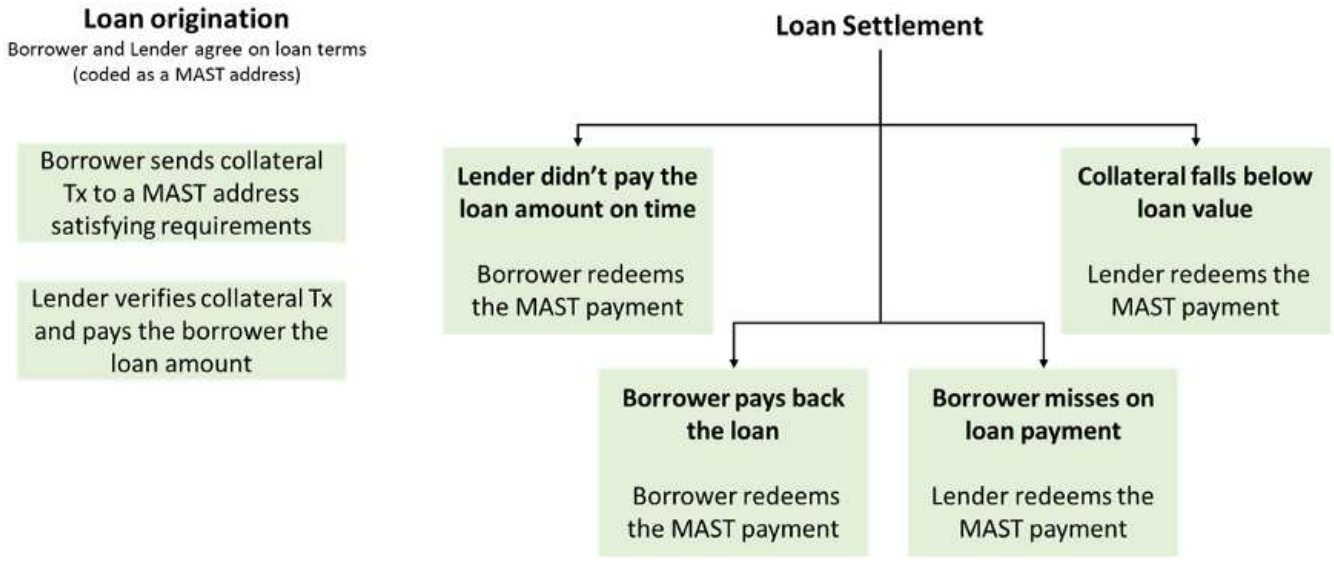
Research to Expand Bitcoin DeFi Capabilities

Merkelized Abstract Syntax Trees (MAST)

Bitcoin, in its current form, has a limited form of smart contract capabilities through the Script language. Script is not a Turing-complete language meaning it cannot be used to describe general programs. However, it still can be used to implement some smart contract functionality. This is done via Pay to Script Hash (P2SH) and SegWit addresses, in which, a transaction cannot be spent unless some conditions (defined through a Script program) are satisfied. The problem with that approach is that complex transactions with multiple conditions would be excessively large, making them too expensive to use. For those reasons, there is a proposalto implement Merkelized Abstract Syntax Trees (MAST) in Bitcoin. MAST is simply an extension to the P2SH capabilities that would make it cheaper and viable to utilize complex conditions to spend Bitcoin transactions. While the obvious benefit of MAST is improving Bitcoin scalability by saving block space, the less obvious benefit is that it could allow for some Bitcoin DeFi use cases. For example, *if we assume a*

decentralized price-feed oracle can be implemented, MAST could allow for decentralized lending or even decentralized stable coin issuance using BTC as collateral.

The following diagram shows a possible decision tree for a decentralized lending scenario using MAST. The various conditions for the loan settlement can be coded into a redemption script and hashed into a MAST address. The MAST address can guarantee fair execution of the loan and that the lender would get the loan collateral if the borrower didn't pay back the loan on time or if the collateral value goes below the loan value plus interest.



Discreet Log Contracts

Another research idea that can expand Bitcoin DeFi capabilities is the Discreet Log Contracts (DLCs) suggested by Tadge Dryja of the MIT Digital Currency Initiative (DCI). A simple explanation of a DLC is that it is a way for two parties to create a Futures Contract which is simply a bet on the future price of an asset. A DLC requires both parties to select an oracle (or a number of oracles) that publicly broadcasts the asset price before they create the contract. At the time of the contract settlement, any of the two parties can use the publicly broadcasted signed messages from the oracle to settle the contract and claim their profits. DLCs utilize Schnorr signatures to hide the contract details from the oracle. This guarantees the oracle cannot game the output of the contract. As DLCs use similar technology to that of Lightning Network, it is possible to integrate DLCs with LN channels.

Conclusion

DeFi protocols have been generating a lot of buzz since early 2018. While Ethereum is recognized as the lead protocol within the DeFi movement, developers and investors have been eyeing the massive potential of Bitcoin in DeFi as the most liquid cryptocurrency. This great interest is pushing many developer teams to figure out the best ways to make it happen. While this would bring even more competition between Bitcoin and Ethereum and probably all new smart contract platforms, such competition is what is needed to encourage progress and deliver the vision of a public decentralized financial system.

I would like to thank Matt Corallo, Tony Sheng and Matthew Hammond for their feedback on this article.

BetterHash: Decentralizing Bitcoin Mining With New Hashing Protocols

An Overview Of Mining Pool Exploits That BetterHash Disables

By StopAndDecrypt

Posted July 14, 2019

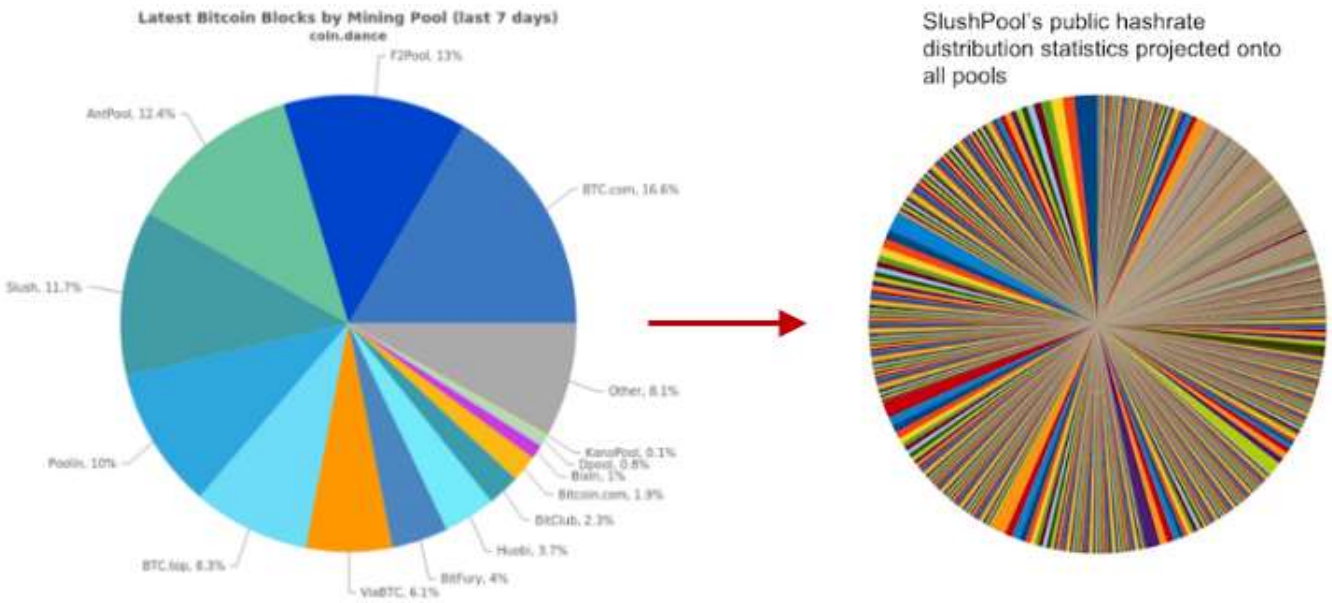
Intro

BetterHash is the working name for alternative mining protocols currently in development. When it's completed there will need to be enough miners willing to switch to a new mining pool using these protocols, or an existing pool that is willing to service both the old and new protocols while miners gradually ready themselves to switch over. In either circumstance the initial switch will need to be supported by enough miners to make doing so profitable, else profit volatility would be too high. Ultimately miners will need to understand why they should switch, and there will need to be forward thinking pool operators who *don't* want the control current pools have. This can only happen if the problems and risks with the current system are properly understood and conveyed.

Disclaimer: This is not a fork, or a consensus rule change.

So what exactly is wrong with Bitcoin mining now?

Bitcoin mining has a representation problem. Bitcoin mining *pools* are not Bitcoin *miners,* yet pools unduly signal for them. Pools run the node, construct the block, select the transactions, and can choose what fork all of their miner's hashpower is used for. This creates a handful of incentive issues and enables some pretty undesirable political leverage. BetterHash aims to address this by giving those responsibilities back to the individual miners, and stripping the mining pools of their influence for the greater good of the network. With BetterHash miners would control their own hashpower, and pools would just coordinate them and distribute the rewards.



Mining **pool** hashpower distribution, versus Slush Pool's **miner** distribution projected onto every pool.

This article aims to highlight the kinds of exploitation pools can conduct under the *current* mining environment — *of which would not be possible if BetterHash-like protocols were adopted* — at the expense of what may be the miner's best interests. Pools can also be hacked and then used by the attacker to engage in this behavior. Before we get to that let's briefly go over the structural differences between what exists now and what BetterHash protocols would change about it.

Currently, many miners don't even run nodes and simply connect their ASICs to a mining pool using protocols like Stratum. The pool runs the node, selects the transactions, creates a block they would like mined, and then sends that block out to all of the miners using their pool and the miners begin hashing it. Once a miner successfully mines a block, it gets sent back to the pool and out to the Bitcoin network.

With BetterHash, miners will individually run their own nodes, select the transactions, create a block, and then mine it. The block would be configured to pay the pool, and just like with the Stratum protocol, those unsuccessful blocks *(called "shares")* would be used by the miners to prove they've been mining for that pool the whole time.

By just changing who creates the block template to be mined to the individual miners, instead of the pool owner, and then building a new protocol around that concept, BetterHash circumvents all the issues we're going to cover.

For a more technical overview on the BetterHash protocols currently in development, this presentation by Matt Corallo should suffice, but is not necessary to understand the exploits this article discusses because conceptually BetterHash is objectively

better, and a fully codified implementation doesn't need to exist in order to grasp how important this is.

It should be noted that the name "BetterHash" is not definitive, as mentioned in the video.

https://www.youtube.com/watch?v=0lGO5l74qJM

The Status Quo

To understand why switching to BetterHash is so important, let's unpack all the problems associated with the way things are now for miners that wouldn't exist if they were using BetterHash.

To be brief, mining on your own has returns that are most likely too volatile, which is why pools have existed since as early as 2010. Critics will point at pool distributions to claim Bitcoin mining is centralized, and while counterarguments assert miners can just switch the pool they use, it's not always that simple. If you're a miner your options are limited to a handful of mining pools, each with their own terms of service that you may or may not agree with. Pools are too large to provide a diverse set of options to pick from.

At the end of the day you have no choice but to choose the pool best suited to you, and if most or all of the pools decide that some practice you don't like or agree with is going to be the norm, then you have no real alternative but to deal with that, since starting your own pool probably won't produce a steady enough income stream. Pools that already exist are relatively large, and by having many miners under each of their umbrellas, pools have the power over their miner's hashpower to do a number of questionable things that we'll go over one by one.

Pools can:

- Determine what transactions do or don't go into a block
- Be bribed to reorganize the blockchain under the right conditions
- Backlog transaction mempools to inflate the fee rate
- Direct hashpower without consent & mine competitive forks
- Dishonestly mine, should they have ulterior motives for doing so
- Signal support for a proposal using a miner's hashpower

All of these issues are essentially the direct result of pools building the Bitcoin blocks instead of the miners, as mentioned earlier. Along with pool exploitation comes third-party exploitation of the pools. Pools can be hacked and then the hackers can potentially conduct these exploits, or pools can be attacked from a network level and then miners are left scrambling to figure things out or switch to another pool. With

BetterHash a pool hack wouldn't be able to control a miner's hashpower, and network level attacks targeting a pool wouldn't have a direct effect on the miners using that pool.

Network level attacks are just as concerning if not more than pools exploiting their miner's hashpower. An attacker can bring down a large chunk of the hashpower or redirect it as they please. BGP attacks are easy to do and the time & resources required to recover from them is concerning, to say the least. **To convey how trivially an attacker can steal a pool's hashrate and conduct any of the exploits written in this article**, watch 3 minutes of this presentation below:

https://youtu.be/k_z-FBAil6k?t=353— Network level attacks discussed at the 5:52 mark, ends at 9:00.

There's no doubting the benefits of a protocol that defends against these kinds of issues, but solutions to often unheard of potentialities don't always do a great job on their own conveying their necessity. I'd like to bring to light some hypothetical scenarios as well as some that have already occurred in some fashion, so that necessity is more readily understood. So let's take a closer look at what each of them are. *(Please note that some of these are hypothetical and unlikely to actually occur, and some require very specific circumstances, while others have occurred in one form or another already.)*

1: Pools determine what transactions go into a block

Often an issue raised when discussing the possibility of 51% attacks, if enough pools can be convinced to blacklist a transaction type or an address, even temporarily , then it doesn't matter if you — *a miner* — personally don't care and would have included it. The motivation for this could be coercion or just a financial incentive to do so, whether the pool's own, or a external one paid to the pool.

Scenario #1: Censoring a service's hot-wallet

Imagine an exchange's hot wallet being blacklisted by 40% of the pools, paid for by a competing exchange? It wouldn't bar that wallet from transacting indefinitely, but it would noticeably slow down their transaction processing. As a miner, maybe you don't think that behavior is healthy for the ecosystem, but maybe you just have no other choice since you have no say in what your pool does in secret.

Scenario #2: Censoring confidential transaction types

"Maybe the developer was the same kind of lazy", resulting in code that ignored shielded transactions.

The tweet above ended up proving — *if we trust his word* — this example to be non-malicious, but it's still important to consider scenarios in which something like this was done intentionally. Bitcoin doesn't have confidential transactions at the moment — *and may never have them* — but it does have different transaction types. If a pool had a reason for doing so, then they could theoretically ignore them so a backlog of specific kinds of transactions exacerbates, raising fees and potentially slowing down any service that makes use of those specific of transactions.

ZCash Shielded Transaction Censorship In ZCash, privacy is opt-in, which unfortunately makes it possible to censor private transactions. medium.com

2: Pools can be bribed to reorganize the blockchain

Similar to the examples above, pools can decide they don't want a specific *version* of a transaction to be included in the ledger, and then try and act on this decision. Such a scenario would be next to impossible to coordinate spontaneously, or in hindsight, but if pools were so inclined then just a few of them could build software in preparation for a bribe, and then act on it immediately without miners having any say in the matter.

Miners might believe this is in their best interest if the bribe was shared with them, but pools have less of an incentive to do this the higher a share they give to the miners. Additionally, in a hacking scenario the hacker could counter the bribe to the pool, muddying the waters even more.

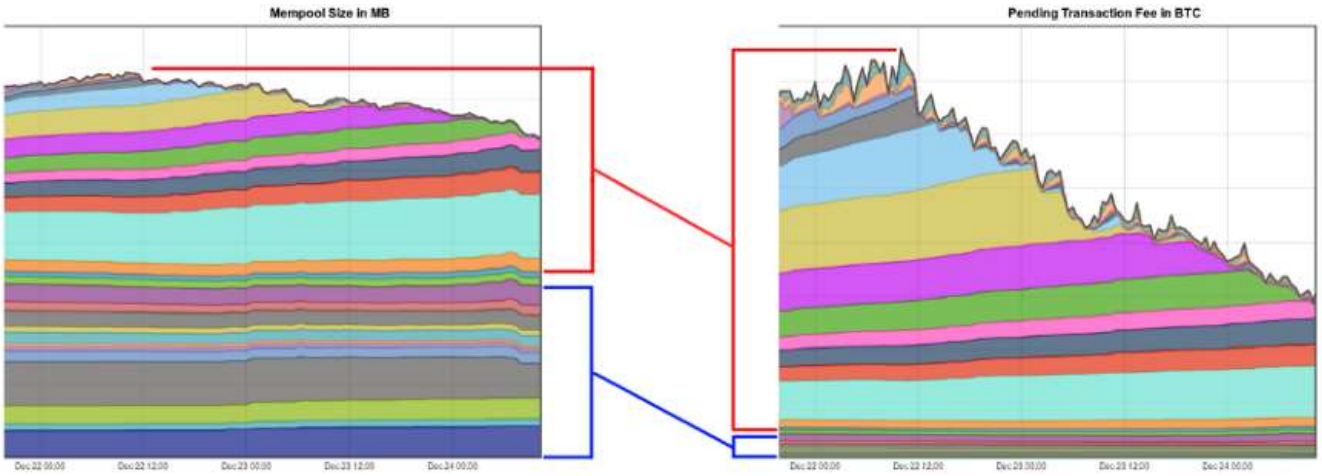
This was a suggestion after the exchange Binance was hacked — *although the pools weren't prepared for it* — and many used this to make arguments about Bitcoin mining being centralized, when in reality it's just the *pools* that have too much leverage over miners that this could even be potentially abused. For more nuance on this subject, give the podcast below a listen and make note that none of the things being discussed in it would matter if BetterHash was being used, because this would have been impossible to even consider if miners built the blocks instead of pools.

3: Pools can backlog transactions to inflate the fee rate

Not only can pools bar specific transactions, they can choose to ignore all transactions below a specific fee rate, raising the costs for everyone trying to transact. Some consider this a trivial issue because smaller pools will take the opportunity to include those transactions since the reward for them is greater, rewarding the underdogs in the long-term. I don't think it's as trivial as this, since we've seen how the effects of this behavior can steer arguments in the political arena over rising fees in the short-term.

Sooner or later a fee market is going to exist, but throttling the network below its consensus enforced limitations shouldn't be a tool granted to a handful of people running pools. While competition may exist at the pool level to counter this behavior, we continue to see empty blocks mined by select pools because the financial incentives are aligned, along with instances in the past where a few specific pools only had transactions that were above 5 satoshis/byte, even when there was room for the remainder of the transactions in the backlog. It might require some coordination among pools to have an effect, but if the incentives align then that coordination isn't difficult or even necessary, and now a small group of pool operators would have a valuable tool at their disposal that nobody else has.

Pools can also do this covertly. Instead of creating "non-full" blocks, they can fill them with what looks like legitimate *but unannounced* transactions that they then collect back to themselves, to throw off people, businesses, and fee estimators by leading them to believe the new "going fee rate" is real. Once the market starts paying the higher price then pools could just adjust their malicious transactions up again. At the time of the image below, the bottom 50% of the TX backlog **in size**accounted for only ~ 7% of the reward miners collected **in fees**. The reward grew non-linearly with the median fee rate in the transaction backlog, making this a lucrative endeavor for any large enough pool wanting to try this out.



https://www.reddit.com/r/Bitcoin/comments/7lwajx/spamming_the_network_unfortunately_doesnt_result/

4: Pools can direct hashpower without consent

In more ways than one, pools choose what chain to extend. Pools feed the miners a block and effectively just say "mine this block", the miners mine that block until it's found by someone, then pools feed them the next block. Miners aren't tracking different branches themselves, and miners generally assume that the pool is being honest and mining the coin/fork you expect them to mine. Many miners aren't running nodes, so they aren't validating the consensus rules. This has caused problems in the past when pools decided that they were also not going to validate blocks, but instead "SPV mine" on top of invalid blocks. As a miner you should want to know that your time and money isn't being wasted by the pool you're using.

A scenario:

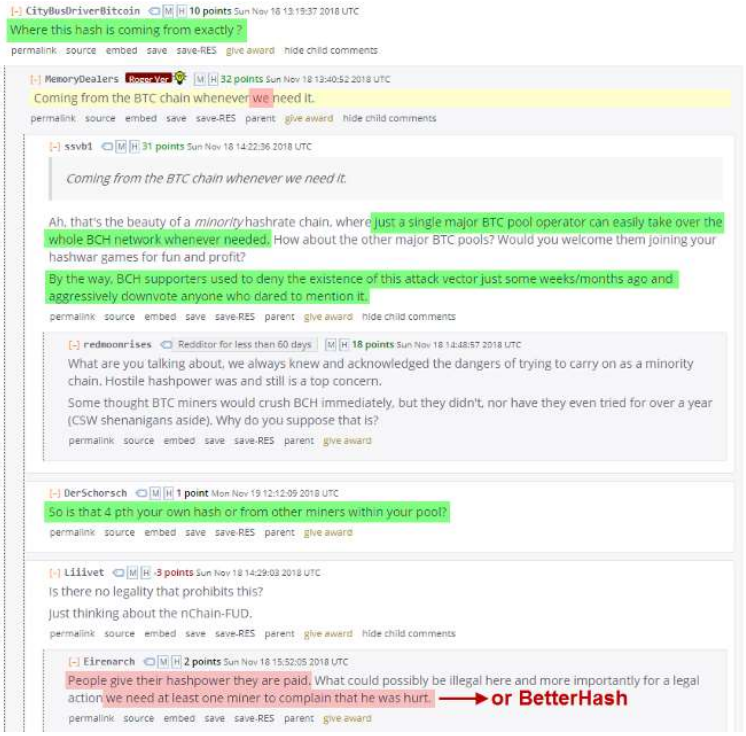
You're a miner, and you're part of Pool_A. You receive a steady stream of payments for the amount of hashpower you provide to the pool. You've done the math, it checks out, and that never changes.

The operator of Pool_A decides they are going to use your hashpower to provide "life support" for another chain that's at risk. One that you don't care about and possibly dislike or consider to be competition. The pool continues to pay you "the market rate" for your SHA256 rigs, but your hashpower isn't *actually* being used on the chain you think you're mining.

Since there's now an entire pool mining a different chain, the network's block production rate slows down — *decreasing rewards* — and the market is potentially fooled into thinking there's more support than there actually is for another chain — *decreasing the potential value of your chain*. As a miner, this is probably a scenario

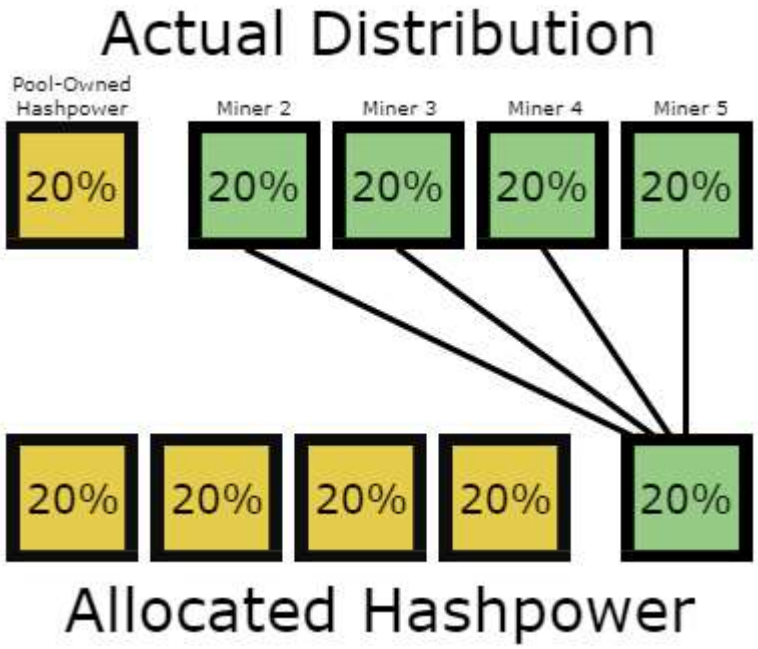
you would want to avoid. Unfortunately, **this scenario has already happened** in real life:

https://www.reddit.com/r/btc/comments/9y5qpj/roger_ver_calvin_if_you_happen_to_watch_this/e9yj4fy/?context=10000
https://www.reddit.com/r/btc/comments/9x2ekv/all_poolbitcoincom_hashrate_to_mine_abc_chain_for/e9ozqes/



5: Pools can dishonestly mine using miner's hashpower

Consider the scenario above to be the best case example of how this would play out: The pool is being *honest* with the miners about their intentions, and they are at least *attempting* to remedy what they think will be the financial burden. They're giving the miners a heads up, and telling them if they don't like it then leave — *which is not always simple*. But what if they were *dishonest*?



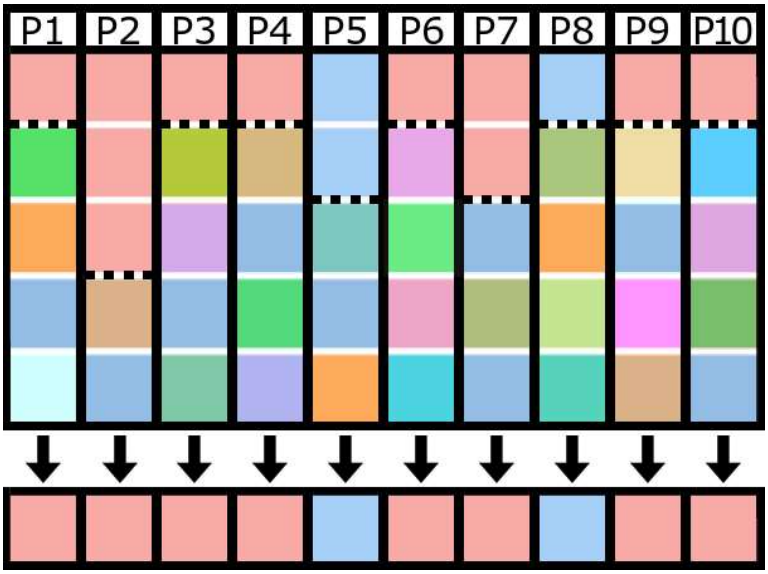
Allocated Hashpower is what a pool signals to the world, but not necessarily what miners intended to mine.

If a pool *showed_they were mining two chains, Yellow & Green at 80% & 20% respectively, and you were mining the Green chain through them,* ***how would you know they were being honest that only 20% of their miners supported that chain?*** *They could individually tell each miner that _they* are the 20% and they're the only ones supporting it, when they really aren't. Miners would have to coordinate on side channels and add up their hashpower to figure out if they're being deceived. The main issue with that is many miners are private, and many want to remain private, will remain private, and should remain private. Coordinating like this is an impractical workaround to avoid being deceived and manipulated.

Not only would this sort of lie allow complete exploitation of all of the miner's combined hashpower, but the disinformation could influence the market's valuation of each chain. Anyone who values the long-term health of the Bitcoin network would want to avoid these kind of scenarios.

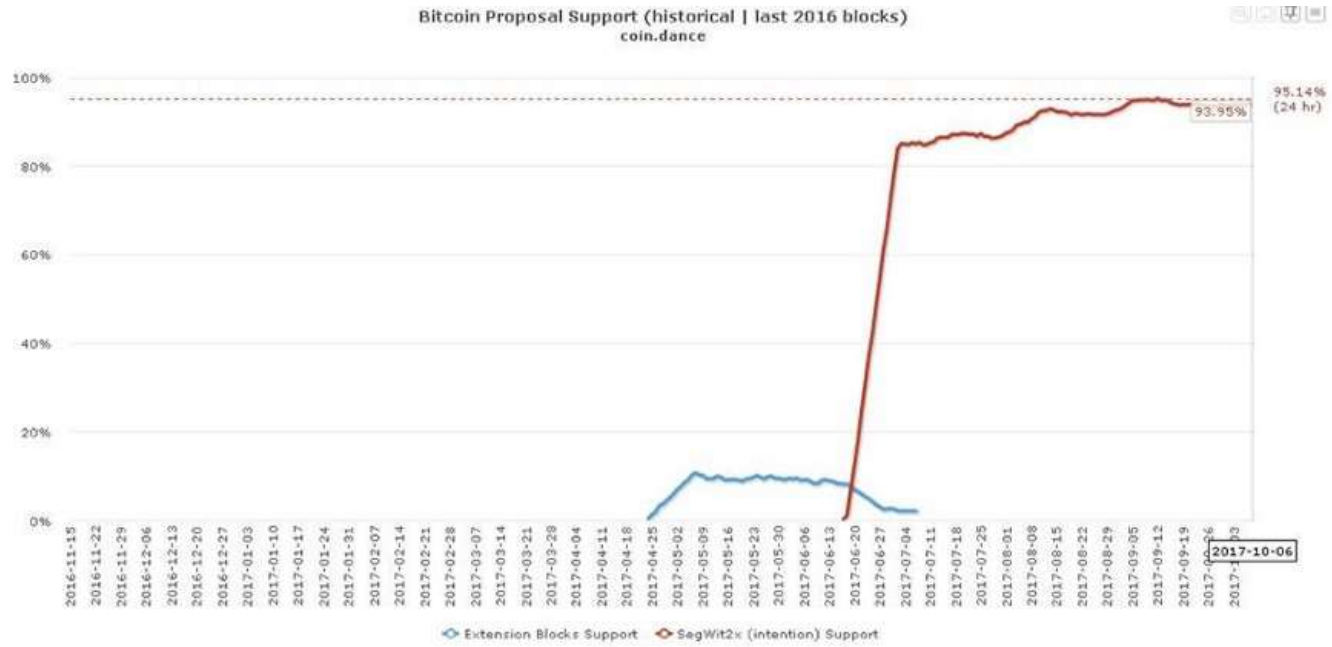
6: Pools can signal for a proposal using your hashpower

There doesn't even need to be an actual chain-split for this kind of manipulation to take place. Since the pool gets to signal for all the hashpower under their umbrella prior to an actual fork, a situation like the one below would give the appearance that 80% of the hashpower is signaling for or against some proposal or fork. Given that signaling isn't a financial commitment, there's little risk involved in doing so. You would only need to persuade the few individuals running these pools to temporarily signal support if you wanted to try and move the market in your desired direction. If it fails — *like we witnessed with NO2X* — then it's at no loss to the mining pools. Everyone's hashpower still works regardless of the result.



Each column represents a pool. The top section of each column represents hashpower owned by that pool, while the bottom section is meant to represent the variety of other miners that use the pool.

No one knows exactly what percentage of hashpower all of the pools actually own versus how much belong to other miners using a pool, but the extra transparency is without a doubt a bonus for the — *effectively* — silent majority of the hashpower without a voice. Nobody wants another NO2X scenario, nor should a handful of pools be able to "decide" that the majority support something when they really don't. Perhaps the NO2X movement wouldn't have been necessary if BetterHash existed a few years ago.



Miners didn't signal for Segwit2X, mining **pools** did.

Conclusion: Perspective Matters

I anticipate there being two different common reactions from people upon reading this, both of which I've already received from a handful of people reviewing it. I think it's important to highlight this for the reader — *you* — and address it.

1. "I didn't know mining pools have so much power."
2. "This can give the appearance that pools have more control than they really do."

Now for the "meta-considerations", at first glance one might think:

"The first person probably didn't know much about mining or Bitcoin in general, and the second person has been around the block and understands the nuances enough to measure these scenarios more appropriately."

Another way one might view this would be:

"The first person is providing a fresh and real perspective on learning about the balances of power in this system, while the second person has been around for a while and has gotten too comfortable and desensitized to the way things are and the potential threats."

Both of those initial reactions are valid. Both of these meta-considerations are valid. If pools had no potential to abuse the system the way it's currently set up than there would be no drive to develop better protocols, and you wouldn't be reading this.

Conversely, if pools were such a significant threat to Bitcoin than they would have abused their power in irreparably damaging ways by now *(see BCash)*.

Alternatively to these polarizing perspectives, this is what I'd like your takeaway to be instead:

BetterHash needs to be implemented, because BetterHash is objectively better than what we have now. Pool abuse and network attacks shouldn't be possible, and we can alleviate these concerns by **simply getting miners to run their own nodes so they can create their own blocks**, and using a better pooling protocol structured around that simple but fundamental change. There's always the potential that something could go seriously wrong if we don't get ahead of a problem that we know how to fix, so let's fix it.

Additional Resources

Bob McElrath: Decentralized Mining Pools for Bitcoin

Off Chain with Jimmy Song : How Mining Pools Work with Matt Corallo

What Bitcoin Did: Matt Corallo on How Bitcoin Works

Thanks to Jameson Lopp and Steve Lee.

Bitcoin Is a Human Right

By Nik Bhatia

Posted July 12, 2019

I have some upsetting news to all the naysayers, doubters, and obituary writers: bitcoin has recovered from yet another supposedly catastrophic price collapse. Bitcoin is now 10 years old and graduated long ago from shady internet drug money to full blown asset class and savings vehicle. The trouble with bitcoin is that it's complicated to grasp. It took me months to half-understand and is so multifaceted only a rare individual could claim to fully understand bitcoin.

I tried to boil down three years of learning into a handful of analogies for the curious bitcoin beginner. This article is written for pre-coiners, a word used to describe people who don't own or use bitcoin yet. I attempt to answer the fleeting question millions of pre-coiners around the world keep asking: what exactly is bitcoin? Bitcoin is money, bitcoin is a land grab, bitcoin is a game, bitcoin works like email, and last but not least, bitcoin is a human right. If you can absorb these five definitions of bitcoin, I have confidence it won't take long to shed your pre-coiner status. And don't forget, you can buy a fraction of a bitcoin!

Bitcoin Is Money

Despite unprecedented levels of price volatility throughout its young life, bitcoin has strongly demonstrated its ability to be used as money around the world. No, you won't necessarily be able to buy a house, car, or meal with bitcoin everywhere you go yet, but you can buy the most useful good of all: US Dollars. Robust markets to exchange bitcoin for Dollars, Euros, and Amazon gift cards are currently flourishing around the world. If you have a gold coin, you might not be able to buy dinner with it, but you're certain to find somebody who will exchange it for dollars. Bitcoin works identically. Several million people around the world already own bitcoin in order to store wealth. They are the early adopters of bitcoin as a new form of money.

Bitcoin Is a Land Grab

There are only 57 million square miles of land on earth. Similarly, there will only be 21 million bitcoin. Mark Twain once said "buy land, they're not making it anymore," and bitcoin should be thought of in the same way. Bitcoin is scarce, just like the amount of land on earth. As more people move from the world of British Pounds, Japanese Yen, and US Dollars to bitcoin world, bitcoin land will only get more expensive and harder to find. People who don't own bitcoin in the future will face the consequence of having to borrow bitcoin in order to use it, much like people that don't own

property renting from landlords. The land grab for bitcoin will continue because people, companies, and governments will realize they cannot afford to be bitcoin renters and not owners. Bitcoin's price has risen over the long term because people are treating bitcoin like prime real estate. There is no single gatekeeper in bitcoin world, making every human being a potential property owner. Ownership will become more difficult and expensive as bitcoin world gets more crowded.

Bitcoin Is a Game

But how does it all work? If bitcoin isn't backed by any government, who controls it? These questions can be answered with the analogy of bitcoin as a game. Every game has a set of rules all players must follow. Bitcoin's rules were created in 2009 and are continually enforced by thousands of players every ten minutes on average (one of the rules). Bitcoin's rules for money creation and value transfer have proven extremely reliable over the years which encourages more people to join the game. You can play the game by downloading software to your computer or phone. Nobody is asking you to learn all the rules to bitcoin today, but you must understand that there are rules just like any sport or video game.

Bitcoin Works Like Email

Everybody uses email. You might not understand the computer science behind how it works, but the simple concept of sending and receiving email is universally understood. Email addresses can be shared with anybody, but only the password holder can access received messages. Bitcoin works in a similar way. You can share your public address with anybody sending you money, but only with your password, called a private key, can you spend it. Bitcoin receives criticism for being difficult to use, but in reality, people just aren't used to it yet. In the near future, understanding and usage of bitcoin will be as ubiquitous as the understanding and usage of email: send and receive.

Bitcoin Is a Human Right

Buying coffee with bitcoin in California isn't revolutionary, but buying food with bitcoin in Venezuela to survive is. With a savings vehicle like bitcoin, every person in the world can now store money safe from seizure and censorship by corrupt governments. Bitcoin is an alternative form of money, one that people should have the right to choose for themselves. Billions of people today have access to send and receive information via the open internet. Tomorrow, billions of people will have access to send and receive value via the bitcoin network. Access to both should be considered basic human rights: if communicating on the internet is freedom of speech, bitcoin is freedom of speech money.

Technical: A Brief History of Payment Channels: from Satoshi to Lightning Network

By Alan Manuel K. Gloria

July 12, 2019

Who cares about political tweets from some random country's president when payment channels are a much more interesting and are actually capable of carrying value?

So let's have a short history of various payment channel techs!

Generation 0: Satoshi's Broken nSequence Channels

Because Satoshi's Vision included payment channels, except his implementation sucked so hard we had to go fix it and added RBF as a by-product.

Originally, the plan for `nSequence` was that mempools would replace any transaction spending certain inputs with another transaction spending the same inputs, but only if the `nSequence` field of the replacement was larger.

Since `0xFFFFFFFF` was the highest value that `nSequence` could get, this would mark a transaction as "final" and not replaceable on the mempool anymore.

In fact, this "`nSequence` channel" I will describe is the reason why we have this weird rule about `nLockTime` and `nSequence`. `nLockTime` actually only works if `nSequence` is not `0xFFFFFFFF` i.e. final. If `nSequence` is `0xFFFFFFFF` then `nLockTime` is ignored, because this if the "final" version of the transaction.

So what you'd do would be something like this:

1. You go to a bar and promise the bartender to pay by the time the bar closes. Because this is the Bitcoin universe, time is measured in blockheight, so the closing time of the bar is indicated as some future blockheight.
2. For your first drink, you'd make a transaction paying to the bartender for that drink, paying from some coins you have. The transaction has an `nLockTime` equal to the closing time of the bar, and a starting `nSequence` of 0. You hand over the transaction and the bartender hands you your drink.
3. For your succeeding drink, you'd remake the same transaction, adding the payment for that drink to the transaction output that goes to the bartender (so that output keeps getting larger, by the amount of payment), and having an `nSequence` that is one higher than the previous one.
4. Eventually you have to stop drinking. It comes down to one of two possibilities:

- You drink until the bar closes. Since it is now the `nLockTime` indicated in the transaction, the bartender is able to broadcast the latest transaction and tells the bouncers to kick you out of the bar.
- You wisely consider the state of your liver. So you re-sign the last transaction with a "final" `nSequence` of `0xFFFFFFFF` i.e. the maximum possible value it can have. This allows the bartender to get his or her funds immediately (`nLockTime` is ignored if `nSequence` is `0xFFFFFFFF`), so he or she tells the bouncers to let you out of the bar.

Now that of course is a payment channel. Individual payments (purchases of alcohol, so I guess buying coffee is not in scope for payment channels). Closing is done by creating a "final" transaction that is the sum of the individual payments. Sure there's no routing and channels are unidirectional and channels have a maximum lifetime but give Satoshi a break, he was also busy inventing Bitcoin at the time.

Now if you noticed I called this kind of payment channel "broken". This is because the mempool rules are not consensus rules, and cannot be validated (***nothing*** about the mempool can be validated onchain: I sigh every time somebody proposes "let's make block size dependent on mempool size", mempool state cannot be validated by onchain data). Fullnodes can't see all of the transactions you signed, and then validate that the final one with the maximum `nSequence` is the one that actually is used onchain. So you can do the below:

1. Become friends with Jihan Wu, because he owns >51% of the mining hashrate (he totally reorged Bitcoin to reverse the Binance hack right?).
2. Slip Jihan Wu some of the more interesting drinks you're ordering as an incentive to cooperate with you. So say you end up ordering 100 drinks, you split it with Jihan Wu and give him 50 of the drinks.
3. When the bar closes, Jihan Wu quickly calls his mining rig and tells them to mine the version of your transaction with `nSequence` 0. You know, that first one where you pay for only one drink.
4. Because fullnodes cannot validate `nSequence`, they'll accept even the `nSequence`=0 version and confirm it, immutably adding you paying for a single alcoholic drink to the blockchain.
5. The bartender, pissed at being cheated, takes out a shotgun from under the bar and shoots at you and Jihan Wu.
6. Jihan Wu uses his mystical chi powers (actually the combined exhaust from all of his mining rigs) to slow down the shotgun pellets, making them hit you as softly as petals drifting in the wind.
7. The bartender mutters some words, clothes ripping apart as he or she (hard to believe it could be a she but hey) turns into a bear, ready to maul you for cheating him or her of the payment for all the 100 drinks you ordered from him or her.

8. Steely-eyed, you stand in front of the bartender-turned-bear, daring him to touch you. You've watched Revenant, you know Leonardo di Caprio could survive a bear mauling, and if some posh actor can survive that, you know you can too. You make a pose. "Drunken troll logic attack!"
9. I think I got sidetracked here.

Lessons learned?

- Bears are bad news.
- You can't reasonably invoke "Satoshi's Vision" ***and*** simultaneously reject the Lightning Network because it's not onchain. Satoshi's Vision included a half-assed implementation of payment channels with `nSequence`, where the onchain transaction represented multiple logical payments, exactly what modern offchain techniques do (except modern offchain techniques actually work). `nSequence` (the field, but not its modern meaning) has been in Bitcoin since BitCoin For Windows Alpha 0.1.0. And its original intent was payment channels. You can't get nearer to Satoshi's Vision than being a field that Satoshi personally added to transactions on the very first public release of the BitCoin software, like srsly.
- Miners can totally bypass mempool rules. In fact, the reason why `nSequence` has been repurposed to indicate "optional" replace-by-fee is because miners are already incentivized by the `nSequence` system to always follow replace-by-fee anyway. I mean, what do you think those drinks you passed to Jihan Wu are, other than the fee you pay him to mine a specific version of your transaction?
- Satoshi made mistakes. The original design for `nSequence` is one of them. Today, we no longer use `nSequence` in this way. So diverging from Satoshi's original design is part and parcel of Bitcoin development, because over time, we learn new lessons that Satoshi never knew about. Satoshi was an important landmark in this technology. He will not be the last, or most important, that we will remember in the future: he will only be the first.

Spilman Channels

Incentive-compatible time-limited unidirectional channel; or, Satoshi's Vision, Fixed (if transaction malleability hadn't been a problem, that is).

Now, we know the bartender will turn into a bear and maul you if you try to cheat the payment channel, and now that we've revealed you're good friends with Jihan Wu, the bartender will no longer accept a payment channel scheme that lets one you cooperate with a miner to cheat the bartender.

Fortunately, Jeremy Spilman proposed a better way that would not let you cheat the bartender.

First, you and the bartender perform this ritual:

1. You get some funds and create a transaction that pays to a 2-of-2 multisig between you and the bartender. You ***don't*** broadcast this yet: you just sign it and get its txid.
2. You create another transaction that spends the above transaction. This transaction (the "backoff") has an `nLockTime` equal to the closing time of the bar, plus one block. You sign it and give this backoff transaction (but not the above transaction) to the bartender.
3. The bartender signs the backoff and gives it back to you. It is now valid since it's spending a 2-of-2 of you and the bartender, and both of you have signed the backoff transaction.
4. *Now* you broadcast the first transaction onchain. You and the bartender wait for it to be deeply confirmed, then you can start ordering.

The above is probably vaguely familiar to LN users. It's the funding process of payment channels! The first transaction, the one that pays to a 2-of-2 multisig, is the funding transaction that backs the payment channel funds.

So now you start ordering in this way:

1. For your first drink, you create a transaction spending the funding transaction output and sending the price of the drink to the bartender, with the rest returning to you.
2. You sign the transaction and pass it to the bartender, who serves your first drink.
3. For your succeeding drinks, you recreate the same transaction, adding the price of the new drink to the sum that goes to the bartender and reducing the money returned to you. You sign the transaction and give it to the bartender, who serves you your next drink.
4. At the end:
    - If the bar closing time is reached, the bartender signs the latest transaction, completing the needed 2-of-2 signatures and broadcasting this to the Bitcoin network. Since the backoff transaction is the closing time + 1, it can't get used at closing time.
    - If you decide you want to leave early because your liver is crying, you just tell the bartender to go ahead and close the channel (which the bartender can do at any time by just signing and broadcasting the latest transaction: the bartender won't do that because he or she is hoping you'll stay and drink more).
    - If you ended up just hanging around the bar and never ordering, then at closing time + 1 you broadcast the backoff transaction and get your funds back in full.

Now, even if you pass 50 drinks to Jihan Wu, you can't give him the first transaction (the one which pays for only one drink) and ask him to mine it: it's spending a 2-of-2

and the copy you have only contains your own signature. You need the bartender's signature to make it valid, but he or she sure as hell isn't going to cooperate in something that would lose him or her money, so a signature from the bartender validating old state where he or she gets paid less isn't going to happen.

So, problem solved, right? Right? Okay, let's try it. So you get your funds, put them in a funding tx, get the backoff tx, confirm the funding tx...

Once the funding transaction confirms deeply, the bartender laughs uproariously. He or she summons the bouncers, who surround you menacingly.

"I'm refusing service to you," the bartender says.

"Fine," you say. "I was leaving anyway;" You smirk. "I'll get back my money with the backoff transaction, and posting about your poor service on reddit so you get negative karma, so there!"

"Not so fast," the bartender says. His or her voice chills your bones. It looks like your exploitation of the Satoshi `nSequence` payment channel is still fresh in his or her mind. "Look at the txid of the funding transaction that got confirmed."

"What about it?" you ask nonchalantly, as you flip open your desktop computer and open a reputable blockchain explorer.

What you see shocks you.

"What the — the txid is different! You— you ***changed my signature***?? But how? I put the only copy of my private key in a sealed envelope in a cast-iron box inside a safe buried in the Gobi desert protected by a clan of nomads who have dedicated their lives and their childrens' lives to keeping my private key safe in perpetuity!"

"Didn't you know?" the bartender asks. "The components of the signature are just very large numbers. The sign of one of the signature components can be changed, from positive to negative, or negative to positive, and the signature will remain valid. Anyone can do that, even if they don't know the private key. But because Bitcoin includes the signatures in the transaction when it's generating the txid, this little change also changes the txid." He or she chuckles. "They say they'll fix it by *sep_arating the _sig* natures from the transaction body. They're saying that these kinds of signature malleability won't affect transaction ids anymore after they do this, but I bet I can get my good friend Jihan Wu to delay this 'SepSig' plan for a good while yet. Friendly guy, this Jihan Wu, it turns out all I had to do was slip him 51 drinks and he was willing to mine a tx with the signature signs flipped." His or her grin widens. "I'm afraid your backoff transaction won't work anymore, since it spends a txid that is not existent and will never be confirmed. So here's the deal. You pay me 99% of the funds in the funding transaction, in exchange for me signing the

transaction that spends with the txid that you see onchain. Refuse, and you lose 100% of the funds and every other HODLer, including me, benefits from the reduction in coin supply. Accept, and you get to keep 1%. I lose nothing if you refuse, so I won't care if you do, but consider the difference of getting zilch vs. getting 1% of your funds." His or her eyes glow. "GENUFLECT RIGHT NOW."

Lesson learned?

- Payback's a bitch.
- Transaction malleability is a bitchier bitch. It's why we needed to fix the bug in SegWit. Sure, MtGox claimed they were attacked this way because someone kept messing with their transaction signatures and thus they lost track of where their funds went, but really, the bigger impetus for fixing transaction malleability was to support payment channels.
- Yes, including the signatures in the hash that ultimately defines the txid was a mistake. Satoshi made a lot of those. So we're just reiterating the lesson "Satoshi was not an infinite being of infinite wisdom" here. Satoshi just gets a pass because of how ***awesome*** Bitcoin is.

CLTV-protected Spilman Channels

Using CLTV for the backoff branch.

This variation is simply Spilman channels, but with the backoff transaction replaced with a backoff branch in the SCRIPT you pay to. It only became possible after `OP_CHECKLOCKTIMEVERIFY` (CLTV) was enabled in 2015.

Now as we saw in the Spilman Channels discussion, transaction malleability means that any pre-signed offchain transaction can easily be invalidated by flipping the sign of the signature of the funding transaction while the funding transaction is not yet confirmed.

This can be avoided by simply putting any special requirements into an explicit branch of the Bitcoin SCRIPT. Now, the backoff branch is supposed to create a maximum lifetime for the payment channel, and prior to the introduction of `OP_CHECKLOCKTIMEVERIFY` this could only be done by having a pre-signed `nLockTime` transaction.

With CLTV, however, we can now make the branches explicit in the SCRIPT that the funding transaction pays to.

Instead of paying to a 2-of-2 in order to set up the funding transaction, you pay to a SCRIPT which is basically "2-of-2, OR this singlesig after a specified lock time".

With this, there is no backoff transaction that is pre-signed and which refers to a specific txid. Instead, you can create the backoff transaction later, using whatever txid the funding transaction ends up being confirmed under. Since the funding transaction is immutable once confirmed, it is no longer possible to change the txid afterwards.

Todd Micropayment Networks

The old hub-spoke model (that isn't how LN today actually works).

One of the more direct predecessors of the Lightning Network was the hub-spoke model discussed by Peter Todd. In this model, instead of payers directly having channels to payees, payers and payees connect to a central hub server. This allows any payer to pay any payee, using the same channel for every payee on the hub. Similarly, this allows any payee to receive from any payer, using the same channel.

Remember from the above Spilman example? When you open a channel to the bartender, you have to wait around for the funding tx to confirm. This will take an hour *at best*. Now consider that you have to make channels for everyone you want to pay to. That's not very scalable.

So the Todd hub-spoke model has a central "clearing house" that transport money from payers to payees. The "Moonbeam" project takes this model. Of course, this reveals to the hub who the payer and payee are, and thus the hub can potentially censor transactions. Generally, though, it was considered that a hub would more efficiently censor by just not maintaining a channel with the payer or payee that it wants to censor (since the money it owned in the channel would just be locked uselessly if the hub won't process payments to/from the censored user).

In any case, the ability of the central hub to monitor payments means that it can surveill the payer and payee, and then sell this private transactional data to third parties. This loss of privacy would be intolerable today.

Peter Todd also proposed that there might be multiple hubs that could transport funds to each other on behalf of their users, providing somewhat better privacy.

Another point of note is that at the time such networks were proposed, only unidirectional (Spilman) channels were available. Thus, while one could be a payer, or payee, you would have to use separate channels for your income versus for your spending. Worse, if you wanted to transfer money from your income channel to your spending channel, you had to close both and reshuffle the money between them, both onchain activities.

Poon-Dryja Lightning Network

Bidirectional two-participant channels.

The Poon-Dryja channel mechanism has two important properties:

- Bidirectional.
- No time limit.

Both the original Satoshi and the two Spilman variants are unidirectional: there is a payer and a payee, and if the payee wants to do a refund, or wants to pay for a different service or product the payer is providing, then they can't use the same unidirectional channel.

The Poon-Dryjam mechanism allows channels, however, to be bidirectional instead: you are not a payer or a payee on the channel, you can receive or send at any time as long as both you and the channel counterparty are online.

Further, unlike either of the Spilman variants, there is no time limit for the lifetime of a channel. Instead, you can keep the channel open for as long as you want.

Both properties, together, form a ***very powerful scaling property*** that I believe most people have not appreciated. With unidirectional channels, as mentioned before, if you both earn and spend over the same network of payment channels, you would have separate channels for earning and spending. You would then need to perform onchain operations to "reverse" the directions of your channels periodically. Secondly, since Spilman channels have a fixed lifetime, even if you never used either channel, you would have to periodically "refresh" it by closing it and reopening.

With bidirectional, indefinite-lifetime channels, you may instead open some channels when you first begin managing your own money, then close them only after your lawyers have executed your last will and testament on how the money in your channels get divided up to your heirs: that's just two onchain transactions in your entire lifetime. That is the potentially very powerful scaling property that bidirectional, indefinite-lifetime channels allow.

I won't discuss the transaction structure needed for Poon-Dryja bidirectional channels — it's complicated and you can easily get explanations with cute graphics elsewhere.

There ***is*** a weakness of Poon-Dryja that people tend to gloss over (because it was fixed very well by /u/RustyReddit):

- You have to store all the revocation keys of a channel. This implies you are storing 1 revocation key for every channel update, so if you perform millions of updates over your entire lifetime, you'd be storing several megabytes of keys, for only a single channel. /u/RustyReddit fixed this by requiring that the revocation keys be generated from a "Seed" revocation key, and every key is

> just the application of SHA256 on that key, repeatedly. For example, suppose I tell you that my first revocation key is SHA256(SHA256(seed)). You can store that in O(1) space. Then for the next revocation, I tell you SHA256(seed). From SHA256(key), you yourself can compute SHA256(SHA256(seed)) (i.e. the **previous** revocation key). So you can remember **just** the most recent revocation key, and from there you'd be able to compute *every* previous revocation key. When you start a channel, you perform SHA256 on your seed for several million times, then use the result as the first revocation key, removing one layer of SHA256 for every revocation key you need to generate. /u/RustyReddit not only came up with this, but also suggested an efficient O(log n) storage structure, the shachain, so that you can quickly look up any revocation key in the past in case of a breach. People no longer really talk about this O(n) revocation storage problem anymore because it was solved very very well by this mechanism.

Another thing I want to emphasize is that while the Lightning Network paper and many of the earlier presentations developed from the old Peter Todd hub-and-spoke model, the modern Lightning Network takes the logical conclusion of removing a strict separation between "hubs" and "spokes". Any node on the Lightning Network can very well work as a hub for any other node. Thus, while you might operate as "mostly a payer", "mostly a forwarding node", "mostly a payee", you still end up being at least partially a forwarding node ("hub") on the network, at least part of the time. This greatly reduces the problems of privacy inherent in having only a few hub nodes: forwarding nodes cannot get significantly useful data from the payments passing through them, because the distance between the payer and the payee can be so large that it would be likely that the ultimate payer and the ultimate payee could be anyone on the Lightning Network.

Lessons learned?

- We can decentralize if we try hard enough!
- "Hubs bad" can be made "hubs good" if everybody is a hub.
- Smart people can solve problems. It's kinda why they're smart.

Future

After LN, there's also the Decker-Wattenhofer Duplex Micropayment Channels (DMC). This post is long enough as-is, LOL. But for now, it uses a novel "decrementing `nSequence` channel", using the ***new*** relative-timelock semantics of `nSequence` (not the broken one originally by Satoshi). It actually uses multiple such "decrementing `nSequence`" constructs, terminating in a pair of Spilman channels, one in both directions (thus "duplex"). Maybe I'll discuss it some other time.

The realization that channel constructions could actually hold more channel constructions inside them (the way the Decker-Wattenhofer puts a pair of Spilman channels inside a series of "decrementing `nSequence` channels") lead to the further thought behind Burchert-Decker-Wattenhofer channel factories. Basically, you could host multiple two-participant channel constructs inside a larger multiparticipant "channel" construct (i.e. host multiple channels inside a factory).

Further, we have the Decker-Russell-Osuntokun or "eltoo" construction. I'd argue that this is " `nSequence` done right". I'll write more about this later, because this post is long enough.

Lessons learned?

- Bitcoin offchain scaling is more powerful than you ever thought.

Why God Loves Bitcoin

By Adam Paul Moore

Posted July 12, 2019

God hates theft.

If you love freedom and prosperity, I've got some bad news.

Governments and Central Banks been oppressing and stealing for many years. They have slowly sucked away your wealth and opportunity, while you weren't even paying attention. Ordinary folks like to blame Wall Street bankers for the problems of inequality in our society today. The truth is, the problem goes much deeper than them. The fault lies with Central Bankers and the politicians who enable them.

Before modern central banking, money was a fixed commodity. It was gold or silver. Un-counterfeitable, immutable, uncensorable. If you moved from one country to another, you could spend your gold or silver as you pleased. Although coins sometimes had someone's face on them, transactions were conducted by weight, and not by "face value." When gold and silver were the currency of the world, we had "sound money."

Sound Money is Good Money

What is sound money, anyway? It's rather simple. Sound money is money that you can trust. It's money that you can rely on. It's money about which you have a reasonable expectation that you can spend it in the future for what you paid for it.

Yes, you pay for money. You pay for it with your labor, goods, or services. You exchange any of these things for money in order to use it for goods and services in the future.

When scarce natural resources were used as money, things weren't perfect, but money was money. Period.

Something sinister happened to our money system. An ancient evil practice re-emerged called divers (think, "diverse" or different) weights and measures. In the ancient world, goods were bought and sold by weight of gold or silver. For instance, an ounce of gold for one cow, etc.

In the marketplace, unscrupulous merchants would have two sets of weights for measuring out goods and money. When they were balancing their false weight against your money, their special weight would be heavier to make the you add an extra bit to your payment.

Imagine if the grocer put his hand on the scale when he was weighing out your bananas at the supermarket, charging you more money than you really owe. That's what the Central Banks have done with our money.

Another underhanded practice in the ancient world was the practice of coin clipping. Each coin should contain a certain weight of metal which was to be standardized across the kingdom. When you spent one shekel you should have a reasonable expectation that it contains all the metal in the coin that's supposed to be there.

But banks and governments got sneaky.

They shaved the edges or clipped the coins to remove a small undetectable amount of metal from each coin they took in. They took that excess metal melted it down, and created new coins to be spent later. In effect, this created new money.

Once someone adds new money into an economy, the value of the current money has been diluted with the new. When a bank or merchant has additional money with which to purchase extra items over and above the original value of the money that they initial acquired, they are tipping the scales in their favor.

They are not operating on an even playing field. They are stealing and oppressing through fraud. One of the OT curses on the Israelites was that their "gold would be turned to dross." Unsound money is bad, so bad that wars have been fought over it.

Your fiat money is not fair money. It's filthy money.

Bitcoin is sound money. God loves sound money.

Since the monetary policy of Bitcoin is fixed and predictable, there is no theft. 21 million coins is all the Bitcoin there will ever be. If you want to opt-in to this money, you are more than welcome. Everyone is playing by the rules.

Because the the supply of coins cannot be manipulated or altered by bankers or governments, there is no possibility of being cheated by Bitcoin.

Bitcoin eliminates the "abomination" of "divers weights and measures," e.g. cheating — theft — fraud. Therefore, Bitcoin is good money.

Bitcoin is God's money.

For more about how Bitcoin is sound money, please read:

The Bitcoin Standard: https://amzn.to/2p0hsr9
Bitcoin Money: https://amzn.to/2RwtNRe
Inventing Bitcoin: https://amzn.to/2Xyi8H5

Tweetstorm: Bitcoin Miners Are Not Intermediaries

By Angela Walch

Posted July 18, 2019

These are reasons why people think #Bitcoin miners (including any of hashers, mining pool operators, cloud mining companies) are not intermediaries, from what I can tell. #crypto

What am I missing, and what do you think?

(1) miners don't know who the sender or recipient of a transaction is, so they can't discriminate amongst them other than based on the txn fee offered.

(2) the economic incentives built into the system deter miners from trying to cheat.

(3) a given miner only gets to censor or order txns in a block they actually win, so a particular miner only has power for a very short time.

(4) it is unknown which miner will actually win a particular block (hashpower only determines the odds of winning), so there is no particular, designated miner at the time a user proposes a transaction.

(5) miners perform purely ministerial tasks involving no discretion or judgement (just run code), so they are purely automata.

(6) there is not a *single central* miner that processes all txns (only have AN intermediary when there is ONLY one).

(7) related to the game theory, there an assumption that a majority of the miners/hashpower will follow the rules of the protocol and not attempt to exploit the system or its users.

(8) anyone can become a miner - there is no permission needed to begin or to stop.

(9) a miner can't include an invalid txn as full nodes won't approve.

(10) Please note that in compiling this list, I am not endorsing any of these stmts as true, nor am I putting forth any legal consequences that should/shouldn't follow.

And I am using the most basic, lay defn of 'intermediary'.

A middleman.

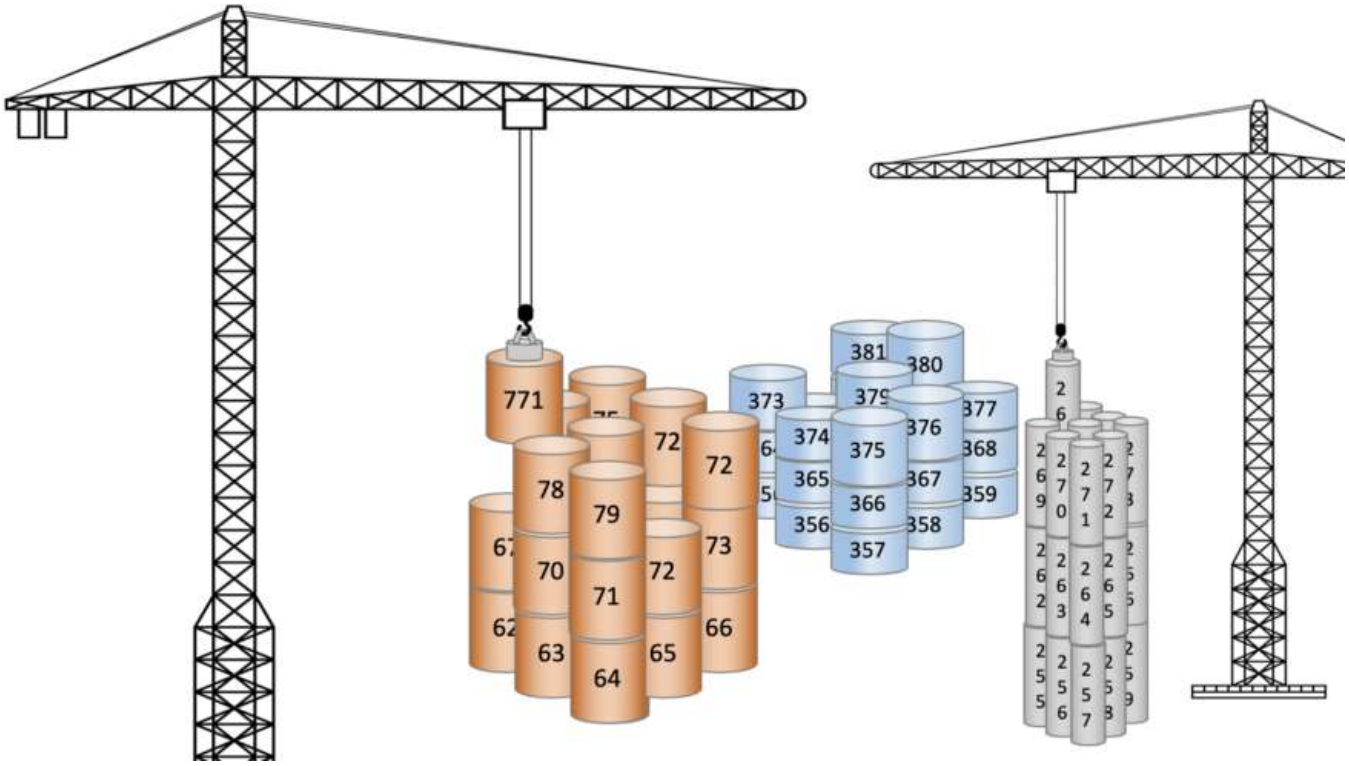
To be clear, I think most of these claims are actually not strictly accurate.

It's the settlement assurances, stupid

How to evaluate blockchains

By Nic Carter

Posted July 22, 2019



What is the time to finality on major blockchains? How long should I wait before considering a Bitcoin transaction settled? What are the risk factors which might cause me to demand additional confirmations? How do confirmations affect settlement?

Surprisingly, none of these questions have good answers, even in 2019, over 10 years after the first Bitcoin block was mined. Rigorous investigation into the properties of proof of work has been hampered both due to a perception that it's just a temporary staging ground for some future, superior consensus/sybil resistance mechanism, and due to a belief among Bitcoiners that its quality is inviolate.

But these questions are fundamental. If you believe that public blockchains with open validator sets and distributed convergence mechanisms will persist and mediate value transfer for the foreseeable future, they are worth pondering. And if you are an exchange and your livelihood depends on correctly assessing the number

of required confirmations on a variety of blockchains, these questions are critical. First, let me explain why I think settlement assurances are the primary thing worth contemplating about any public blockchain.

What's the interesting thing about Bitcoin?

This is a surprisingly difficult question to answer. Ask ten different Bitcoiners, and you'll get a dozen different responses. Disagreements about what what Bitcoin is for, its teleology, nearly tore the community asunder in the 2014–17 period. Hasu and I tried to chronicle these competing visions in a piece a while back. Others have noticed this and have covered it in detail. I particularly like Murad Mahmudov and Adam Taché's take. Daniel Krawisz covered the topic ably in 2014.

In Krawisz' piece, he posits that Bitcoin is understood very differently by two major tribes: the investors and the entrepreneurs. The investors, he posits, believe that Bitcoin is a new form of high-powered money which primarily upholds the sovereignty of the individual. The investors tend to believe that Bitcoin will catch on because of the innate strength of its monetary properties. For them, evangelism is pointless: price is the best evangelist. The 'entrepreneurs', as he dubs them, are more interested in Bitcoin as a global payments system, and emphasize its use in commerce. As anyone who paid attention in 2015–17 knows, these two sides fought a bitter civil war over Bitcoin's *telos*(purpose) with the block size being the main battleground.

Perhaps these views can be harmonized. I tend to believe that the interesting thing about Bitcoin is its capacity to facilitate the transfer of value through a communications medium with extremely strong assurances. (I made an effort to disentangle and evaluate those assurances here.) I think that Bitcoin is a novel institutional technology— high-assurance wealth storage and transfer *without* reliance on the State or a financial system — which will unlock new modes of human organization and will enable productive commerce in places where property rights are poorly enforced.

So if the assurances you get around settlement are the most interesting thing about the system, how can we evaluate them? And how do we make consistent comparisons between Bitcoin and other systems with open validation?

Evaluating settlement

So what are settlement assurances exactly? They refer to a system's ability to grant recipients confidence that an inbound transaction will not be reversed. Wire transfers using a messaging system like SWIFT are popular in part because they are practically impossible to reverse. They are considered safe for recipients because originating banks will only release the funds if they are fully present in the sender's account.

This is why the thieves behind the $1b Bangladesh bank robberyused SWIFT and bank wires; they wanted to leverage their settlement assurances. In other words, they chose to use a system for the theft which they knew would be hard to reverse. Ultimately, $61m from that heist remains unaccounted for. Far from being evidence of a failure of SWIFT + bank transfers, this demonstrates the system's strengths. Even in this case, where virtually everyone involved wanted to reverse the transaction, they could not. The system is resistant to rollbacks, discretion, and post-hoc edits. This doesn't make it a bad system. This makes it a system that gives counterparties a good deal of reassurance that a transaction will be final.

In a similar manner, Bitcoin is a useful system because it provides users powerful settlement assurances. Just *how* good, we don't know exactly. LaurentMT wrote probably the most scientific exploration in his excellent Gravity series. Generally though, the properties of Bitcoin's PoW have not been fully explored. It has suffered a few reorgs in its history, but, as far as we know, no deliberate, adversarial reorganizations where money was stolen. And we know that miners allocate a staggering amount of real-world resources into mining transactions. This means that recipients of a Bitcoin transaction can have extremely high confidence that, once buried under a few blocks, a transaction is unlikely to be reversed.

However, this isn't the case for many competing cryptocurrencies. While they look cosmetically similar to Bitcoin in many cases, none have the same settlement assurances. This isn't necessarily because of any design flaw, but simply because Bitcoin's block space has more accumulated costliness — and hence cost to attack — per unit time, and because Bitcoin is a near-monopolist on its hash function and has dedicated hardware. Somewhat surprisingly, many weaker chains haven't been exploited, even if the cost to do so has been low. This is likely to due to the fact that monetizing a 51% attack requires exploiting an exchange, which introduces additional complexities. And quite frankly, most smaller coins aren't worth much in the first place (and don't have any liquidity on the short side), capping the yield from an attack.

To get an idea of just how vulnerable many cryptocurrencies are, take a cursory look at crypto51.app. The methodology somewhat unrealistically assumes an attacker can rent sufficient hardware on Nicehash, but it still nicely depicts a lower bound of the cost to attack these systems.

So what are they key variables for evaluating settlement in a public blockchain system? Let's divide them into to the easily quantifiable ones and the harder-to-quantify variables.

Before we jump in, let's pause for a tiny literature review to credit some prior work in the space:

- For a much more succinct take on the matter, read Anthony Lusardi's Understanding (and Mitigating) Reorgs.
- For a comprehensive investigation into the qualities of Bitcoin's Proof of Work, see:Beyond the doomsday economics of "proof-of-work" in cryptocurrencies by Raphael Auer of the Bank for International Settlements
- For a fascinating implementation of a what a model incorporating some of these variables might look like, see A Lower Bound on Miner Rewards, by Kevin Lu of BKCM

Quantifiable settlement variables

Ledger costliness

Ledger costliness is the most profound and direct variable available to us to evaluate a blockchain's settlement guarantees. Put simply, it is equivalent to **the amount paid to validators/transaction selectors per unit of time**. In Bitcoin, miners receive a per-block subsidy and transaction fees as an incentive to stay honest and "play by the rules." In proof of work, miners attach an unforgeable proof that they have burned some energy and hence incurred a cost to each block proposed. At the time of winning a block, the miner necessarily has to have burned resources roughly equivalent to the value of the block (typically with a small margin), unless they are extraordinarily lucky. Because of this, miners are incentivized to create valid and rule-following blocks.

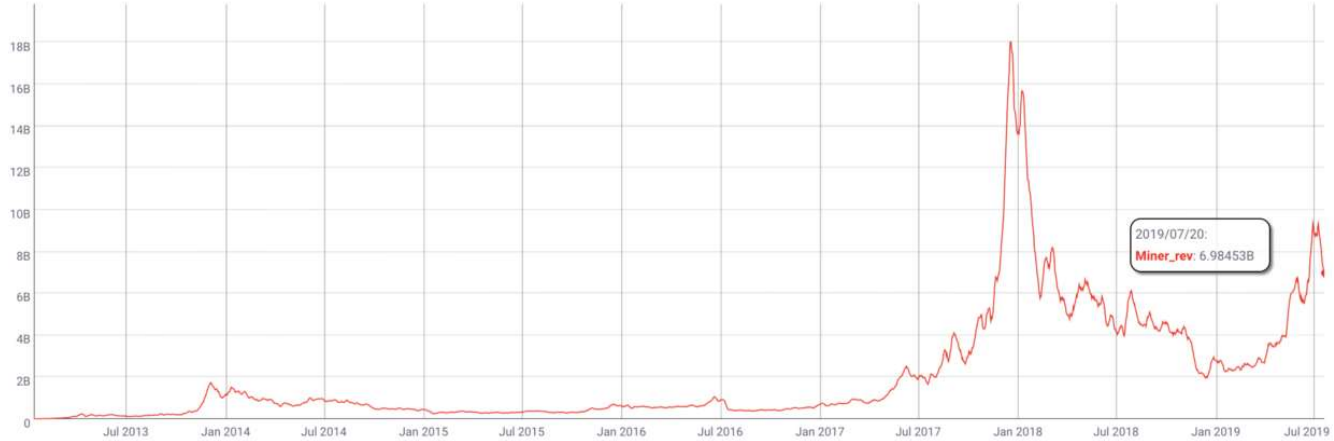
Think of it as a bit like a school project where you had to read a book and produce a book report. You need to prove to your teacher that you read the book, so you produce a book report (a valid block hash with a sufficient number of leading zeroes) which you could only have created if you actually read the book (computed sufficient hashes). Because your teacher is a stickler for style, you also have to format your book report correctly (produce a well-formed and valid block). It would be a tragedy to read the whole book, only to present a digest which is malformed and ends with you getting an F. Proof of work is the same: the work is upfront, with the payoff only coming later. You've incurred a real cost, and your business depends on you carrying out the final bureaucratic steps to collect your reward, so you do your best not to screw that part up. Recently, a miner did all the requisite work to be eligible for a block but fell at the last hurdle by creating an invalid block.

For a more complete description of how the PoW incentive works, read Hugo Nguyen's piece:

The Anatomy of Proof-of-Work Proof-of-Work (PoW) was originally invented as a measure against email spams. Only later it was adapted to be used in...bitcointechtalk.com

So why does more ledger costliness per unit time mean more security for transactors? Because a greater salary to miners (who are presumed honest) means you need a larger army of mercenaries to defeat them. These resources have to come from somewhere: you need to marshal resources and hardware capable of producing hashes, electricity, and so on. (There's an argument out there that since attackers collect the subsidy when 51% attacking, only fees provide security in PoW. I don't have the space here to engage with this fully here—for now I'll just maintain that the subsidy, especially with dedicated hardware, is itself an enormous cliff which must be scaled before 51% scenarios can be theorized.)

To sum up, outbidding the set of honest miners dutifully producing blocks on Bitcoin is very expensive. They collectively take a salary of **$6.9 billion dollars per year**right now, and many of them have presumably invested in their businesses in anticipation of future cashflows (meaning that the hardware active on the network might be even higher than current miner revenue would imply).



Annualized Bitcoin miner revenue, USD terms. Data: Coinmetrics.io

So Bitcoin is protected not only by the daily salary that the protocol pays its miners, but by the discounted rewards these miners expect to earn in the future. This means Bitcoin isn't just protected by the reality on the ground today, but miner *expectations* about rewards in the future.

We don't have an easy way to model expectations, so the easiest thing to do is to simply take the **miner salary per unit time and compare blockchains on that basis**. If you stopped reading this article now and just retained that one sentence, you would already have a better understanding of security than most people. Very few entities, even those for whom the stakes are very high like exchanges, bother benchmarking blockchains like this.

Usefully, Anthony Lusardi has already done some great expository work on the topic. He introduces the BitConf — demonstrating how many confirmations are required for one Bitcoin confirmation's worth of security on other blockchains, like Litecoin.

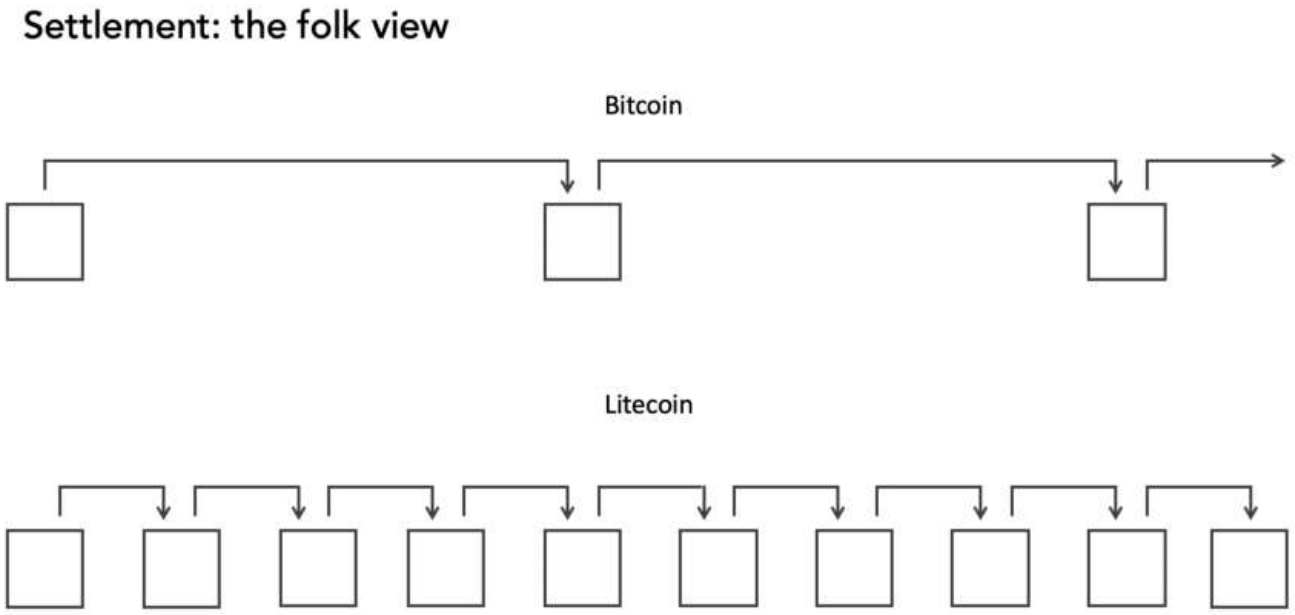
Your Exchange Needs More Confirmations: The BitConf Measure In cryptocurrency we regularly advise against accepting zero-conf transactions but are entirely happy to accept...medium.com

Suffice to say, most people do not use BitConfs, or try to index settlement to work done. Quite the contrary, the 'folk theory' of settlement holds that settlement is a linear function of the number of confirmations. This is sadly a very common view. Even the Litecoin Foundation website implicitly makes this claim:

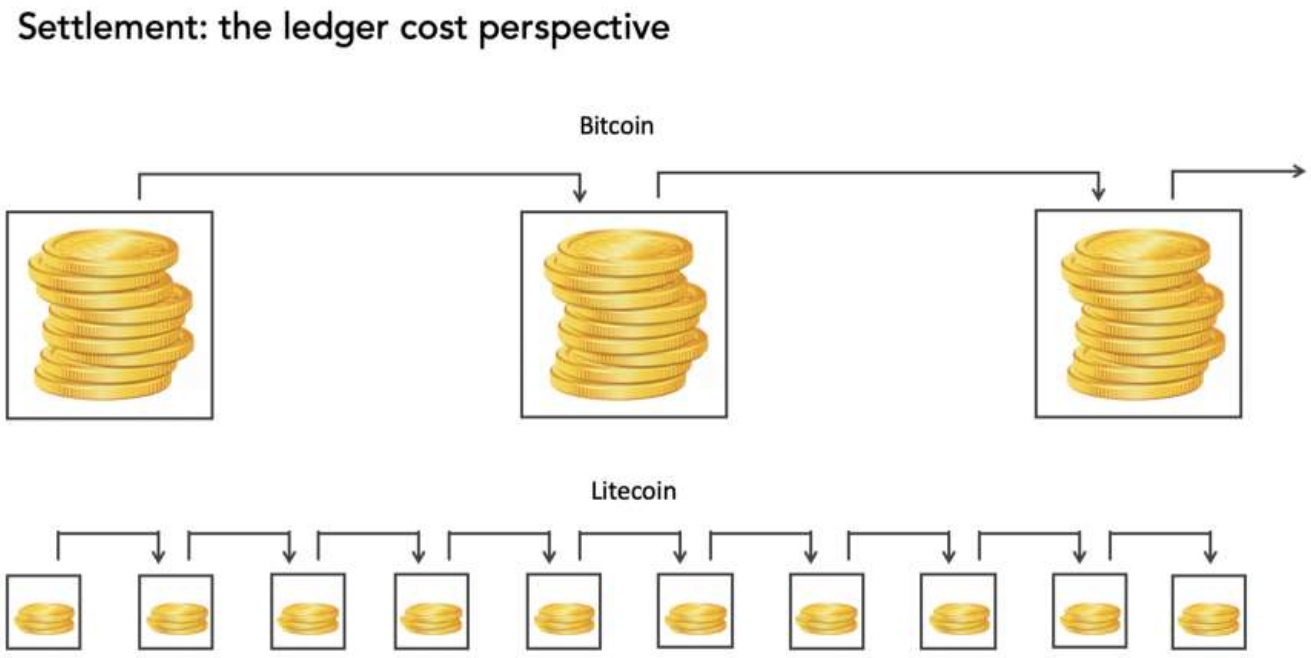
Litecoin transactions are confirmed faster than other cryptocurrencies like Bitcoin because it generates a block every 2.5 minutes as opposed to Bitcoin's 10 minutes. This means your money gets to its destination quicker.

The initial moment when a transaction is plucked out of the mempool and included in the chain is indeed reliably faster in Litecoin, but in cryptocurrency probabilistic settlement must be contemplated. In other words, if you only care about the first confirmation, then Litecoin is "faster", but the moment you start to care about longer term settlement (over multiple confirmations), it becomes clear that it is much slower.

If you believe that Litecoin and Bitcoin confirmations confer the same amount of settlement guarantees, then you might depict settlement as follows, with Bitcoin apparently slower:

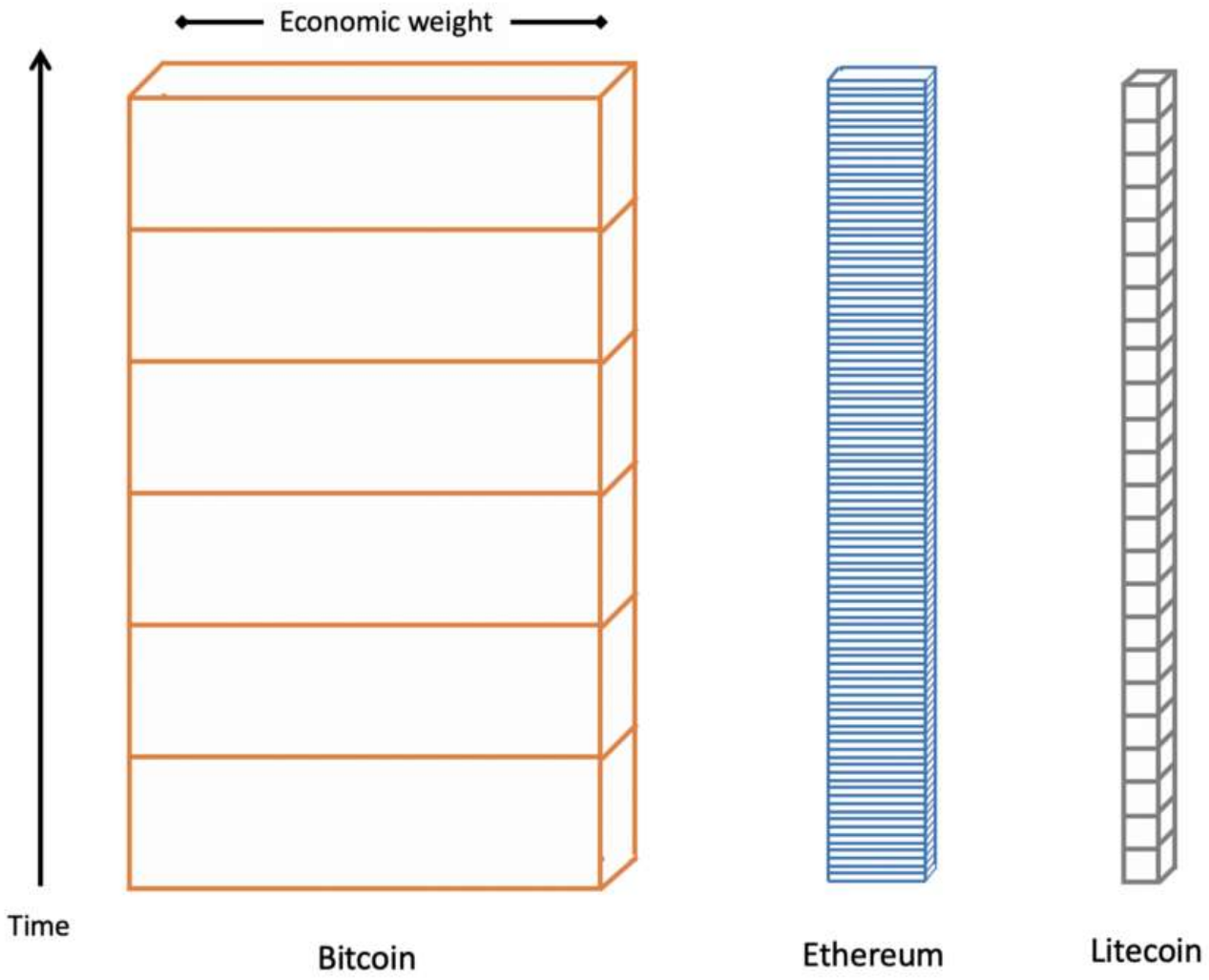


But this is mistaken. Litecoin has more blocks per unit of time, but it accumulates ledger costliness much more slowly. In reality, Bitcoin pays its private army of miners far better, and as a consequence, they produce far more security per minute in the form of hashes.



Bitcoin blocks are 'heavier' with accumulated cost than Litecoin blocks are. Even if Litecoin had a 10 minute block-time, a Bitcoin block would still be worth 14.5 times more than its Litecoin equivalent. Confirmations don't really matter. The opportunity cost incurred by miners per unit of time does.

You could alternatively visualize ledger costliness as blocks getting piled on top of their predecessors, with transactions getting more and more final as they are buried deeper and deeper in the pile of blocks.



Block width is roughly proportional to the relative security spend of each blockchain

As more and more blocks get added to the heap, it becomes more and more implausible that they would be reverted, and transactions become more final. In this graphic I've scaled the width of blocks to the relative ledger cost incurred, and depicted the granularity of blocks.

The point here is that settlement in a blockchain system is a flow. Block time is largely irrelevant. Ethereum has many more blocks per hour than Bitcoin does, but settlement should be compared between the two based on ledger cost, rather than number of confirmations.

Yield from reversal: transaction size

Ledger costliness isn't the only thing that matters in settlement. Also important is the incentive someone might have to try to reverse a transaction. The purest codification of this incentive is simply the size of the transaction. If you are a recipient of a 50,000 BTC transaction, you might wait more than the six block rule of thumb out of an abundance of caution. If you are receiving 1000 sats, one confirmation is likely sufficient. In short, transactions have more or less perceived settledness based on the stakes at hand.

Elaine Ou formalized this concept in a fantastic Bloomberg article, arguing that recipients should wait **until the transaction's value and ledger costliness match** to consider a transaction settled.

Elaine's formulation handily conjoins two of the most important quantitative variables in blockchain settlement: ledger cost and yield from reversal. If you wanted to settle a $10m inbound transaction in BTC, according to this rule, you'd wait 60 blocks, or 10 hours. (It's a neat coincidence that at a price of $13,330 Bitcoin accumulates ledger costliness at a rate of exactly $1m/hour). Henceforth, I'll refer to this simple formula as the **Ou Rule**.

Now that we have the two most critical settlement variables enumerated, let's put down some numbers and compare the major PoW networks.

	Daily miner revenue (7 dma)	Miner revenue per 10 mins	Days to settle $1m (Ou rule)	BTC finality multiplier
Bitcoin	$ 23,972,000	$ 166,472	0.04	1
Ethereum	$ 4,159,000	$ 28,882	0.24	5.8
Litecoin	$ 1,655,000	$ 11,493	0.60	14.5
Zcash	$ 718,734	$ 4,991	1.39	33.4
Bitcoin Cash	$ 711,419	$ 4,940	1.41	33.7
Bitcoin SV	$ 346,040	$ 2,403	2.89	69.3
Dash	$ 262,325	$ 1,822	3.81	91.4
Ethereum Classic	$ 188,818	$ 1,311	5.30	127.0
Monero	$ 179,670	$ 1,248	5.57	133.4
Bitcoin Gold	$ 49,087	$ 341	20.4	488.4
Dogecoin*	$ 48,396	$ 336	20.7	495.3
Verge	$ 13,800	$ 96	72.5	1,737.1
Vertcoin	$ 6,503	$ 45	153.8	3,686.3

* = Dogecoin is merge mined with Litecoin

Numbers as of 07/15/2019. Data: Coinmetrics.io

Needless to say, Bitcoin is by far the fastest-settling blockchain (just including these two variables and none of the other salient ones). Settling even a $1m inbound transaction can be extremely slow on many blockchains. Aside from Bitcoin, Ethereum, and Litecoin, it takes over a day for every other decentralized ledger (I'm not including Ripple and Stellar in these examples because they don't have meaningfully decentralized validation). Smaller chains simply do not have enough miner reward to make settlement suitably quick.

Luke Childs' Howmanyconfs offers a dynamically updated version of parts of this table:

How Many Confs? How many confirmations are equivalent to 6 Bitcoin confirmations? howmanyconfs.com

It's also worth calling attention to the fact that Bitcoin Cash and Bitcoin SV settle transactions 33 and 69 times more slowly than Bitcoin, respectively. While they are functionally identical to Bitcoin in most respects, because they offer miners less of a bounty, they are vastly slower. This directly contrasts with their common positioning as "faster" blockchains.

This is also an interesting case study in how Bitcoin resists duplication. You can create something which looks cosmetically similar to Bitcoin, but you cannot replicate the settlement assurances which derive from the costliness of the ledger. Miners obey economic reality and cannot be cajoled to lend their support to a protocol which doesn't pay them well enough. In fact, as we will learn, Bitcoin Cash and Bitcoin SV are even worse off that this table suggests, because of a third variable.

Monopolist on its own hash function

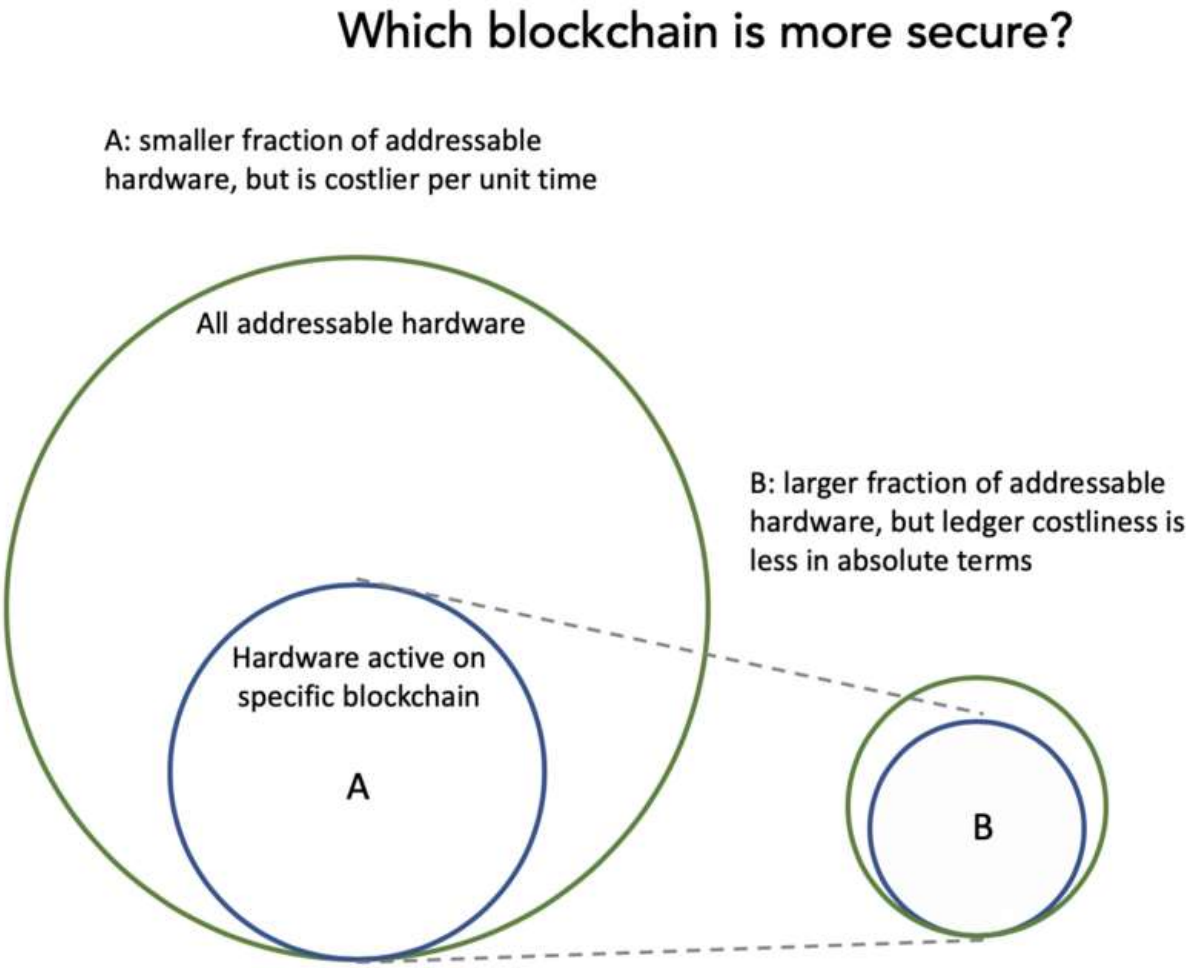
So far, I haven't mentioned a third critical variable which directly affects the settlement guarantees of a given blockchain: whether or not it holds an effective monopoly over the hardware which is addressable to its hash function. As I implied above, Bitcoin Cash and Bitcoin SV are at a massive disadvantage relative to Bitcoin because they have a minute fraction of all the SHA-256 ASICs. What this means is that even a mid-size or small pool mining Bitcoin could temporarily redirect its hashpower to one of Bitcoin's smaller forks and 51% attack it at will.

Relative share of miner revenue; BTC (orange), BCH (green), BSV (red). Coinmetrics.io

The fact that these blockchains have not been attacked yet is not evidence of their security. It may well be the case that there are no miners on Bitcoin willing to

maliciously interfere with either minority fork today — but depending on the goodwill of miners makes for an extremely tenuous security model. Since this risk is ever-present, it could be posited that neither blockchain ever reaches effective finality, regardless of the number of confirmations. This is because there are ample mining pools on Bitcoin which could create a 100+ deep reorganization in BSV for instance without too much difficulty.

This variable introduces more complexity into the analysis. It is not the case that more hashrate means that a blockchain is more secure; it must also occupy a large fraction of the addressable hardware.



In this example, I'd characterize blockchain A as less secure than B, even though it has more ledger costliness in absolute terms, because it is theoretically easier to marshal enough hardware to attack A.

So consider this variable to be a boolean; if the blockchain is a monopolist on its own hardware the analysis is straightforward. If it is in the unfortunate position of splitting

hardware with one or many other blockchains, and retains a minority share of that hash-function-specific hardware, it is likely fundamentally unsafe. But it's hard to determine just how unsafe it is; the risk of an attack is a function of the attackers ability to amass sufficient electricity and hardware.

Less quantifiable settlement variables

The three variables mentioned above aren't exhaustive, but simply the easiest to quantify. With those, you could probably build a plausible model which is superior than those used by many exchanges today. But there are many more factors to consider.

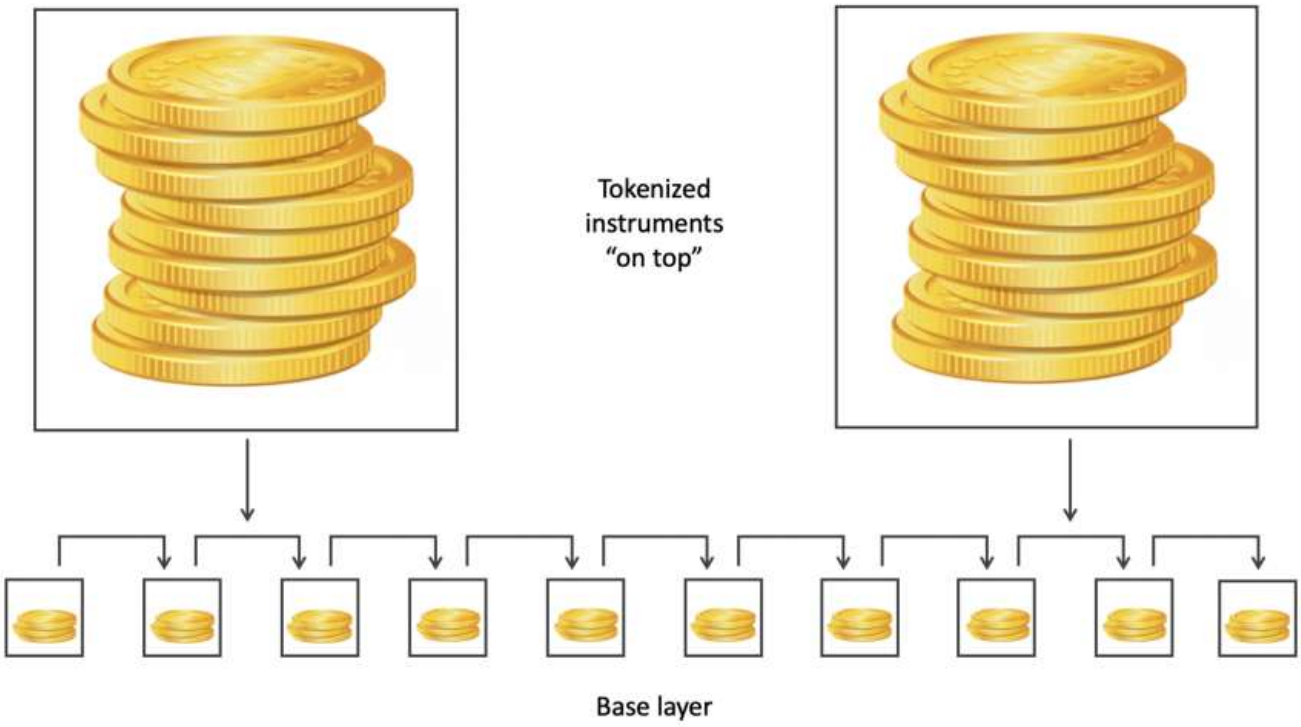
Yield from reversal: goldfinger attacks

Goldfinger attacks take their name from the Bond film in which the villain plans to irradiates all the gold in Fort Knox, making all of *his* gold more valuable. The term describes a class of attacks where the attacker is motivated by some extra-protocol financial interest. Joseph Bonneau more scientifically describes themas attacks where the "attackers [have] an extrinsic motivation to disrupt the consensus process."

The risk of these attacks is virtually impossible to quantify, since attackers have a variety of different motivations, and they tend not to disclose them *a priori* (before an attack). Here I'll give two further examples where the yield from reversal dramatically increases, rendering settlement guarantees less certain.

Top Heaviness

This refers to the condition in which a large number of financial significant assets are created as tokens *on top* of some base layer protocol — for instance Omni assets on Bitcoin or ERC20s on Ethereum. As these tokens inherit their security from and are wholly dependent on the base layer, they are vulnerable to attacks on the underlying chain.



As the asymmetry develops between the value of the instruments on top and the cost to attack the base layer, the top heaviness problem starts to manifest. If the asymmetry becomes large enough, an attacker might seek to take out a short on some instrument on the top layer and simultaneously attack the base layer, either by mining empty blocks and DOSing the tokens in question, or creating reorgs and confusion.

We have real world examples of the consequences of top-heavy systems. Attackers have recently made a habit of attacking the underlying index which sets the price for derivatives on Bitmex. Since there's a big asymmetry between the collateral present on Bitmex (the top) and the underlying reference market (the bottom), it's lucrative to burn funds market-selling on Bitstamp because the attacker can monetize by causing an outsize move on Bitmex as margin positions are liquidated.

I don't believe any blockchain faces this problem today, but as more instruments are tokenized and inserted on top of blockchains the returns from attacking the base layer will increase.

Liquid derivatives markets

This is rather straightforward. Derivatives, options in particular, give financial market participants the ability to obtain leverage and magnify their returns even relative to a small move in the underlying. As with the top heaviness condition, the risk to the

blockchain comes when a significant asymmetry exists between the cost to mount an attack and the returns from an attack.

The creation of liquid derivatives markets enables attackers to magnify their returns from predicting price action; and if they can induce a drop in the price of the asset by mounting an attack, the settlement guarantees of the chain are potentially at risk. As the return from an attack grows, so does the amount of resources that an attacker is willing to contribute to an attack. So the creation of leverage on the short side potentially impairs a blockchain's settlement assurances. But due to the heterogeneity of actors and uncertainty about the ability to monetize such an attack, it's impossible to quantify this risk and add an appropriate security discount.

Of course, one counterbalancing factor here is the potential unwillingness of an exchange to pay out on a successful bet if they suspect that the trader in question was coordinating with an attacker to interfere with the blockchain.

Additional hardware considerations

Implicit in the earlier point on hash function-specific hardware is the well-documented notion that GPU-mined coins *cannot ever* be monopolists on their hardware because there are so many GPUs in the world (thanks to gaming and other non-cryptocurrency applications). I won't belabor this point: David Vorick has cleanly laid out the case for why GPU-mined chains are fundamentally at risk, and why long term incentive-alignment (in the form of ASICs) is so critical.

Choosing ASICs for Sia We recently announced that we would be manufacturing and selling ASICs for Sia, an announcement that received a lot…blog.sia.tech

Thus GPU-mined coins should always be assessed additional confirmations. It's hard to know exactly what the ratio should be for one GPU-mined unit of ledger costliness to an ASIC-mined unit. But there absolutely should be a discount for GPU-produced security. It's simply too easy to acquire hardware to mine a GPU-mined chain.

Case study: Kraken's confirmation requirements

Startlingly, from my conversations with exchanges, who have a lot to lose from miscalibrated rules around settlement, it appears to me that they tend to give little thought to confirmation rules. I couldn't find much detail on how many inbound confirmations exchanges reserve until a transaction is considered settled. Helpfully, Kraken have made their criteria freely available.

I decided to benchmark Kraken's confirmation requirements against what a naive implementation of Lusardi's BitConf would look like — simply requiring that all chains provide the equivalent of six confirmations on Bitcoin.

	Block time (mins)	Kraken confs required	Bitcoin 6-conf equivalent confs	Kraken settlement time, mins	BTC equiv. single conf time, mins	Confs for $100,000 worth of security
Augur	0.22	30	173	6.5	346	160
Ethereum	0.22	30	173	6.5	346	160
Gnosis	0.22	30	173	6.5	346	160
Melon	0.22	30	173	6.5	346	160
Dash	2.50	6	548	15	5,483	220
Dogecoin	1.04	20	290	21	869	84
Ethereum Classic*	0.24	120	15,235	28	7,617	3,245
Litecoin	2.50	12	174	30	869	35
Monero	2.00	15	2,001	30	8,005	401
Tezos	1.03	30	5,230	31	10,461	1,013
QTUM	2.00	24	67,036	48	167,589	8,389
Bitcoin	10.00	6	6	60	60	0.6
Tether (Omni)	10.00	6	6	60	60	0.6
Zcash	2.50	24	800	60	2,001	80
Bitcoin cash	10.00	15	505	150	2,022	20

*Deposits are halted

Source: Kraken Deposit Processing Times, Coin Metrics estimates

The results are startling. Depending on how you put it, Kraken makes either extremely stringent demands of Bitcoin transactions, or extremely loose demands of non-Bitcoin chains. While Kraken asks for six Bitcoin confirmations to consider deposits settled, they ask a mere 12 of Litecoin (where the equivalent in Bitcoin security terms would be 174), 30 for Ethereum (Bitcoin equivalent: 173), and 15 for Monero (where Bitcoin-indexed security would demand 2000).

My guess is that six confirmations is massive overkill for Bitcoin, making Kraken's lesser settlement demands of other chains more reasonable. Still — when the ledger costliness variable is consistently applied, the results are occasionally comical. QTUM, for instance, if held to the same standard as Bitcoin, would need 67,000 confirmations, equivalent to a wait of 115 days. (QTUM may well have some alternative settlement mode I'm not familiar with: I computed the numbers simply based on the payouts it makes to validators).

Of course, this is a very naive implementation of the model. A more sophisticated version would include higher security demands for non-monopolist chains, GPU-mined coins, large inbound transactions, and so on. I would encourage exchanges like Kraken to consider a systematic ruleset for inbound transactions, if they don't already. Whatever the particular formula chosen, it would likely suggest fewer confirmations for Bitcoin and more for smaller chains.

Some takeaways

What's the practical significance of all this? Well as we continue to await the formalization of these variables into a model that makes sense and is directly applicable to everyday usage of cryptocurrency, here are a few takeaways:

I. Block time is arbitrary, and changes little

The only thing that a lower blocktime alters is reducing variance in the time to the initial confirmation. If you are impatient, you probably prefer a blockchain with a 2.5-

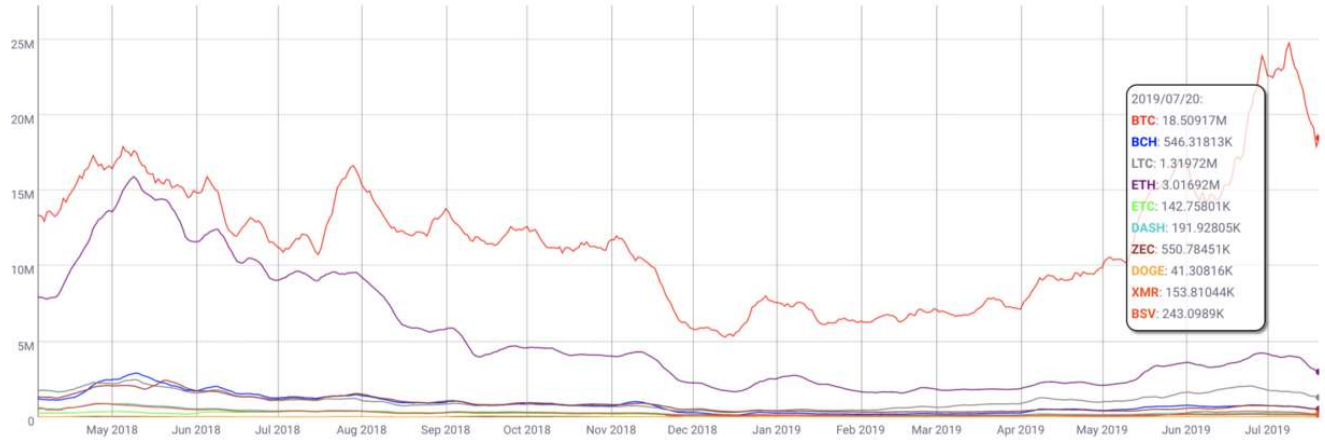
minute blocktime, but this doesn't mean that settlement is any "faster". Ledger costliness still accrues at the same rate, being a function of issuance and unit value per coin.

Indeed, Bitcoin could reduce its block size by 25% and switch to a 2.5 minute blocktime and virtually no one would notice the difference. The system would be functionally identical — the six block rule of thumb would become a 24 block rule of thumb. Satoshi opted for 10 minute blocks because he did not know how well the system would be able to come to convergence. Latency and large blocks interfere with validation, and make convergence among nodes more difficult. A healthy 10-minute blocktime gives the system plenty of breathing room — and also gives us an indication of what kind of a system Satoshi was envisioning (hint: not suited for in-person, petty cash payments).

It's true that the first confirmation matters some small amount, since your transaction cannot start to be buried under the weight of subsequent blocks until it is included in a mined block. Additionally, a lower blocktime reduces variance in variables like daily issuance. However, aside from that, blocktime is completely arbitrary. The security spend per unit of time, in addition to the *quality* of that ledger costliness, is what matters for settlement. A lower blocktime just means that you're chopping up that security flow into smaller bits. It doesn't make final settlement any faster.

II. Bitcoin is either providing massive security overkill, or other blockchains are critically at risk

This is the clearest takeaway from the various benchmarking exercises I did for this article. If you measure blockchains purely based on the salary paid to transaction selectors (miners and validators) per unit of time, for the most part, they look devastatingly weak compared to Bitcoin. Just have a look at this chart. Aside from Bitcoin, Ethereum, and Litecoin, virtually nothing is visible on the chart, because their security spend is so minimal.



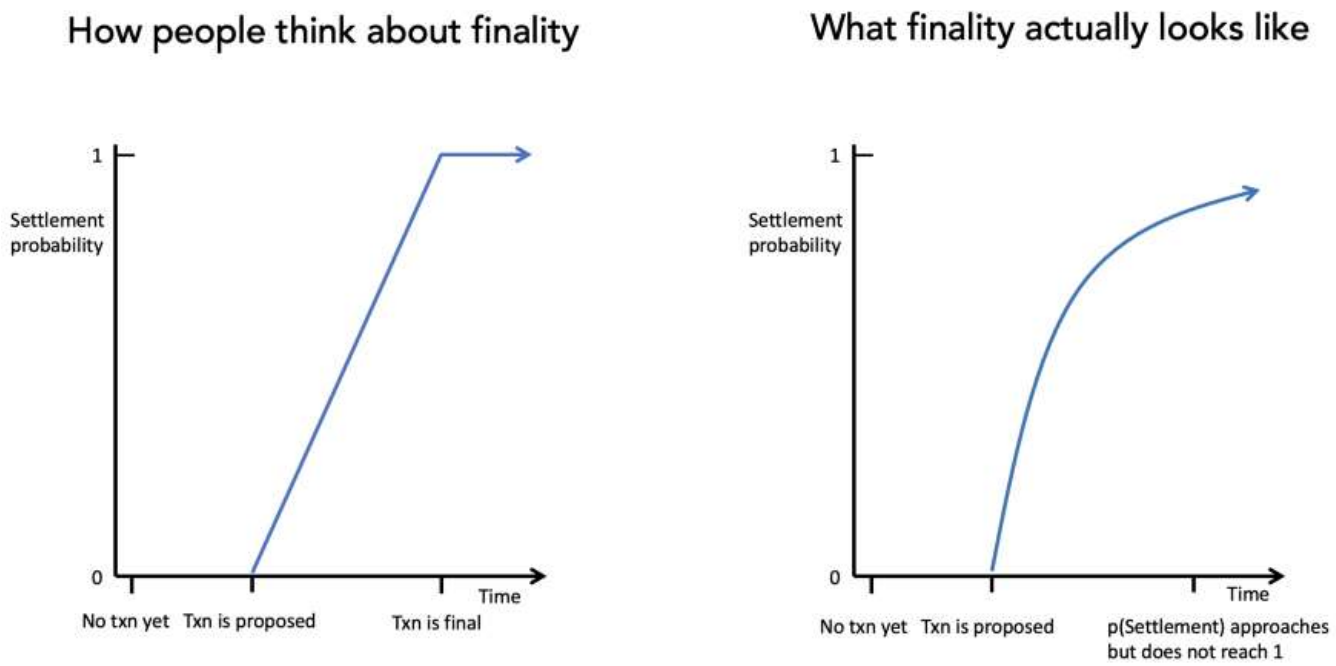
Daily USD miner revenue, smoothed (7dma). Coinmetrics.io

This isn't necessarily fatal. It could be the case that Bitcoin is way overpaying for security, for instance, and that proof of work is 'better' than we think. This is actually my current view — that due to the current subsidy conjoined with the high unit value of Bitcoin, Bitcoin is probably spending "too much" on security. But it does wrap the protocol in a warm blanket which gives it a good degree of protection as it enters its teenage years.

So this data is not necessarily apocalyptic for smaller blockchains. After all, even though Satoshi ordained the six-block rule of thumb, it could be the case that for most transactions 1 or 2 blocks are sufficient. This would lessen the heavy load placed on other blockchains trying to match Bitcoin's security spend.

III. Settlement is always probabilistic

I will admit that I chafe a little bit when new blockchains tout their 'absolute finality'. The only way to truly have finality is to have an organization vouch for transactions, effectively endorsing them. But when this happens, authorities that might have an interest in reversing transactions (say if they suspect they are related to criminal activity) will typically ask that entity to facilitate the rollback, poking a hole in the perceived finality.



Take the example of EOS. EOS has a concept called the Last Irreversible Block which, according to EOS Canada,

[M]eans that you can trust with 100% confidence that that transaction is final, fully confirmed, and immutable. If the block number of a block is lower than the Last Irreversible Block, that means it is considered final.

According to EOS Network Monitor, the current Last Irreversible Block is trailing the chaintip by 330 blocks, equivalent to about 2 minutes and 40 seconds. All together, this makes EOS' claimed time to finality very short.

Except there's a catch. EOS has (had?) a bureaucratic process through which individuals could appeal to the 'EOS Core Arbitration Forum' and ask for funds from suspected thefts to be frozen and returned to the victims, effectively reversing long-settled transactions. One batch of these reversals took place in June 2018. This was possible because there were only 21 entities (the block producers) tasked with processing transactions, and all were known to the leadership and hence accountable.

While many onlookers cheered the return of stolen funds, from a settlement perspective this undoes the qualities that transactors seek when they use a blockchain. In practice, any mechanism which can reverse settlement can be abused. The reason credit cards embed a fee into transactions is because chargeback fraud is rampant.

Imagine a sophisticated scam where someone sold EOS for fiat in a p2p transaction, and then appealed the transaction to the ECAF, and managed to get the EOS in the transaction returned to him under the guise of having been scammed. These are the kind of schemes that result from administrative exceptions to finality.

There are any number of examples I could give on this topic, but I'll stick with one for now. In practice, many of the blockchains that claim to have full and effective finality also insert the capacity to create discretionary rollbacks and account freezes into their systems. You still have to consider the probability of a reversal, even if it's not explicitly codified.

IV. By being open about its security model, Bitcoin's PoW is usefully transparent

Echoing Elaine Ou once again, one of the most useful features of Bitcoin's security model is how transparent and easily apprehensible it is. The precise guarantees are not easy to determine ("how many confs to settle $1b?") but the resources being spent to backstop the system are. At any point, an onlooker can trivially determine how many hashes, and by rough extension, how much energy, it would take to overpower the system. For years now, it has been clear that no entity outside the most potent state actors could muster sufficient resources to outweigh the honest majority.

By contrast, other blockchains seek security through obscurity, security through complexity, or through untransparent institutional modes of finality. Verge, for instance, conjoined five different hash functions in its exotic proof of work model, and that was ultimately its downfall. An attacker realized they could perform a 'time warp attack' by targeting just one of the hash functions and lowering difficulty to 1. Far from providing extra security, the insertion of more complexity into the system introduced new attack vectors.

Summing up

If there's anything I could have you take away from this piece, it's the following. Instead of viewing settlement as a function of some preconceived number of confirmations, think of settling a transaction in a proof of work system as the process of wood petrifying slowly. It happens at a given rate and can't be accelerated. The rate is determined by the variables enumerated above: chiefly, ledger costliness, transaction size, and the availability of addressable hardware. Once completed, the wood has been replaced by minerals and is rock solid, no longer soft and malleable. The features of the wood are forever frozen in time.

Similarly, as Nick Szabo has said, blockchains are computational amber. Amber starts life as tree sap, only later becoming hardened, in the process storing bits of

information (insect DNA and so on) within it. The essential process of burying past changes to the ledger under unforgeable cost, provided by proof of cost incurred, provides the same slow-moving settlement assurances. As more blocks accumulate, the gravity of the blockchain exerts itself, and makes distant rewrites colossally expensive and unwieldy.

The bounty available to miners — and hence the cost incurred — is a function of issuance, unit price, and fees. None of these aside from issuance can be directly programmed. And a high issuance alone cannot guarantee security, as investors have to buy into the chain's prospects and backstop its value. In this sense, strong settlement assurances in a proof of work system cannot be planned for, they can only emerge. Whether you find this to be a dismal conclusion or not is up to you.

In this article, I tried to enumerate the variables which I believe are most critical for evaluating the settlement assurances of blockchains, especially those built on proof of work. But you'll notice I provide no formal model nor a recommended solution to the problem. Many of these variables cannot be easily quantified and there are likely some which I am leaving out. A more comprehensive — or implementation-focused — model I will leave to subsequent authors.

If we ignore these questions, they will be forced upon us through necessity. As short-side liquidity emerges for a larger share of the market, whole new classes of attacks will open up and exchanges will find themselves targeted more and more. Equally, as major custodians and clearinghouses start to take cryptocurrency deposits totaling hundreds of millions or billions, they will need to devise formal rules for what constitutes settlement. They would do well to think deeply about the security of the blockchains that they are reliant on.

Thanks to Anthony Lusardi, Hugo Nguyen, and Matt Walsh.

Tweetstorm: On Bitcoin Paradigm Shifts

By Meltem Demirors

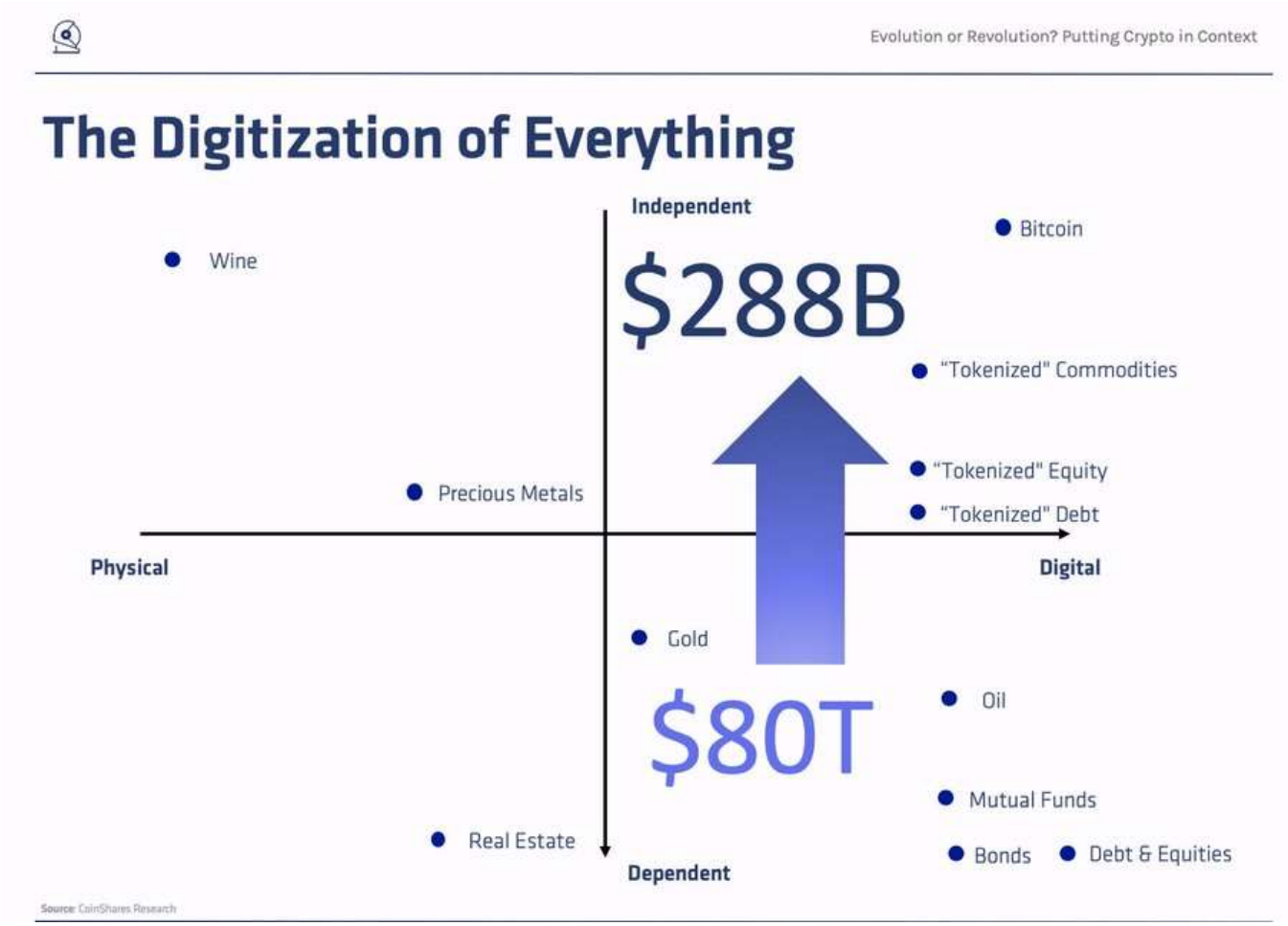
Posted july 23, 2019

1/ paradigm shifts seem to be a big topic these days.

there are two important ones happening right here and right now, which have been *proven* possible by bitcoin.

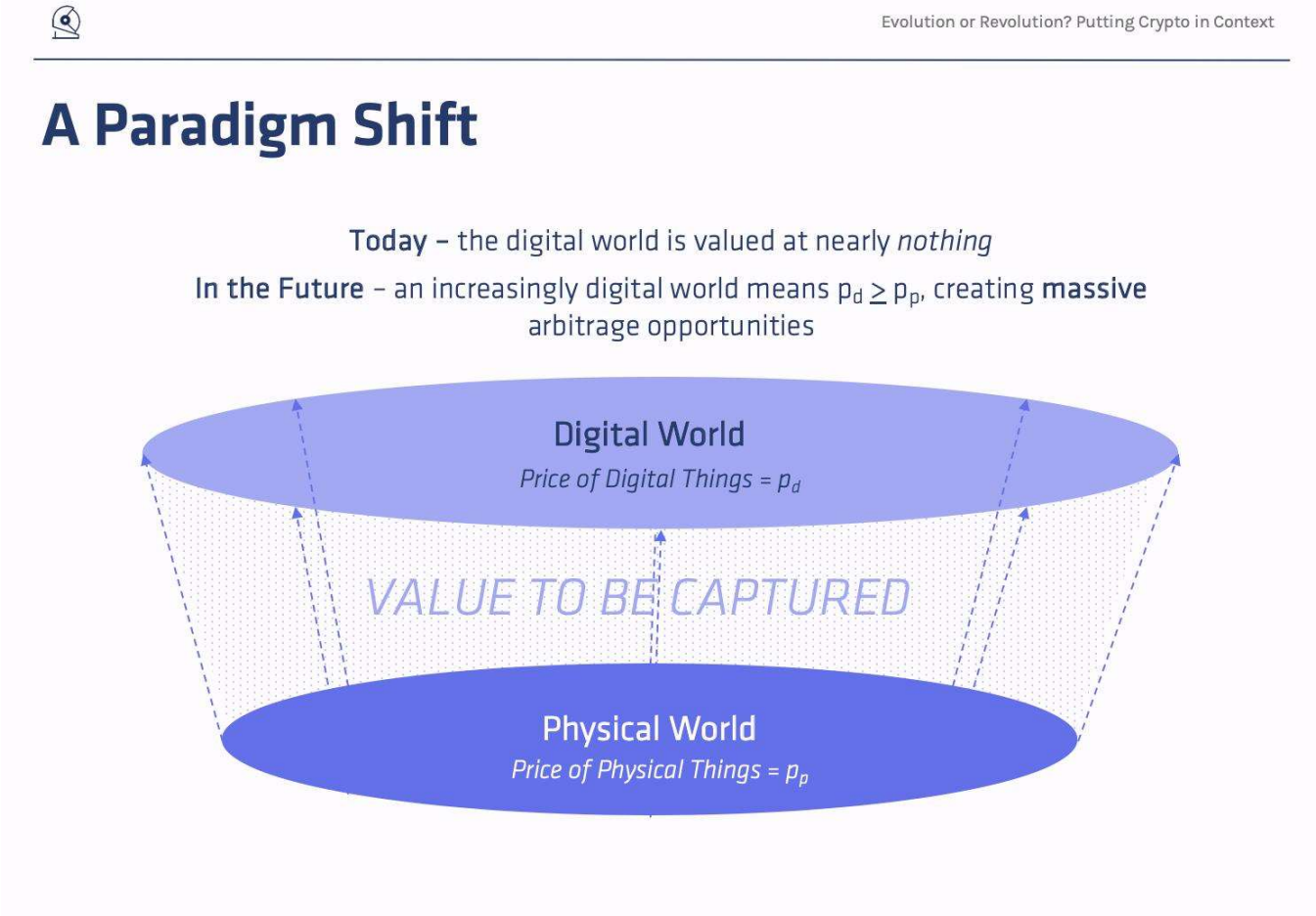
digitization and disintermediation.

a very short thread...



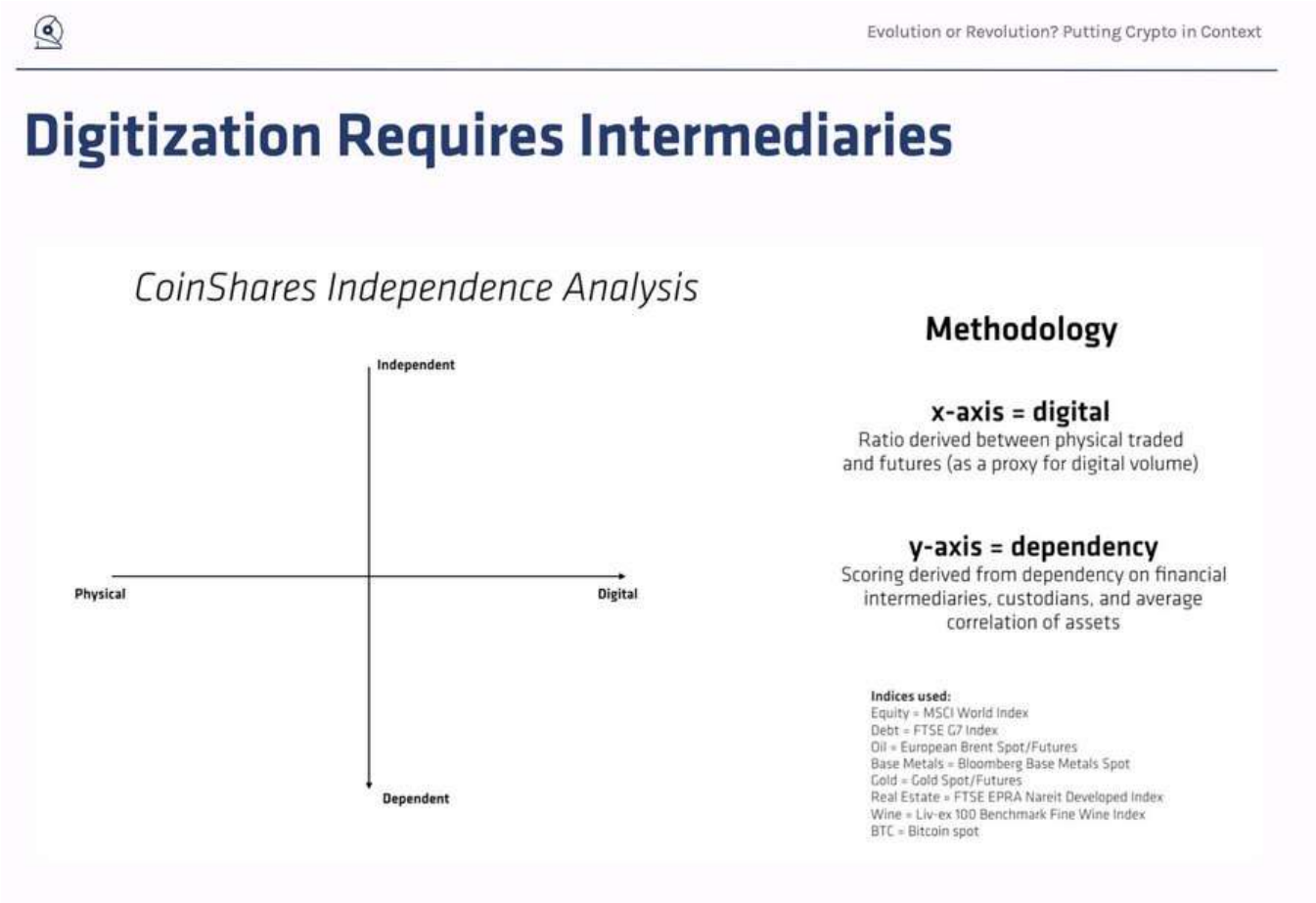
2/ today, the realm of digitally native assets is worth nearly nothing. digitization is largely taking existing (often physical) assets and transposing them to a new medium.

bitcoin is a digitally native asset that is backed by its own scarcity and the demand for it.



3/ historically, digitization requires *more* reliance on intermediaries, not less.

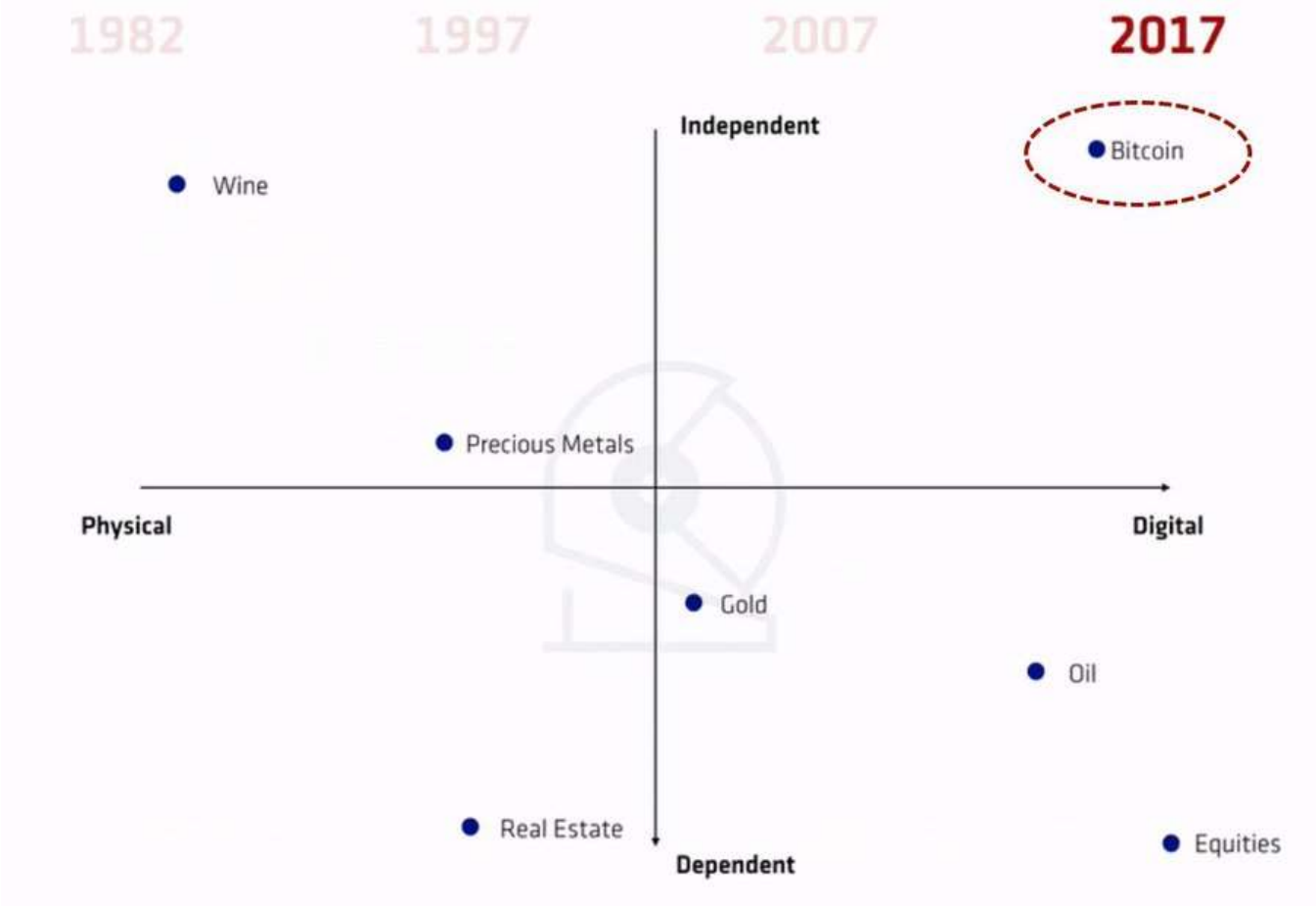
my colleague @RyanRadloff wrote a brilliant analysis on intermediaries and their role in digitization - medium.com/coinshares/bit...



4/ bitcoin breaks that trend. it requires no trust in an intermediary.

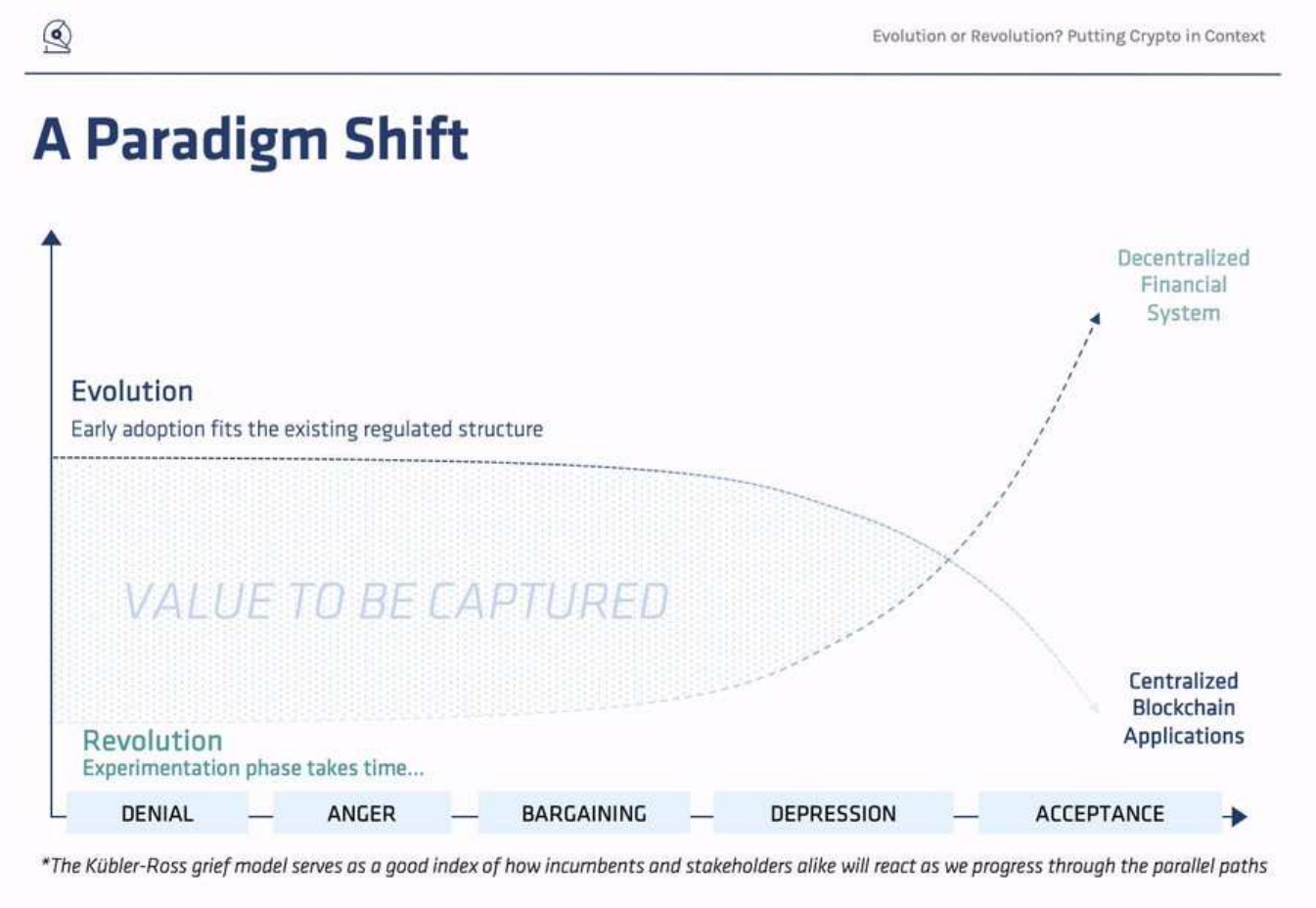
unlike most “digital” assets, bitcoin requires no intermediaries. some may *choose* intermediaries, but bitcoin requires no such thing.

it took me a long time to process how profound of a change that is.



5/ and that leads us to a second paradigm shift - disintermediation.

in the short term, people may opt to use intermediaries to access bitcoin (as they do today.) longer term, a new behavior will emerge - one that is a *revolution* and makes the asset independent.



6/ trust has long been the grease that drives the grinding gears of capitalism.

but trust in markets, in economies, in institutions - is at an all time low. and for good reason.

a world without trust necessitates a new model.

this @cryptograffiti piece 👇 captures it nicely:

7/ this new model doesn't materialize overnight.

our psychological anchoring keeps us rooted in the world of the physical, and the idea that intermediaries protect us from risk.

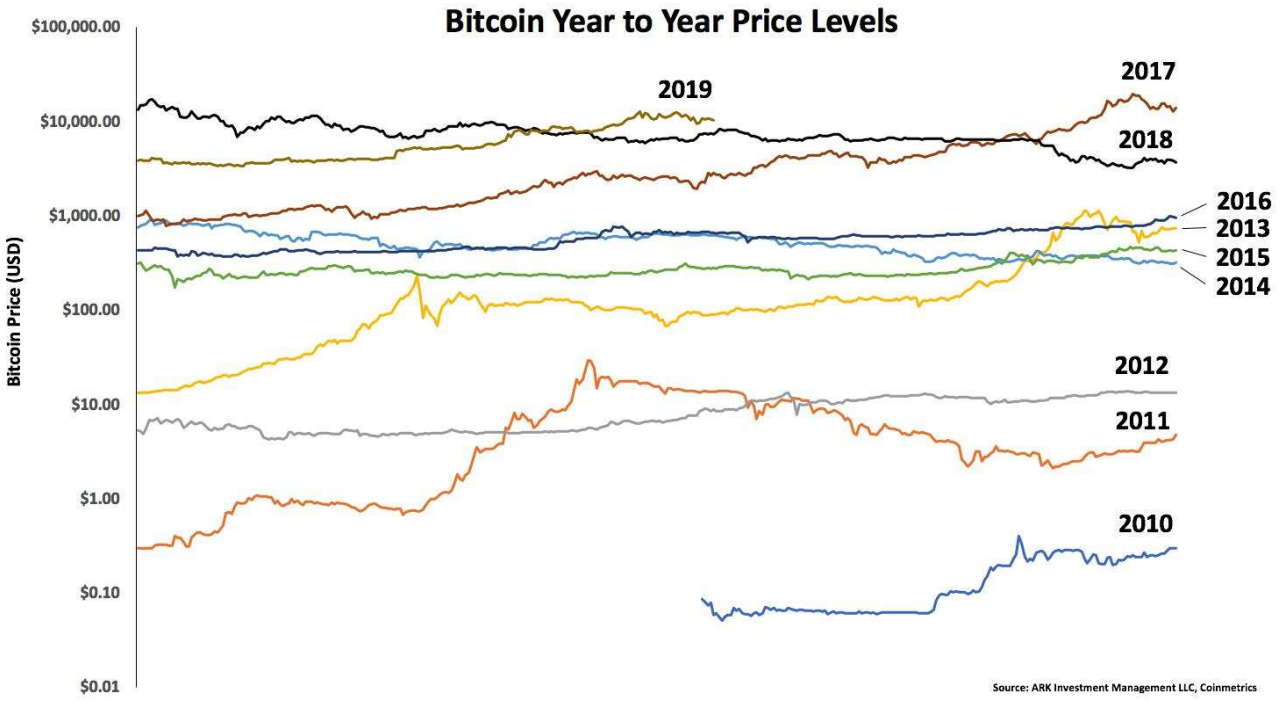
@eiaine captures this brilliantly. change is coming. slowly at first, then suddenly and at once.

Tweet: Bitcoin's year to year price level

By Yassine Elmandjra

Posted July 23, 2019

Five orders of magnitude later, a look at Bitcoin's year to year price levels.



Symmetrical and asymmetrical power

By Oleg Andreev

Posted July 23, 2019

Symmetrical power is defined by the risk being proportional to the potential gain. This automatically translates into “the bigger guy wins”. Example 1: security of the physical gold, which is easily confiscated by the state and is now largely held by central banks. Example 2: second amendment in US. Militia formed by armed citizens is going to lose against same-sized army professionally organized by the state.

Asymmetrical power is defined by the risk being significantly lower than the potential gain. Example 1: state-organized army. The generals and politicians bear virtually zero risk, while reaping all the gains. Example 2: Bitcoin. It is significantly cheaper for individuals to protect their bitcoins against large-scale confiscation, than to perform such attack.

It is easy to see that asymmetrical munitions will always win over symmetrical munitions.

There is an interesting difference between the armies and Bitcoin, though. Armies are asymmetrically powerful in the hands of their leaders at the large socialized expense: maintaining loyalty of the citizens who have to pay ever-growing taxes. Costs of running Bitcoin are measurable and adjusted by the market, without the use of coercion, voluntarily supported by the expanding entirety of the Bitcoin users (who pay for the inflation and fees).

Success of the army means expansion of the empire and further concentration of the power in the hands of the state. Success of Bitcoin means that wealth spreads further instead of being confiscated and concentrated, diminishing relative coercive power of every individual.

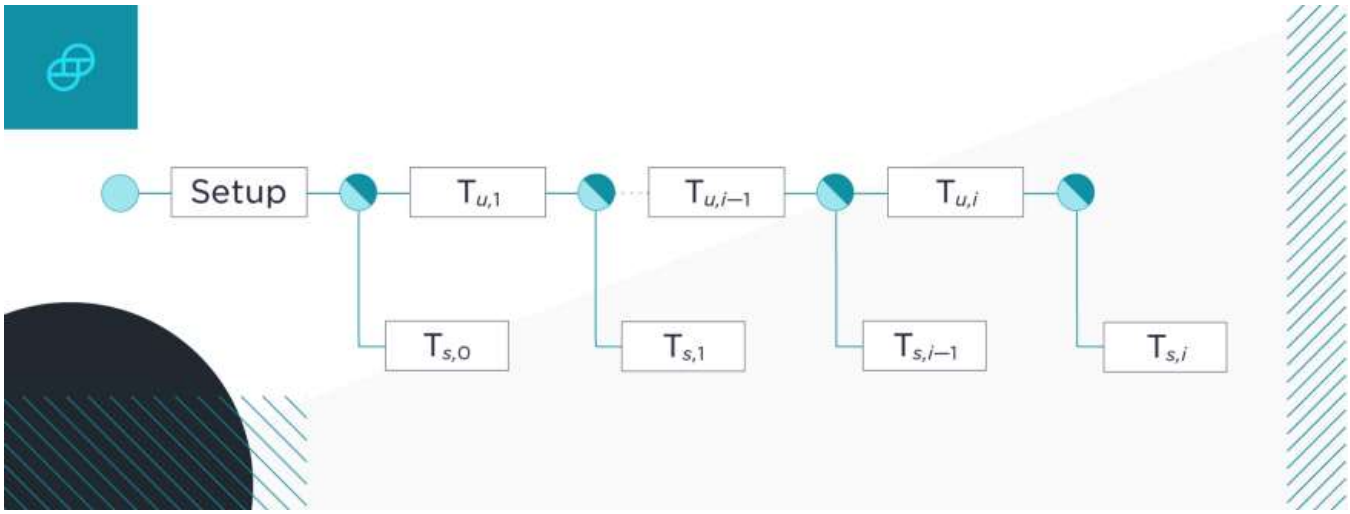
We can now formulate the crypto-anarchy conjecture:

1. The traditional political process is application of symmetric power and will not scale down empires.
2. Second amendment and militia are also symmetrically powerful and will not protect people from empires.
3. Empire’s asymmetrical power towards its population expands until it destroys the economy it feeds on.
4. Bitcoin being asymmetrically secure is better than any other known tool in protecting individual’s wealth.
5. Dynamic of the (4) vs (3) means that Bitcoin may cause the state run out of money before the economy is destroyed.

Breaking Down the Bitcoin Lightning Network: eltoo

By Brandon Arvanaghi

Posted July 25, 2019



The Lightning Network is a Layer 2 solution that allows you to create micropayment channels with other Bitcoiners. It allows instant and trustless peer-to-peer transacting while limiting the amount of data needed on-chain.

In this post, I break down exactly how it works, as well as a newly proposed update protocol within it called ***eltoo*** (named after *L2*).

Unidirectional Channels

Unidirectional payment channels are the simplest to implement in the Lightning Network because money only flows in one direction. The most common use case is streaming money; for example, a micropayment for each minute of a video you watch.

Say you want to start such a channel with Netflix. First, you create a **funding transaction**, which is you locking up a certain amount of your money that you are willing to pay to Netflix (but have not yet paid them).

Say you fund this transaction with 10 Bitcoin and publish it on the Bitcoin blockchain. After being mined, this funding transaction can be spent by a 2-of-2 multisig consisting of your's and Netflix's keys.

As Netflix starts streaming you bytes of video, you start streaming them money — say .000001 Bitcoin per minute of video — via partially signed transactions that spend this funding transaction.

Using the funding transaction as input, you create two new outputs: one sending .000001 to Netflix, and the other 9.999999 to you. You sign this transaction and share it with Netflix off-chain (that is, without attempting to publish it to the Bitcoin blockchain). This transaction is considered "partially signed" because it only contains one of the two signatures necessary to spend.

When Netflix receives this partially-signed transaction, they are in control. Netflix can choose to claim that .000001 Bitcoin immediately, and in the process send the remaining 9.999999 Bitcoin back to you, by adding their signature to the partially signed transaction and publishing it. This is considered *closing the channel* or a *settlement*.

Instead, Netflix will continue streaming you video so long as you keep providing larger partially signed transactions every minute. After another minute, you send Netflix another partially signed transaction using the same funding transaction as the input. This new partially signed transaction would send .000002 Bitcoin to Netflix (to reflect the two minutes of watch time), and 9.999998 Bitcoin to you. You keep doing this every minute.

With unidirectional payment channels, there's no possibility of cheating. If you stop sending Netflix partially signed transactions every minute for higher amounts each time, Netflix will stop streaming you video. They will sign the most recent partially signed transaction you sent them (which entitles them to the most Bitcoin), publish it, and thus close the channel.

Furthermore, there's no risk of anyone publishing an "outdated" transaction. Netflix is the only one capable of spending any of the partially signed transactions (since Netflix has your signatures, but you don't have any of theirs), and every newer partially signed transaction you send Netflix is strictly better for them than any older one. Netflix can only cheat *itself* by publishing an earlier transaction.

When money flows in both directions, this gets trickier. Both parties can publish transactions, so incentives exist to publish an outdated transaction.

The Problem with Bidirectional Channels

Say Alice and Bob open up a payment channel and each lock up .5 Bitcoin in the funding transaction. Now, Alice agrees to pay Bob .1 BTC for a carwash. She sends Bob a partially signed transaction that uses the funding transaction as its input with two outputs: one that sends .4 BTC to her, and one that sends .6 BTC for Bob.

By not publishing this transaction, Bob keeps their channel open. He later agrees to pay Alice .3 BTC for a painting.

If Bob sends Alice a partially signed transaction that uses the funding transaction as its input, they will each be in possession of a different, yet valid, spend of the same funding transaction. Transactions have no expiration date in Bitcoin, so their transactions will be valid forever.

It doesn't matter if they keep sending partially signed transactions back and forth for other goods and services. Either of them can act maliciously by publishing any earlier transaction that entitled them to more Bitcoin, thereby closing the channel, and making all other signed transactions invalid.

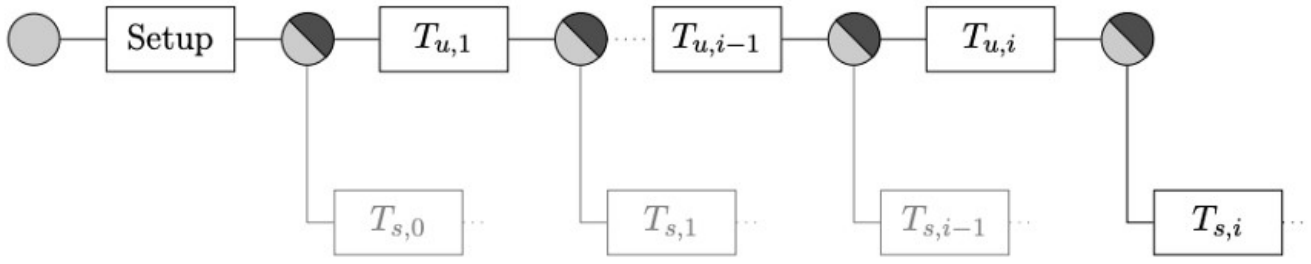
Bidirectional channels need a way to *invalidate outdated transactions* so that only the *most recent signed transaction* can be used to close the channel. That's where *eltoo* comes in.

eltoo

Bidirectional payment channels in the Lightning Network work out-of-the-box today because the whitepaper created a working protocol to invalidate outdated transactions. This protocol, named *LN-Penalty*, penalizes participants who try to publish outdated transactions by allowing the other party to steal the cheating party's Bitcoin.

Though LN-Penalty works today, it has problems. Besides its complexity, edge cases exist where it risks accidentally penalizing an honest user. *eltoo* is not yet usable because it relies on a proposed signature scheme ***SIGHASH_NOINPUT*** which has yet to be adopted, but because it is not penalty-based, there's no risk of losing your funds.

In eltoo, the two parties create the funding transaction denoted by **Setup** in the diagram below. The funding transaction could contain Bitcoin from both parties, because we anticipate money flowing in both directions.



Each circle represents a transaction output. Diagram from the eltoo whitepaper.

Before signing the funding transaction, Alice and Bob first sign a *settlement transaction*(**Ts,0** in the above diagram) which refunds the Bitcoin in the funding transaction to each appropriate party. In eltoo, the term "settlement transaction"

describes any transaction that distributes funds back to the participants, rather than to a multisig output that they both control.

After they sign the first settlement transaction, the parties can safely sign the funding transaction. The locking script for the funding transaction looks as follows:

```
OP_IF
  10 OP_CSV
  2 A_{s,i} B_{s,i} 2 OP_CHECKMULTISIGVERIFY
OP_ELSE
  <S_i + 1> OP_CHECKLOCKTIMEVERIFY
  2 A_u B_u 2 OP_CHECKMULTISIGVERIFY
OP_ENDIF
```

Locking script for the funding transaction, and any other update transaction. Image from the eltoo whitepaper.

There are two ways to spend the funding transaction: one in the *IF* branch, and one in the *ELSE* branch. These two branches rely on two separate sets of keys: the *IF_branch requires _settlement keys*, and the *ELSE* branch requires *update keys*. The two parties, Alice and Bob, each control one key from both sets of keys.

You'll notice that the settlement branch of this locking script contains **10 OP_CSV** (short for ***OP_CHECKSEQUENCEVERIFY***) as its first instruction. Any transaction attempting to spend this funding transaction by unlocking the *IF* branch can only do so if 10 blocks have passed from when the funding transaction entered the blockchain. If Alice and Bob exchanged signatures for the settlement transaction, then published the funding transaction to the Bitcoin blockchain, then published that settlement transaction, it would take 10 blocks before their settlement transaction could be mined to give them control of their respective funds.

Instead of publishing the settlement transaction, Alice and Bob keep the channel open. Say Alice wants to send 1 Bitcoin to Bob, so their new balances are 4 Bitcoin for Alice, and 6 Bitcoin for Bob.

The first thing Alice and Bob do is exchange signatures for a *new* settlement transaction. This new settlement transaction will pay 4 Bitcoin to an address only Alice controls, and 6 Bitcoin to an address only Bob controls.

Here's the key point of eltoo: this new settlement transaction does not spend from the same funding transaction. Instead, it spends the output of a transaction Alice and Bob have yet to make: an *update transaction*.

An update transaction's purpose is effectively to double-spend the funding transaction, so that the original settlement transaction (that Alice and Bob both signed, which had a block delay of 10 blocks), becomes unusable.

Recall the locking script of the funding transaction:

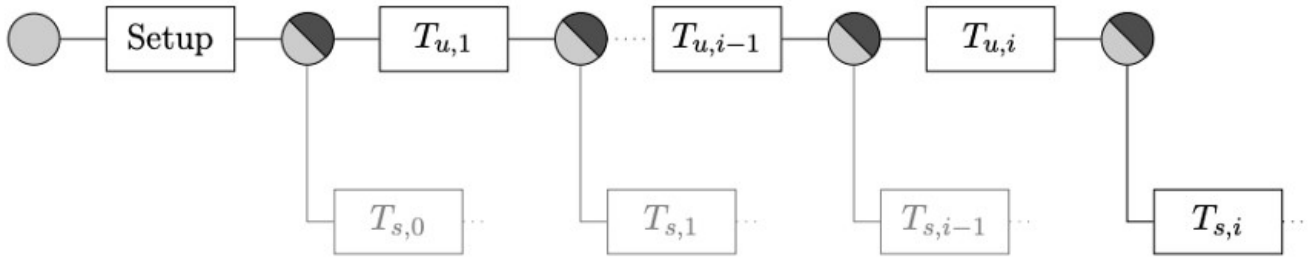
```
OP_IF
   10 OP_CSV
   2 A_{s,i} B_{s,i} 2 OP_CHECKMULTISIGVERIFY
OP_ELSE
   <S_i + 1> OP_CHECKLOCKTIMEVERIFY
   2 A_u B_u 2 OP_CHECKMULTISIGVERIFY
OP_ENDIF
```

The locking script from the funding transaction

While the settlement branch has a 10 block delay, the *update* branch does not. If Alice and Bob ever exchanged signatures from their respective *update keys*, they could spend the funding transaction by unlocking its update branch well before the settlement transaction they signed ever could.

After Alice and Bob sign the new settlement transaction that sends 4 Bitcoin to Alice and 6 to Bob with their settlement keys, they exchange signatures from their update keys to create the update transaction. With that, the old settlement transaction that refunded their initial balances becomes irrelevant, and the new settlement transaction — which spends the update transaction — is the only one that can issue payouts.

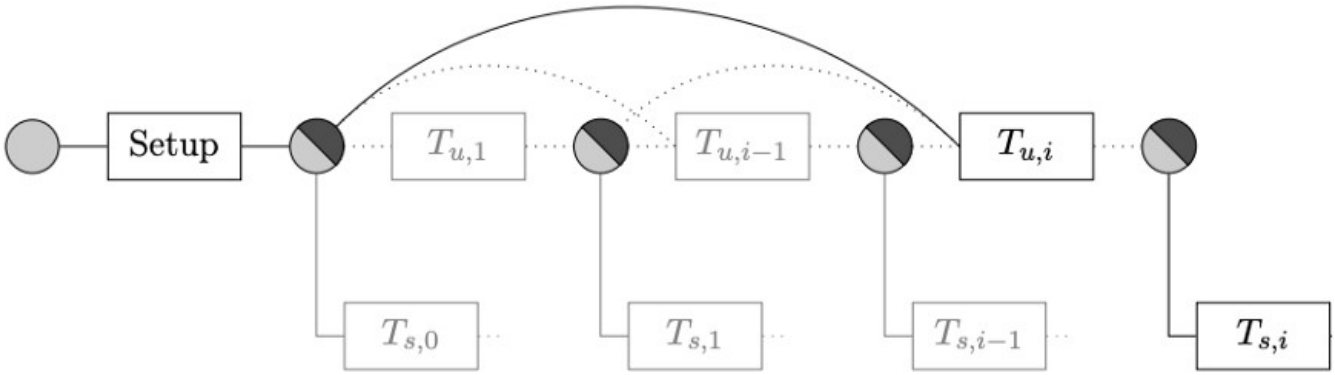
This process of creating update transactions and settlement transactions can continue like this indefinitely, as the image from earlier showed. The most recent settlement transaction ***Ts,i*** is the only one that matters, because Alice and Bob have signed a chain of immediately-publishable update transactions that guarantee none of the earlier settlement transactions could take effect.



Each circle represents a transaction output. Diagram from the eltoo whitepaper.

You'll notice that while this proposed model works, it requires every intermediary update transaction to be published on-chain. This defeats the purpose of the Lightning Network, which transacts off-chain to keep on-chain data light.

That's where ***SIGHASH_NOINPUT*** comes in. Instead of having to publish the entire sequence of update transactions all the way to your most recent settlement transaction, ***SIGHASH_NOINPUT*** allows you to skip over all update transactions until the one you need.



SIGHASH_NOINPUT allows "binding" to any earlier transaction.

Though an output's locking script can dictate that a *specific set of keys* must provide a signature to spend it, it does not dictate *what that signature must contain*. Usually, you sign every input and output in your transaction, and inform Bitcoin nodes that you have done this by appending the ***SIGHASH_ALL*** flag next to your signature. This means that you are announcing to every Bitcoin node that your transaction should only be considered valid if the specific combination of inputs and outputs contained in your signature are present in your transaction. If any other combination — a different input, an output with a slightly different value, etc. — appeared than what you signed, you are telling Bitcoin nodes to consider your transaction invalid.

With ***SIGHASH_NOINPUT***, you can instead create a "free floating" transaction. You are announcing to Bitcoin nodes examining your transaction that you *don't care what the input* to your transaction is — you only care about the output. That means that your signature will be valid on *any unspent output* that required those specific keys to spend. You don't care *which* unspent output you're spending — you're OK with spending any of them.

As in the diagram above, using the ***SIGHASH_NOINPUT*** flag allows us to bind the last update transaction to the funding transaction. The last update transaction has already been signed, and though it initially pointed its input to spend the update transaction just before it, we can change which unspent output it spends without making the signature invalid because we explicitly state that the input is not part of

or relevant to our signatures. All other intermediate update transactions can safely be skipped.

Thus, only three transactions must be published by the end of the channel: the funding transaction, the last update transaction, and the last settlement transaction which distributes the final balances to each party by spending that last update transaction.

Issue with Ordering

You might notice that free floating update transactions present an issue. If the last update transaction can bind to to any earlier update transaction (including the funding transaction), then the opposite is true: any of the earlier update transactions can bind to the last update transaction as well. This would nullify the last settlement transaction!

To address this, eltoo cleverly invokes the concept of *state numbers* in its locking scripts. This maintains an ordering between update transactions, such that update transactions can bind *backwards_indiscriminately, but not _forwards*. Again, the locking script on any of our update transactions looks as follows:

```
OP_IF
  10 OP_CSV
  2 A_{s,i} B_{s,i} 2 OP_CHECKMULTISIGVERIFY
OP_ELSE
  <S_i + 1> OP_CHECKLOCKTIMEVERIFY
  2 A_u B_u 2 OP_CHECKMULTISIGVERIFY
OP_ENDIF
```

The locking script from the funding transaction

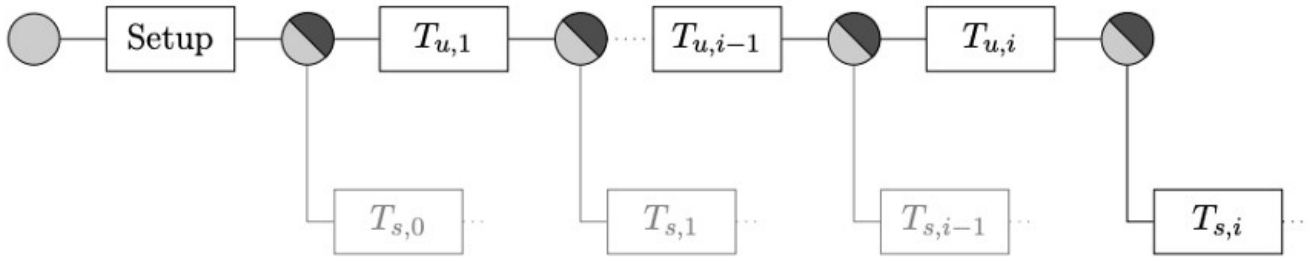
The *ELSE* branch is for update transactions, and the first instruction is:

<Si + 1> OP_CHECKLOCKTIMEVERIFY [OP_CLTV for short]

*OP_CLTV_in an unspent output checks the **nLockTime** of the transaction that attempts to spend it. When you submit a transaction with an nLockTime of over 500,000,000, Bitcoin interprets it as a Unix timestamp. That is, the spending transaction won't be mined until that timestamp is met. Any value less than that is treated as a minimum block height; that is, your transaction can't be mined until the Bitcoin blockchain is _this tall*.

But there's a clever trick here! If you make *nLockTime* greater than 0, less than 500,000,000, *and* less than the Bitcoin blockchain's height, then any transaction

you publish can be mined immediately. This defeats the purpose of using nLockTime to delay transactions from being mined, but we can use that entire range of values to create an ordering between our update transactions without arbitrarily delaying them from being mined.



Say the funding transaction specified an *OP_CLTV_of 1. This means that the first update transaction, denoted by* ***Tu,1****, would need an nLockTime of at least 1, so Alice and Bob make sure the next update transaction has an nLockTime of 1. The output produced by the first update transaction would then specify an _OP_CLTV* of 2 in its locking script. The next would specify 3, and so on.

Now, if Alice and Bob tried to bind the first update transaction to a later output — say, the third output — the Bitcoin blockchain would reject it, because the first update transaction's nLockTime is 1, while the third output has a locking script requiring an nLockTime of at least 3.

Although all of the update transactions are signed with ***SIGHASH_NOINPUT***, no earlier update transactions could bind to a later update transaction, because the nLockTime would be below the required *OP_CLTV* in that output's locking script. This protects the integrity of the last settlement transaction, denoted **Ts,i**.

Settlement transactions must also use ***SIGHASH_NOINPUT*** . In the event the output it spends changes its input to point to the funding transaction (because the channel is closing), that output's transaction ID would change, because the input of a transaction is part of what makes up a transaction ID. Thus, any settlement transaction needs to be able to change its input to reflect the new transaction ID without making its existing signature invalid.

However, you'll notice the settlement branch of the locking script does not contain any concept of state numbers like the update branch does.

```
OP_IF
  10 OP_CSV
  2 A_{s,i} B_{s,i} 2 OP_CHECKMULTISIGVERIFY
OP_ELSE
  <S_i + 1> OP_CHECKLOCKTIMEVERIFY
  2 A_u B_u 2 OP_CHECKMULTISIGVERIFY
OP_ENDIF
```

The locking script from the funding transaction, and any subsequent update transaction.

At first glance, it would seem this would cause the same problem we described earlier: old settlement transactions could be applied to future update transactions, producing a race condition to see which settlement transaction would be mined on-chain.

Instead of using state numbers, the solution here is that each settlement transaction uses a *different keypair* that gets *derived from the state number* of the output it spends. Thus, while the settlement transaction maintains the flexibility of changing the transaction ID in its input without invalidating its signature by using ***SIGHASH_NOINPUT***, it can still only spend *that specific output_because the keypair from its signature _only unlocks that specific update transaction*. Thus, settlement transactions maintain a unique binding to a specific output by having a specific keypair that only works with that output.

Wrapping Up

Bidirectional state channels can be complex, but eltoo provides a simple, innovative way to implement them. I hope you enjoyed this view into the Lightning Network — stay tuned for similar posts!

Why Bitcoin Needs to Become a Medium of Exchange

By Roy Sheinfeld

Posted July 29, 2019

Despite its awesomeness, not everyone loves bitcoin. Beyond government institutions threatening the best cryptocurrency in existence, more or less centralized and private virtual currencies, like Libra and Ripple, are pseudo-competition. For all of bitcoin's advantages and its sizeable head start, the race is not yet won.

In fact, there is a risk that bitcoin could be marginalized. Yes, it's a great store of value (SoV) at the moment, but bitcoin's utility as an investment depends on being able to convert it into currency *at some point*. HODLers love HODLing, and it's not a bad strategy in the short to medium term, but an investment is worthless unless you can cash it in.

Serious question: will conversion always be an option?

People struggling — recently — to liquidate their assets. Bitcoin is too good for this. (Source: Wikimedia)

As long as bitcoin remains "only" an investment alongside soybean futures and rare coins, only of interest to the FinTech few, it is vulnerable to censorship. Censorship just means that bitcoin's connections to the real economy would be dictated by some third party, not by the peers on the network. Bitcoin's technological and mathematical foundations would stay intact, but it can be throttled, stifled, and relegated.

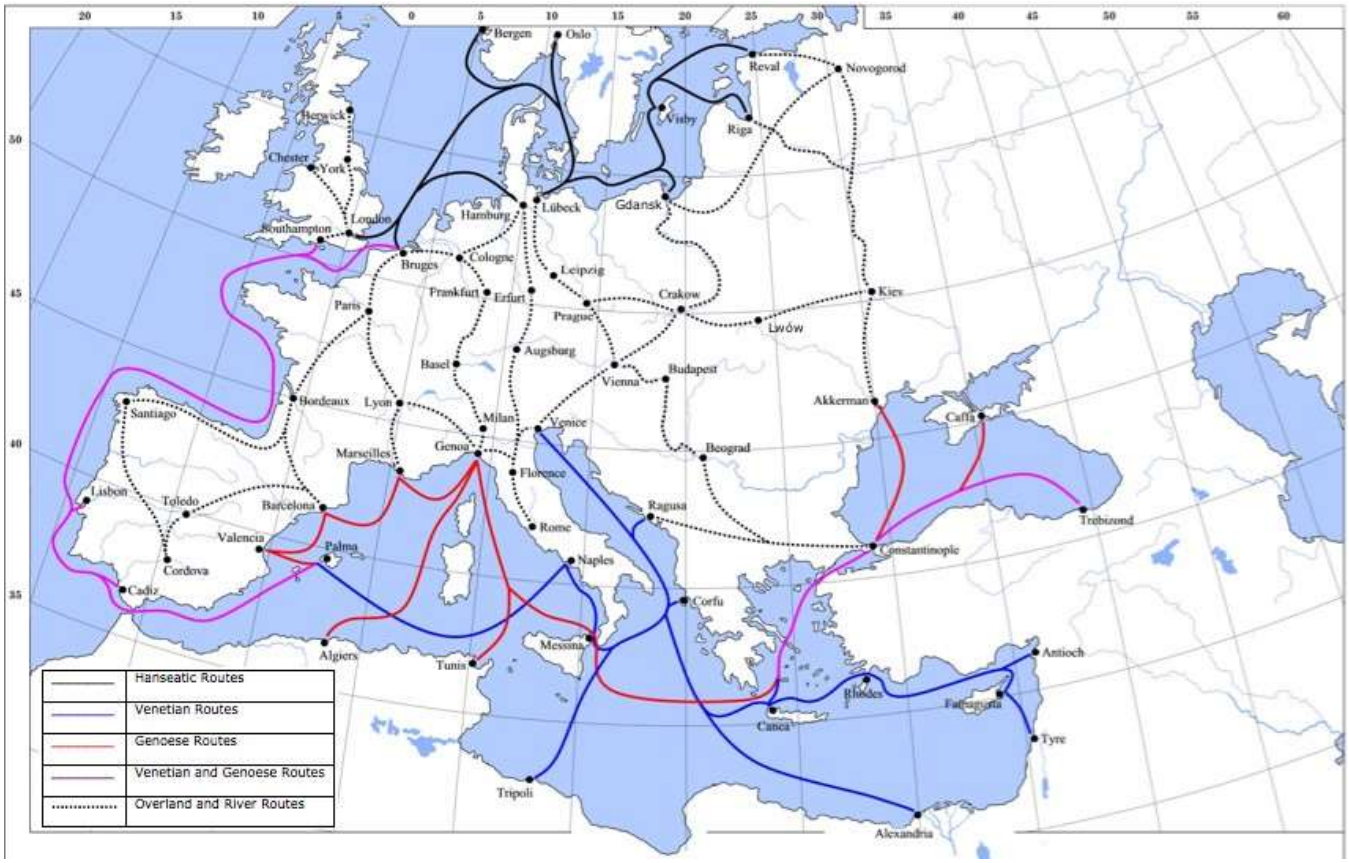
So let's talk about the choke point that threatens bitcoin's bright future and, just as importantly, how to eliminate it.

Choke Points: How to Censor Efficiently

Fun fact: income tax wasn't really a thing until about 200 years ago. All those castles, canals, and wars were financed without collecting a significant amount of income tax. I'm sure many rulers would have loved income tax, but without reliable censuses, population registries, and a banking system through which most money flowed, they simply didn't have the technical ability.

Instead of income tax, rulers mostly generated income through import tariffs. The great advantage of tariffs was that imports and exports generally crossed the border at a limited number of mountain passes, bridges, straits, and ports. The population was dispersed, but imports were concentrated.

Choke points — limited, narrow interfaces between domains — made imports easy to control and exploit.

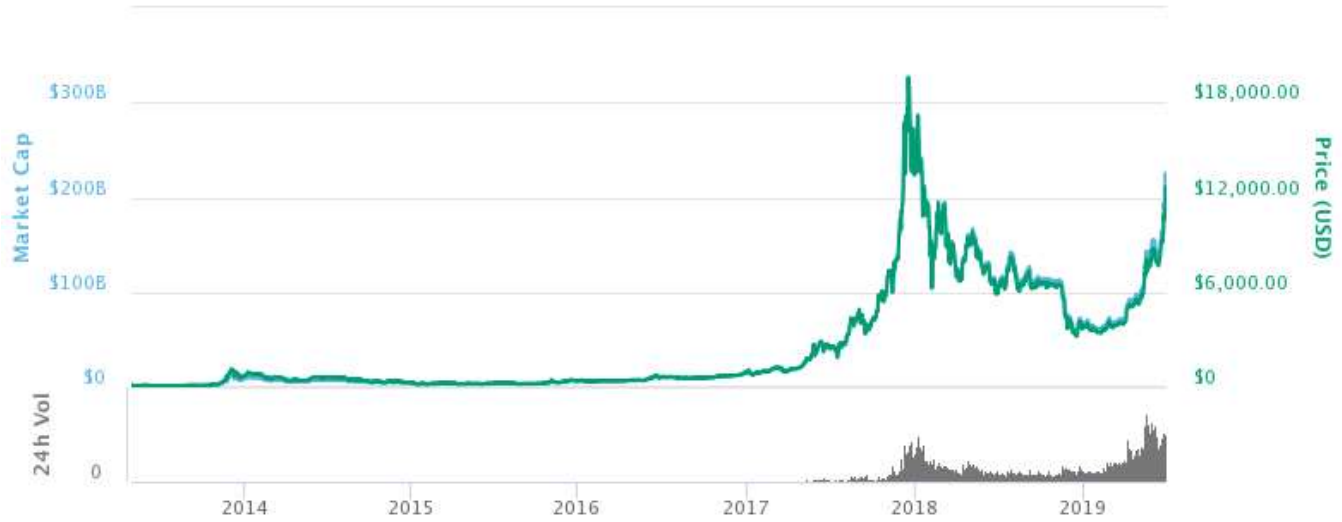


Bureaucrats are lazy. They'd rather control a few dozen trade routes and ports than 100 million cranky peasants. (Source: Wikipedia)

For example, spices came from the Far East across the Indian Ocean or the Silk Road, and they concentrated in a few ports in the Eastern Mediterranean, like Alexandria and Tyre. Controlling the choke points was so profitable that some argue it was an ulterior motive of the Crusades. It made the famous fortunes of Venice and the Ottoman Empire. In fact, the Ottoman Empire muscling in on the spice trade is one reason why Ferdinand and Isabella of Spain took the very risky move of financing Christopher Columbus's (at the time) insane voyage only four decades after the Ottomans sacked Constantinople.

Bitcoin's Choke Point

I'm not arguing against bitcoin's utility as a SoV. That's not the issue. In the last 10 years, its price has gone from about $0.03 to around $10,000, vastly outstripping the 20% inflation in the same period. Anyone who doubts bitcoin's utility as an investment simply hasn't been paying attention.



Bitcoin's price development over the last decade. Your Honor, the defense rests. (Source: BitcoinWiki)

Rather, the question is how to realize that value. Long-term investing is fine, but the destiny of every investment, at some point, is liquidation — conversion into spending money. Otherwise, what's the point?

For any currency, the interface between the SoV and the medium of exchange (MoE) is a choke point. Anyone controlling that interface can either interrupt the connection between them or inflate the currency into oblivion. Without convertibility, a SoV is just paper (or digital ledger entries, as the case may be). The way to censor bitcoin is to interrupt its convertibility into the currencies of the real economy.

Predators, prize fighters, and vampires all implicitly know how to find and use a choke point … and you don't want any of them coming after you. (Source: Wikimedia)

How to Overcome Bitcoin's Choke Point

In *The Bitcoin Standard*, Saifedean Ammous suggests two ways to overcome the scalability limitations that prevent bitcoin from becoming a MoE: custodial intermediaries and second-layer solutions.

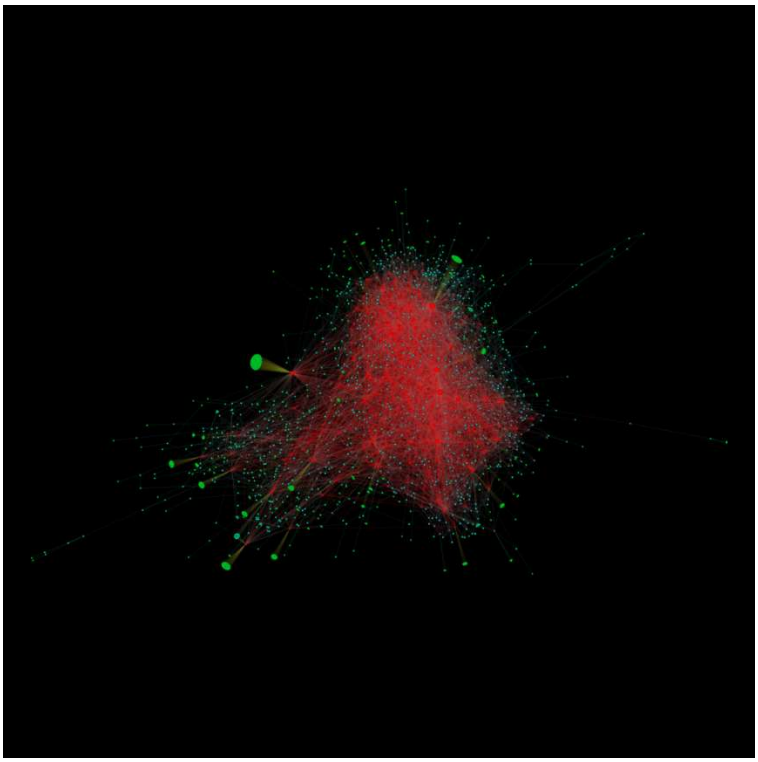
Custodial intermediaries can issue bitcoin-proxy vouchers that would be faster and computationally lighter than bitcoin. However, they also introduce a new choke point. With custodial intermediaries, their digital vouchers are the MoE, and bitcoin is stuck in its current role as the SoV. The interface remains, and it requires significant trust that the intermediary is honest and secure. Any third party who wanted to control or shut bitcoin down would only have to lean on a limited number of choke-point intermediaries.

The best way to eliminate the choke point is to, well, eliminate the interface between the SoV and the MoE. *Until bitcoin works as a MoE, this choke point will remain. As long as bitcoin requires conversion, as long as it's investment-only rather than currency, it is vulnerable.* But when bitcoin works — and is actually used — as a MoE as well as a SoV, there is no more choke point. It would be impossible to censor, impossible to stop.

But it has to be bitcoin.

Lightning is the second-layer, peer-to-peer, (virtually) trustless way of turning bitcoin into a MoE. *Lightning is bitcoin* without compromises. It maintains all of bitcoin's defining characteristics: open, borderless, neutral, censorship resistant, decentralized, public, immutable. It removes bitcoin's block-size limitation, and transaction fees drop low enough to make bitcoin practical for even the smallest purchases, like a pack of gum or a subway token. We can also make Lightning light enough to run on mobile — Android or iOS — with a UX rivalling fiat's best.

Non-custodial Lightning preserves bitcoin's status as *the* genuine peer-to-peer cryptocurrency, and it eliminates the interface between the SoV and the MoE. They become one and the same thing. Instead of fortifying the choke point against capture, Lightning eliminates it.



Here's a graph of the Lightning Network. Find the choke point. I'll wait. (Source: Wikipedia)

MoE is Evolution, not Revolution

Now this isn't just some theoretical discussion about how to make currencies censorship resistant. We actually have to act. We have to help bitcoin evolve from "just" a SoV into a MoE. And that means we have to spend it. We have the peer-to-peer, trustless, cheap, mobile technology. There's no excuse anymore. Nothing is stopping us from creating a circular economy based solely on bitcoin.

You'll be doing yourself and bitcoin a favor. Growing into a MoE will help bitcoin by connecting it more deeply to the real world. At the moment, bitcoin's value depends on its relative scarcity and ephemeral expectations. But if everybody knows that you can buy a decent meal, a bottle of wine, or a couple hundred gigs of flash memory with 150,000 Satoshis *anywhere in the world or online*, then those Satoshis really are worth those things. Bitcoin's value would enter the real economy and become just as real as everything in it.

Bitcoin's widespread use as a MoE also helps those who already hold it by insulating them against volatility. At its fastest, bitcoin manages about 15 transactions per second, and the normal rate is around 5. Just a couple dozen big trades in quick succession can rapidly and radically distort the price, making bitcoin relatively easy prey for speculative arbitrage. But in a field of thousands or millions or successful Lightning transactions every second, each one carries less weight relative to the aggregate total. If we all start spending bitcoin, we gain herd immunity against speculators … and probably pizza.

Keeping the fish captive might feel like protecting them, but only those that can swim freely will evade predators and catastrophes. (Source: EktaVaria & Pixabay)

Every Investment is Speculation - Move on!

By Jeff Dorman

Posted July 29, 2019

U.S. stocks hit all time highs again, amidst better than expected GDP data, progress in trade and budget talks, and hopes for looser monetary policy ahead of this week's FOMC decision. Not to mention, Congress lifted the debt ceiling again (which at this point appears to be more like a limbo bar than a ceiling). Meanwhile, the crypto markets continue to go the other direction, declining roughly 10% week-over-week. Crypto prices are now down 40% from recent highs, and are making lower highs and lower lows during this period of heightened volatility.

Bitcoin seems caught in a full fledged tug-o-war between long-term positives and short-term negatives. On the positive side, supply/demand is in Bitcoin's favor (in August 2020, mining rewards will be cut in half), so if demand remains the same, prices will rise. Additionally, a deteriorating macro backdrop propped up by unprecedented and continuous inflationary monetary policy almost explicitly screams "Buy Bitcoin". On the negative side, Bitcoin is still small and largely irrelevant as a global store of value, it has massive swings in value based on leverage and speculation, and can be considered overvalued based on current usage metrics.

However, the far more common view is that Bitcoin can't be owned at all - a view that we think is completely uninformed.

In a recent story, Edward Jones investment strategist, Kate Warne, claims that people investing in cryptocurrencies are setting themselves up for a disaster. She opines:

"We don't like the specifics of bitcoin, and we really think the price is moving around on speculation, rather than something else. When you think about bitcoin, you're looking to buy something that you hope to sell for more to somebody else who's more excited than you are. That's the essence of speculation. We would not advise investing in them or speculating in them. If it goes up, sell it. If it goes down, sell it. But get out quick."

Giorgio Carlino, a managing director and CIO of the global multi-asset team at Allianz Global Investors, New York, also went on record stating that Bitcoin is not investable:

"As an institutional investor, you should not, you could not actually, explain a position in bitcoin … or any other crypto in your portfolio as an asset allocation. The valuation of the cryptocurrency is not possible as of today. They have no income, there's no

intrinsic value, there's no guarantee by a state or a central bank. It is an interesting concept and I'm fascinated, but it's not an investment."

Carlino's colleague, Andreas Utermann, AllianzGI CEO and global CIO, went further stating:

"The value of a cryptocurrency is in the eye of the beholder. This makes cryptocurrencies entirely unsuitable for investing in."

Let's break this down starting with the term "intrinsic value". This is an entirely made up term for investing, based on a philosophical concept, wherein the worth of an object or endeavor is derived in and of itself—or, in layman's terms, independent of other extraneous factors.

The representatives of Edward Jones and Allianz above don't really say anything controversial. They simply say that Bitcoin doesn't have value by itself, and therefore it is just speculation based on what someone else will pay for it. But here's the problem with this simple and completely naive narrative.

EVERYTHING IN INVESTING IS SPECULATION!

While it is true that equities have a price floor based on the difference between assets and liabilities, and bonds have a price floor based on asset coverage, and even commodities have a price floor based on production value, the current price of ALL of these asset classes is many, many, many multiples above this floor. If these asset classes traded at "intrinsic value", the entire investable universe would plummet.

Think about this for a moment. When you buy a stock, you are speculating that the company will increase cash flows, or that multiples will expand. Further, when a stock trades at a 15x P/E ratio, or at 2x Price/Sales, or at 8x EV/EBITDA, these values are WAY above intrinsic value. These values are based on what the market perceives someone else will pay for it (either another investor or a strategic buyer). When you buy a corporate bond, especially a BBB-rated or high yield bond, there is ZERO chance that this company can pay off maturing debt using free cash. Instead, you are buying these bonds based on speculation that other investors will help refinance these bonds when they mature with the purchase of new speculative bonds or stock to pay off the old debt. When you invest in commodities, you're speculating that there will be increased or continuous usage. Even when you invest in early stage technology companies via private stock, you are speculating that mass adoption will occur with no data to support it. Finally, I wonder if anyone at AG Edwards or Allianz has ever owned a call option or a put option? If you bought a $3500 December 2019 SPX call option right now, the intrinsic value of that option is ZERO. But it has value due to time, volatility and other factors in the Black-Scholes model.

To say that you should not invest in Bitcoin because it is speculation is ill-informed. For naysayers that don't believe the speculation is justified, that's fine – this would be a logical conclusion and everyone is entitled to their opinion. But the word "speculation" is flat out lazy. To quote Howards Marks: "I'd much rather be an intelligent speculator than a conventional investor."

On the flip side, for those that understand risk/reward and understand how to value speculation, Bill Miller just taught a course on how to incorporate risky assets like Bitcoin into a broader portfolio- his fund rose 46% in the 2nd quarter led by his Bitcoin long position. Yes, this Bill Miller:

Miller, 69, has found success by following the same playbook he used during his three-decade run at Legg Mason:picking beaten-down securities that trade at a large discount to their **intrinsic value**.

Once we agree that everything is speculation, it's much easier to see why speculating on digital assets makes sense as a complement to other investments, and perhaps eventually, as an outright replacement. Arca's own David Nage continues to spell out the bull case each and every day to those who will listen, and he is starting to attract others who want to tell their digital asset stories as well (we highly recommend his recent interview and webinar with Cambridge Associates' Marco Veremis).

Stop Looking Just at Bitcoin - an Entire Asset Class Sits Below

We're not done with Allianz. Not only can we easily debunk their anti-Bitcoin stance, but we can also debunk their anti-Digital Assets stance. For anyone who is seriously considering this asset class as an investment, or who feels confident enough to deride its existence, it would make sense to move beyond just Bitcoin and cryptocurrencies and explore the other investable digital assets that make up the rest of this asset class. A crypto investor wouldn't make a statement that healthcare stocks don't exist simply because the media focuses on FANG stocks. That would be foolish and uninformed right? In the same fashion, Allianz and many others undoubtedly have no idea these other digital assets exist. A majority of the investable token landscape does not fall into the "cryptocurrency" sub-category.

We are in the midst of an evolution where tokens now take on a variety of unique investment characteristics. Some are essentially equity-linked notes of cash-flow producing companies, others are more akin to "airline miles". A few tokens thrive on community engagement and growth mechanisms, while others represent asset transfers in forms that were previously unheard of (i.e. transferring computer file storage).

Let's focus on one of the easiest digital asset sub-categories to understand. Many crypto exchanges that allow investors to buy and sell digital assets have issued

"tokens" that serve as part utility / part security. In its basic form, if you own an "exchange token", you are typically entitled to discounted trading fees on their site (utility), and a percentage of the company's revenue/profit (security) in the form of a token buyback. Many of these companies have net profit margins that would put US and International publicly traded companies to shame.

These exchange tokens can also be valued, both on an absolute basis and a relative value basis. While the actual valuation techniques we use at Arca are above the scope of this market recap, let's look at a very simple example. While "market cap" is not necessarily the best indicator of value, we can use it as a proxy. Here are 4 exchange tokens currently on the market:

- Binance is the largest and most well known
- Bitfinex is the oldest, and the largest by Bitcoin volume
- RenRenBit is a little over a year old, and just completed a small token raise last week to grow its business further
- FTX is a brand new,interesting but completely unproven exchange, and is about to launch a token this week at an incredibly lofty valuation

Source: Arca Proprietary Data and Company Estimates, similarweb

These tokens are clearly not "Currencies" and, instead, give investors and users of their platforms a chance to participate in the company's growth. All of these companies are real companies, with real equity values that are distinct and separate from their token values. Further, they are similar enough that relative value matters. For example, it's pretty clear that successful, proven leaders like Binance and Bitfinex can capture tremendous value in the form of user growth and revenue. Meanwhile, newcomers like RenRenBit that are realistic about their company's value can give "venture-like" returns to investors and users who want to bet on their growth, while others like FTX may be trying to take advantage of unsophisticated investors with absurdly high initial valuations. Eventually, as we continue to move away from just protocols and "decentralized everything", you end up with interesting tokens like these that derive value based on their users. And user growth can be measured. And measurements can be compared.

So a word to the prognosticators out there making public statements. Educate yourself before becoming a meme.

Blockchain, Bitcoin, and Libra

By Alex Svetski

Posted July 30, 2019

I've been told my "definition" of Blockchain differs from the "commonly used" one.

This is probably true, so I decided to examine why.

First of all, what's meant by "commonly used". I have a problem with this idea because I'm yet to understand the parameters of "commonly used", and am still trying to understand what anybody is actually referring to when they begin to throw the word "blockchain" around [with so much certainty].

A number of years ago, I found myself personally entangled in the term "blockchain", attempting to explain it to people at the local "bitcoin & blockchain" meetups I was hosting. The argument centred around grouping data in blocks & cryptographically hashing it to the data in the previous block in an attempt to build some form of "immutable ledger" (another term that gets thrown around) that could act as the basis of a more secure method of data storage.

Whilst on the surface, this sounds interesting, in reality it's neither special, unique, profound or even useful.

I still remember the "aha" lightbulb moment where I realised that this concept was not the basis of Bitcoin's immutability, & that immutability of the historical data on the ledger had very little to do with hashing to the previous block & everything to do with using that data structure/methodology together with the economic game of probability that Bitcoin used to achieve autonomous consensus (ie; its inclusion of PoW in its solution to the Byzantine Generals problem, aka; Nakamoto Consensus).

What I've since informed anyone I come across (or at least those who choose to listen) is that defining "blockchain" outside of the context of Bitcoin is like trying to define a carburetor without the existence of a car.

Blockchain for Lettuce

The sad truth is that since Bitcoin's inception, there have been many, many attempts to take absolutely necessary parts out of the Bitcoin Recipe (see page 5 of https://bitcointimes.news) in order to deliver something called a "blockchain" - for just about every application imaginable.

When one tries to understand the application or definition of their 'blockchain', you quickly realise it's just a glorified database, utilising some simple time stamps, &

maybe data segmentation. Something we've had for decades, & in most instances, the use of which is completely pointless.

In a bid to stay ahead of the curve, the "blockchain" narrative evolved into "DLT"; standing for Distributed Ledger Technology, where the "block" part of the blockchain was removed & the "distributed" element (also part of the broader Bitcoin recipe) was now glorified. The new narrative is just a variation of the old. "It's immutable because every validator has a record of the ledger".

The problem this time around is that if every validator is known, or permissioned, then have we really created something new? One could argue that in some corporate applications where more checks & balances are required, or there is a need for shared decision making, this could be useful, but by no means is this immutable, broadly applicable, or as one of the ridiculous narratives goes; "faster".

Having more parties participate in validation is by definition slower - and that's fine - especially if you want more checks, but digital immutability is a binary term. You either have it or you don't. The private, permissioned distributed ledgers are not immutable in any way, because there is no cost to change the historical record - only a requirement to collude via the quorum of the group. If anything, DLT is just a glorified multi-party authentication system - which like I said, is fine in some cases - but not when painted with "all the glorious things" it's going to give the world.

Open, decentralized networks [insert blockchain word here] such as Bitcoin are immutable, distributed & happen to group transactions together to achieve autonomous consensus amongst network participants who do not know each other. The result is a digital network that is inherently tied to real world cost via real-world energy. The more energy & cost associated with the network, the greater it's degree of immutability.

Therein lies the innovation.

It is unprecedented & its application to something that requires an extraordinary degree of censorship resistance, eg; a non-sovereign form of monetary unit, is where "the killer app" lies. Not IBM's "Blockchain for Lettuce".

Is this recipe useful anywhere else?

Many have argued that using the entire Bitcoin recipe, & applying its output (ie; digital immutability & censorship resistance) to things outside of a non-sovereign monetary network + unit is a good idea. Enter Ethereum, etc.

Whilst I won't go into the details here, I am very skeptical of the need to apply immutability & censorship resistance (or make it an integral component of the stack) to many things in the world due to the inherent cost of doing so.

I'm extremely skeptical of the idea of "Dapps". Even if we assume Ethereum is censorship resistant (the numbers don't add up), & that the Dapps are also actually decentralized (they're not), how many applications really need to have immutability or resistance to censorship as a native part of their stack? Maybe an "ebay for Hitmen" - but by & large, if you have an idea for an app, in today's day and age - just go spin up an AWS instance, and make it happen!

Bitcoin's unique recipe is very useful for a specific set of things, much like building a tank is useful for a specific set of things. Putting the tank on a race track or removing all the armour to make it faster & then sending it into battle are both misguided.

The Verdict?

The world Blockchain was popularised in 2013 & 2014 by groups of banking consortiums, who are inherently threatened by the disintermediation that Bitcoin presents.

Seeing the banks, accounting & IT giants, like the Big 4, the IBM's & Accenture's of the world, tout DLT or Blockchain is just classic PR. They're announcements by large, (in most cases boring) corporates who are desperately trying to show that they're still somehow "innovative". Similar to how they use (and exaggerate) the words "cloud", or "Ai", or "big data".

There is very little innovation there. So I call Bull$#%!.

Onto Libra

Libra has red-pilled more people into Bitcoin recently than just about anything else. The idea that a non-sovereign currency can be issued, by an entity which is not a government or a state has actually opened the minds of millions of people who could not perceive that earlier.

The fact that Facebook has circa 2bn people on their network makes it the largest community (country) in the world, & people's ability to grasp the notion of that community having their own money is a much easier mental leap.

Once they make that leap, they then have an easier time understanding Bitcoin, as seen by the journey people like Joe Kernan from CNBC Squakbox are on.

Whilst Facebook has used the term "Blockchain" in their definition of what Libra is, it's actually an inaccurate representation. I won't do the argument as much justice as Jameson Lopp did, so I'll link to his article here:

https://onezero.medium.com/thoughts-on-libra-blockchain-49b8f6c26372

But suffice it say; it's not a blockchain.

In fact, Facebook & the Libra consortium have ZERO interest in building their own "blockchain". What they're attempting with Libra is something so much larger, & it's exactly why all the governments (big or small) are up in arms about it.

Let's think about it for a moment.

- Libra is in direct competition with government based fiat currencies (and they all know it)
- Consider what a population in a jurisdiction with a weaker national currency would do if LIbra launches there. Why would a citizen hold their hard earned wealth in something that's depreciating by 10 - 20% per annum?
- You quickly come to the realisation that there would be a "bank-run" on the national currency, with all the capital flowing onto Libra. The result would be catastrophic for the government in power, as it's economic lever is the basis of its control of the population.

Governments are scared—and rightly so. Facebook is arguably the largest "country" in the world, & their currency would be more useful to more people than the fragmented fiat ones they're using today.

This is the real play. Libra is attempting to do their own Bitcoin - they couldn't care less about Blockchain.

Bitcoin is the "Killer App".

Bitcoin is fundamentally unique.

Its immaculate conception & organic introduction to the market, its initial broad based adoption for strong, libertarian reasons & the timely disappearance of the founder, leaving no "head of the snake" to cut off are just a few of the things that make it impossible to replicate.

Digital scarcity, Bitcoin's core innovation is by definition, a one-time event. Every other cryptocurrency, optimising for complex, turing complete smart contracts on the base layer, or faster payments are quickly being shown as irrelevant or short term noise.

Bitcoin's focus on being a censorship resistant public network, owned by the participants, that's broadly decentralised & organically priced by the market is the killer app.

Libra by facebook reinforces all of the above, by making all other cryptocurrencies who optimised for the wrong thing obsolete, & giving us a strong contrast to what Bitcoin represents for the world, ie; a money of & for the people—that cannot be shut down, censored, confiscated or inflated.

This was a once-off opportunity.

The smart money knows this & Bitcoin will continue to suck up all the capital & liquidity whilst all the other noise (crypto) will continue to trend toward $0 against Bitcoin in both dollar terms & relevance.

Bitcoin VS Libra: The real showdown.

Libra inherently validates Bitcoin.

It opens people's minds to the idea of a floating, global currency that is not managed or issued by a state of government.

The question is, would you use it? Or would you prefer to use something like Bitcoin?

Whilst there are similarities between them, I would argue that Bitcoin is the antithesis to something like Libra, which to me sounds like we're jumping from the frying pan into the fire.

Whilst I'm not a fan of government or central bank-decreed fiat money, I question the logic of moving from a global USD reserve to a Libra reserve.

Sounds a little like 1984 to me. Not to sound conspiracy theorist, but the idea of one party, or even a consortium of the "big boys" having the final word on the most important resource in society, ie; money, ie; the unit of account that measures the input of all participants in society + the world at large → sounds dangerous to me.

This, fellow readers, is why Bitcoin matters. It's exactly why Bitcoin optimised for censorship resistance, privacy & self-sovereignty, not "fast payments" or "smart contracts" like all the other now-irrelevant crypto's did.

All of the "potential" that's promised (amongst the noise) in crypto will be built on top of the most robust network. What remains to be seen is whether that's Bitcoin, or whether that's Libra (or both).

A new Money is the real battle-ground. Not Blockchain.

And in my mind, Bitcoin is the only real alternative to a potentially Orwellian future.

Verdict on Libra? Big Brother.

Conclusion

Bitcoin is the most under-appreciated innovation in History, but as with all great zero to one innovations, it's the contrarian aspect that makes it so much more profound.

In 1000yrs, the concept of money will very much still exist—because it's the foundational element required for any society to function.

Much like the internet, Bitcoin is a public good—owned by the people—and by taking the ***only*** two finite resources that we know of (time & energy), Bitcoin is able to give the world a superior monetary network & unit that we can use to better collaborate & function as an open society.

Blockchain is not an alternative, nor does it even matter & nor will it even be spoken about in the coming 5yrs. The real alternative is potentially 1984-stye big brother currencies, whether they're government issued (eg; China's social credit system), or issued by non-state consortiums with disproportionate influence in the world (eg; what FB is doing with Libra).

It's the opt out of those that gives Bitcoin the brightest future of all.

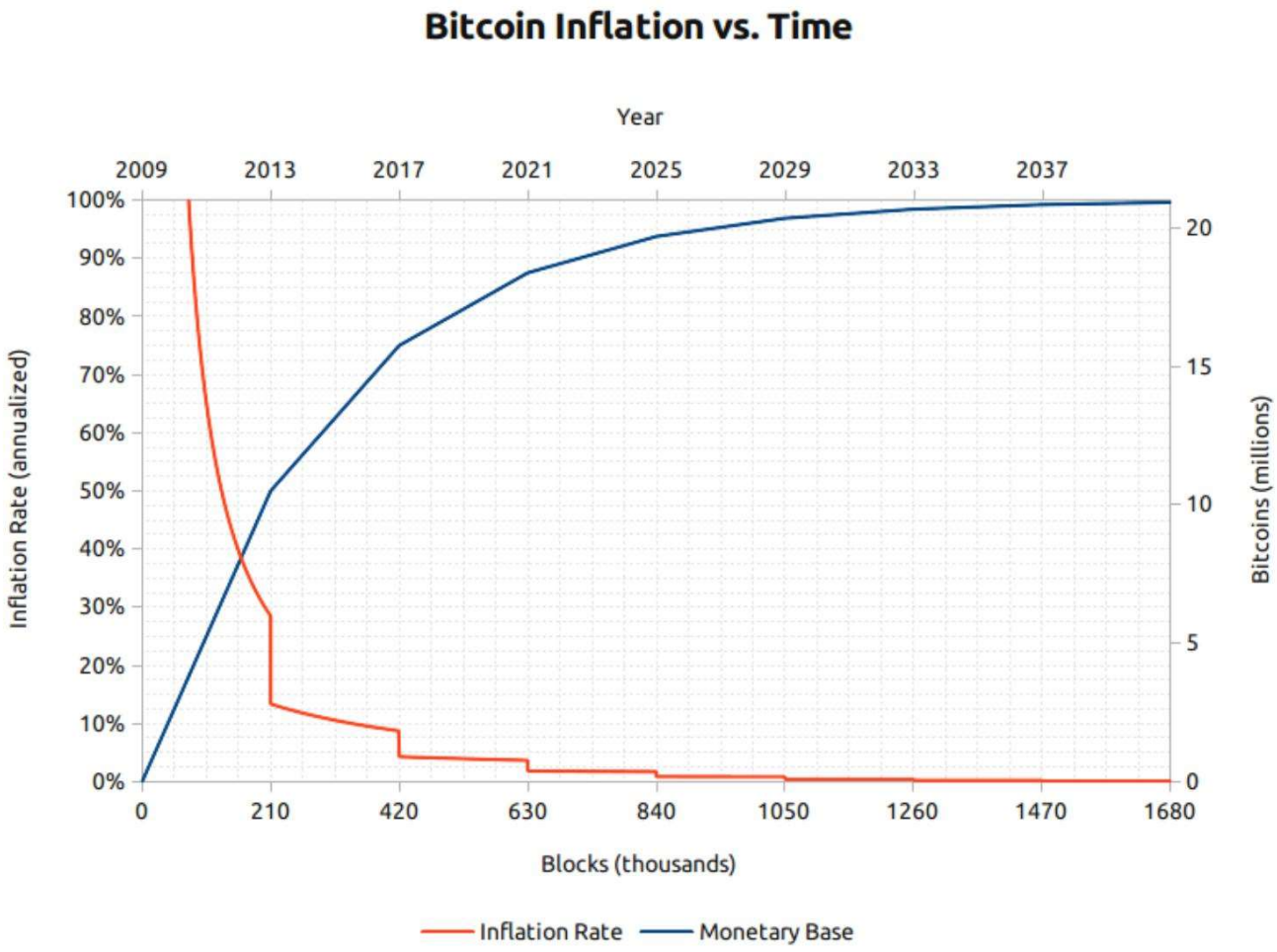
Verdict on Bitcoin? **Brilliant.**

Tweet: This is my favorite graph, what's yours?

By Pierre Rochard

Posted July 31, 2019

This is my favorite graph, what's yours?



Disclaimer:

THANK YOU, CREATORS.

WORDS

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

This Journal does not contain reference to any of the investment products or services currently offered by 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.

DYOR | BTFD | HOLD