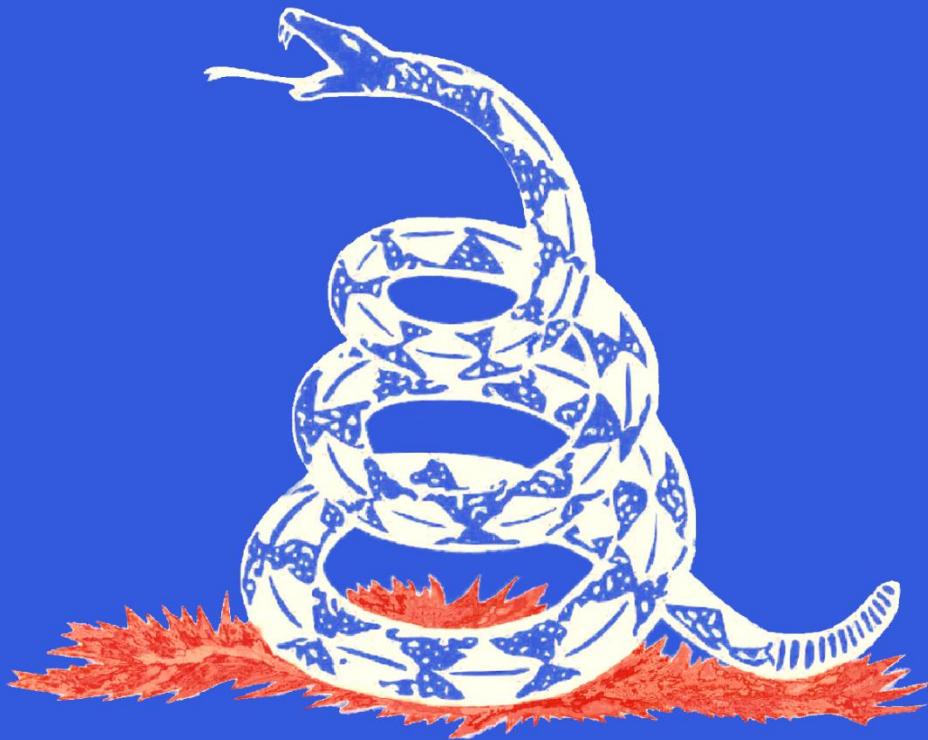


WORDS

June 2020



DONT TREAD ON ME

Contents

Contents	2
Goals and Scope	3
Support WORDS.....	4
Cover Art by Clancy Rodgers.....	5
57 Varieties of Pyrite: Exchanges Are Now The Enemy of Bitcoin	6
Bitcoin for the Open-Minded Skeptic.....	8
Bitcoin Mining's Three Body Problem	16
Anarchy and Monarchy: A Natural State.....	28
The State vs. Bitcoin	35
Bitcoin and the intolerant minority.....	47
A Peaceful Protest - Opt-Out, Buy Bitcoin.....	50
Mining for the Streets.....	57
Bitcoin: Reform or Revolution? Part 1	73
Bitcoin Has to Be for Everyone	78
Bitcoin is Antifragile	81
Bitcoin Needs You As Much as You Need Bitcoin	94
Why Bitcoin is a silent protest against corrupt governments everywhere.	99
Tweetstorm: Bitcoin Marketing.....	103
The End Of Gold.....	108
The Bitcoin Journey	114
Bitcoin's Town Square.....	123
How I checked over 1 trillion mnemonics in 30 hours to win a bitcoin	133
Bitcoin and the Trust Problem: Is Bitcoin adoption accelerated by the abuse of trust?	143
Disclaimer:.....	240

Goals and Scope

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

History

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

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

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

Support WORDS

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

⚡ Support WORDS

Spread the word

The only way to spread the good word is to share it. Consider sharing *WORDS* with friends on social media. Share <http://words.pub> or <https://bitcoinwords.github.io>

Follow us on social media

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

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

🐦 Twitter

Subscribe to the newsletter

The journal is published monthly and is distributed via Twitter and newsletter. Consider subscribing to the newsletter. If you're not on Twitter all day, it might make sense to subscribe so you never miss a publication.

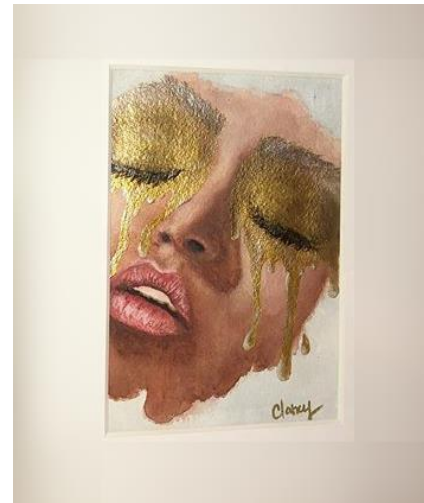
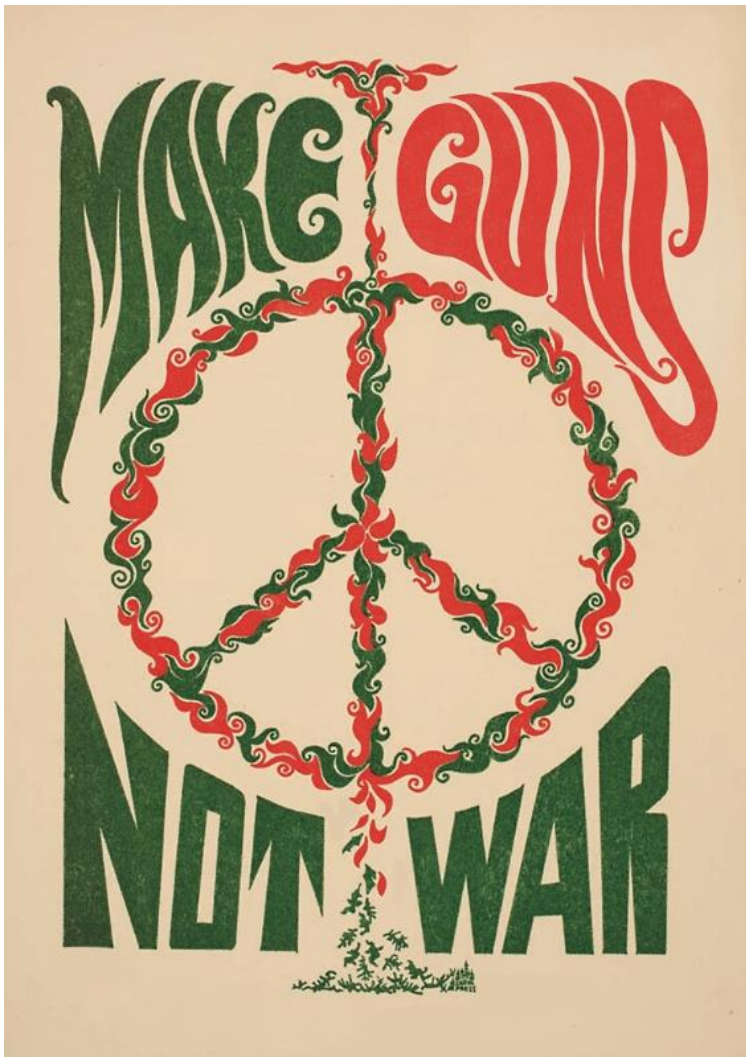
Subscribe

Our pledge

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

Cover Art by Clancy Rodgers

This month's cover art is by Clancy Rodgers. She's a multi-medium artist who's recently picked up the digital art brush (She's also my wife). Clancy is a true-believer and well worth a follow. She posts her art to Instagram, Twitter, and for sale on Redbubble.



57 Varieties of Pyrite: Exchanges Are Now The Enemy of Bitcoin

By **Rusty Russell**

Posted May 27, 2020

TL;DR: exchanges are casinos and don't want to onboard anyone into bitcoin. Avoid.

There's a classic scam in the "crypto" space: advertize Bitcoin to get people in, then sell suckers something else entirely. Over the last few years, this bait-and-switch has become the core competency of "bitcoin" exchanges.

I recently visited the homepage of Australian exchange btcmarkets.net: what a mess. There was a list of dozens of identical-looking "cryptos", with bitcoin second after something called "XRP"; seems like it was sorted by volume?

Incentives have driven exchanges to become casinos, and they're doing exactly what you'd expect unregulated casinos to do. This is no place you ever want to send anyone.

Incentives For Exchanges

Exchanges make money on trading, not on buying and holding. Despite the fact that bitcoin is the only real attempt to create an open source money, scams with no future are given false equivalence, because more assets means more trading. Worse than that, they are paid directly to list new scams (the crappier, the more money they can charge!) and have recently taken the logical step of introducing and promoting their own crapcoins directly.

It's like a gold dealer who also sells 57 varieties of pyrite, which give more margin than selling actual gold.

For a long time, I thought exchanges were merely incompetent. Most can't even give out fresh addresses for deposits, batch their outgoing transactions, pay competent fee rates, perform RBF or use segwit.

But I misunderstood: they *don't want to sell bitcoin*. They *use bitcoin to get you in the door*, but they want you to gamble. This matters: you'll find subtle and not-so-subtle blockers to simply buying bitcoin on an exchange. If you send a friend off to buy their first bitcoin, they're likely to come back with something else. That's no accident.

Looking Deeper, It Gets Worse.

Regrettably, looking harder at specific exchanges makes the picture even bleaker.

Consider *Binance*: this mainland China backed exchange pretending to be a Hong Kong exchange appeared out of nowhere with fake volume and demonstrated the gullibility of the entire industry by being treated as if it were a respected member. They lost at least 40,000 bitcoin in a known hack, and they also lost all the

personal information people sent them to KYC. They aggressively market their own coin. But basically, they're just MtGox without Mark Karpales' PHP skills or moral scruples and much better marketing.

Coinbase is more interesting: an MBA-run "bitcoin" company which really dislikes bitcoin. They got where they are by spending big on regulations compliance in the US so they could operate in (almost?) every US state. (They don't do much to dispel the wide belief that this regulation protects their users, when in practice it seems only USD deposits have any guarantee). Their natural interest is in increasing regulation to maintain that moat, and their biggest problem is Bitcoin.

They have much more affinity for the centralized coins (Ethereum) where they can have influence and control. The anarchic nature of a genuine open source community (not to mention the developers' oft-stated aim to improve privacy over time) is not culturally compatible with a top-down company run by the Big Dog. It's a running joke that their CEO can't say the word "Bitcoin", but their recent "what will happen to cryptocurrencies in the 2020s" article is breathtaking in its boldness: innovation is mainly happening on altcoins, and they're going to overtake bitcoin any day now. Those scaling problems which the Bitcoin developers say they don't know how to solve? This non-technical CEO knows better.

So, **don't send anyone to an exchange**, especially not a "market leading" one. Find some service that actually wants to sell them **bitcoin**, like CashApp or Swan Bitcoin.

Bitcoin for the Open-Minded Skeptic

By **Matt Huang** on behalf of **Paradigm**

Posted May 2020

Download the original *Bitcoin for the Open-Minded Skeptic* report PDF.

Bitcoin has grown from idea (2008), to working system (2009), to its first real-world use at <\$0.01 per coin (2010), to a global currency valued at \$8K+ per coin and \$150B+ in aggregate (May 2020).

Although Bitcoin is empirically one of the best investments of the past decade, it still remains controversial. Is it a new form of money? A speculative bubble? Or a bit of both?

Investors have well-established frameworks for evaluating assets like equities, credit, and real estate. But a new monetary asset such as Bitcoin appears so infrequently that no clear framework exists.

This paper outlines a simple and intuitive framework for Bitcoin as a new monetary asset.

Why Now?

In the course of our work, we are often in the position of explaining Bitcoin to investors and institutions approaching it for the first time. Never before have we seen more interest in Bitcoin and its potential as a digital companion to gold.

Financial crises stress the limits of existing systems and can highlight the need for new ones. This was true during the financial crisis of 2008 (out of which Bitcoin was born), and it is perhaps more true today with the unprecedented levels of monetary and fiscal stimulus being pursued by governments worldwide.

There has been no shortage of writing about Bitcoin over the past 11 years. This paper does not claim any novel insight. Instead, it is a summary of the conversation we often have with investors seeking to understand Bitcoin for the first time.

Money

“The two greatest inventions of the human mind are Writing and Money – the common language of intelligence and the common language of self-interest.” –Mirabeau

Money is an old and complex idea. Historically, it has taken many forms: from decorative axes and cowry shells to precious metals and representative paper. The last major shift was arguably in the early 1970s with the end of the US gold standard and the beginning of the modern fiat currency system.

We can think of money as a competitive market like any other. Gold dominated for centuries not by accident but by possessing important features such as being scarce and unforgeable. Today, fiat currencies dominate largely through local monopoly power, but all monetary assets still compete globally, with gold, US Dollars, and Euros favored as reserve assets.

Like written language, money is a protocol standard with immense network effects. A new monetary asset can only emerge if it better fulfills the core functions of money, and it can overcome the adoption hurdle of a new money. We believe Bitcoin offers a compelling answer to both.

Store of Value

One of the primary functions of money is to be a store of value: a mechanism to transfer purchasing power across time and geography.

All successful money fulfills this function. If a monetary asset loses trust as a store of value, then savings quickly flow elsewhere, as seen in hyperinflationary economies like Venezuela.

Gold

Gold has been trusted as a store of value for millennia. Importantly, the supply of gold on Earth is scarce. Confidence in this scarcity rests in humanity's understanding of nature: that gold cannot yet be cost-effectively synthesized (despite alchemists' best efforts throughout history).

Gold also has many other desirable properties, such as being easy to recognize (no tarnishing), easy to divide, easy to measure (by weight), and easy to verify (through melting), so it is no surprise that gold replaced predecessors to become a global standard.

Paper Currency and the US Dollar

Paper currencies emerged to simplify the daily use of precious metals as a means of exchange (another core function of money). Although paper notes were initially linked to precious metals, today most paper currencies are free-floating and established by government fiat.

The US Dollar is the leading fiat currency and has been the global reserve currency for much of the last century (replacing the British sterling before it). In addition to being a trusted store of value, the US Dollar is the leading means of exchange and unit of account. A significant share of global trade is priced and settled in US Dollars, whether or not the United States is directly involved.

Confidence in the US Dollar rests on trust in the government (e.g., to wisely manage its monetary policy). There is great efficiency in placing such trust in a single institution, but there is also risk. Fiat currencies can lose credibility and be devalued through the actions of the government, who in times of crisis may face short-term pressures that outweigh concerns for long-term credibility. Countries like Venezuela offer an extreme precedent for currency value in the face of eroding trust: the currency becomes worthless.

Many investors, including central banks, own both gold and US Dollars (or US Dollar denominated assets) because they offer complementary trade-offs. We can think of the US Dollar as a centralized monetary asset, which can be devalued by a single actor, and gold as a decentralized monetary asset, which cannot.

Bitcoin

Bitcoin is a new decentralized monetary asset, akin to gold. It combines the scarce, money-like nature of gold with the digital transferability of modern currency. Although it remains relatively nascent, Bitcoin has great potential as a future store of value based on its intrinsic features.

As with any monetary asset, Bitcoin must be scarce, portable, fungible, divisible, durable, and broadly accepted in order to be useful. Bitcoin rates strongly across most of these dimensions, except for broad acceptability:

- **Scarcity:** Bitcoin supply is scarce, and asymptotically approaches 21 million coins. Achieving scarcity in digital form was Bitcoin's great technical breakthrough (building on decades of computer science research).
- **Portability:** Bitcoin is extremely portable, especially relative to gold. Arbitrary amounts of value can be held in a USB stick, or digitally transported across the globe in minutes.
- **Fungibility:** Any two Bitcoins are practically interchangeable, although each Bitcoin has a distinct history on the public ledger.
- **Divisibility:** Each Bitcoin can be divided into 100 million smaller units (called "satoshis").
- **Durability:** Bitcoins are durable and do not degrade over time.
- **Broad Acceptability:** Bitcoin's primary weakness: it is far less broadly accepted than gold or US Dollars, although it has made impressive strides over the past decade. We can think of broad acceptability along two dimensions, both of which are important: the % of people who trust and accept Bitcoin, and the % of wealth that trusts and accepts Bitcoin.

Beyond these classic monetary features, Bitcoin is also:

- **Digital:** Digital money like Bitcoin is cheaper to store and easier to transfer than gold, which is physically cumbersome. Bitcoin is also instantly verifiable, whereas gold can require a slow and manual verification process.
- **Programmable:** Bitcoin is programmable, which has subtle but far-reaching implications. Today Bitcoin scripting enables applications like escrow or micropayments. Over time we may be surprised by what can be built with Bitcoin (much as we were surprised by the Internet, another programmable substrate).
- **Decentralized and Censorship-Resistant:** The rules of the Bitcoin network (such as its monetary policy) are governed by a decentralized peer-to-peer network, involving a disparate and global user base of consumers, investors, companies, developers, and miners. It is impractical (if not impossible) for a single actor to unilaterally influence the rules of the system. This affords Bitcoin holders a special kind of confidence: that Bitcoin cannot be devalued by arbitrary monetary policy decisions, and that they will always be able to hold and transfer their Bitcoin freely. This could be valuable not just to individuals and companies but also to governments whose foreign currency reserves may be subject to the whims of foreign entities.
- **Universal:** Similar to physical bearer assets like US Dollar bills or gold, Bitcoin is a digital bearer asset that anyone can hold and transfer. The same is not true of digital US Dollars (which require a

bank account that supports US Dollars) or digital exposure to gold (which requires a brokerage account).

A broadly accepted store of value with the above features would represent a significant improvement over gold, but Bitcoin still lacks broad acceptance and remains nascent as a store of value (as compared to gold's millennia of history and credibility). A better product is not enough—Bitcoin must have a go-to-market strategy to reach broad acceptance.

Bitcoin as a Bubble

Since Bitcoin's inception, many intelligent investors have observed that it appears to be a bubble. They are more right than they know.

If we define a bubble asset as one that is overvalued relative to intrinsic value, then we can think of all monetary assets as bubble assets. By definition, a store of value is an intermediate asset that people demand, not for its direct utility, but for its ability to be valuable in the future. This value is reflexive: people will believe in a store of value if they expect others to believe in it (who in turn should expect others to believe in it, and so on).

This phenomenon is distinct from other asset classes, which have utility-based demand, with speculation occurring around this underlying utility. For monetary assets, the utility is in the collective speculation itself.

As Nobel-laureate Robert Shiller observes: "Gold is a bubble, but it's always been a bubble. It has some industrial uses, but basically it's like a fad that's lasted thousands of years." This is not an argument against gold (or Bitcoin) as a valuable monetary asset, but an astute insight into the bubble-like, reflexive nature of money.

We can think of money as a bubble that never pops (or that hasn't popped yet) and the value of fiat currency, gold, or Bitcoin as relying on collective belief. Other factors like a government's power, the industrial utility of gold, or the robustness of Bitcoin's codebase can help reinforce this belief, but belief is critical.

Such large amounts of value emerging from collective belief may seem circular and nonfundamental. However, there is real value in the social and economic coordination that monetary assets facilitate (much as there is real value in common language). Moreover, such collective belief cannot arise around any arbitrary asset—a successful monetary asset must compete to earn this belief based on intrinsic features. Having superior intrinsic features explains why gold is preferred to silver or fur pelts and Bitcoin is preferred to any number of Bitcoin copycats.

Bubbles as a Go-To-Market Strategy

If Bitcoin succeeds in becoming a trusted store of value, then its end state is to be a bubble. Bubbles are also how Bitcoin gains broader acceptance.

Throughout Bitcoin's 11-year history, there have been at least four Bitcoin bubbles of note.

- 2011: From ~\$1 (Apr 2011) to ~\$31 (Jun 2011) to ~\$2 (Nov 2011)
- 2013: From ~\$13 (Jan 2013) to ~\$266 (Apr 2013) to ~\$65 (Jul 2013)
- 2013-2015: From ~\$65 (Jul 2013) to ~\$1242 (Nov 2013) to ~\$200 (Jan 2015)
- 2017-2018: From ~\$1000 (Apr 2017) to ~\$19500 (Dec 2017) to ~\$3500 (Dec 2018)

Each bubble has a familiar pattern. High conviction investors start buying when Bitcoin is boring and unloved. The resulting rise in Bitcoin price attracts media attention, which then attracts investors (or speculators), many with lower conviction and shorter time horizons. This drives the price of Bitcoin higher, which drives further attention and investor interest. This cycle repeats until demand exhausts and the bubble crashes.

Although painful for those involved, each bubble leads to broader awareness and motivates Bitcoin's underlying adoption, gradually expanding the base of long-term holders who believe in Bitcoin's potential as a future store of value. This dynamic is evident in the successively higher price floors that Bitcoin reaches during times of maximum disillusionment: ~\$2 in 2011, ~\$200 in 2015, and ~\$3500 in 2018. Broader awareness also encourages the building of Bitcoin infrastructure by startups like Coinbase and incumbents like the CME and Fidelity, further improving Bitcoin's liquidity and utility as a monetary asset. Through successive bubbles, Bitcoin reaches greater levels of scale in users, transaction volumes, network security, and other fundamental metrics.

The Future of Bitcoin

As Bitcoin becomes more broadly accepted, what will its future look like? Some wonder whether people will be earning salaries or making everyday payments in Bitcoin. While these behaviors may exist to some degree, Bitcoin seems unlikely to challenge the US Dollar as the leading means of exchange and unit of account (at least anytime soon). Instead, Bitcoin is likely to earn a place alongside gold as a sensible part of many investment portfolios. This has already begun with an early-adopter, tech-forward crowd, and we expect it to grow to include a broader set of investors and institutions over time. Eventually, central banks may come to view Bitcoin as a complement to their existing gold holdings.

Ultimately, monetary assets rise and fall on timescales that stretch beyond human lifespans, making them a challenge to forecast. There was a time before the US Dollar reigned when the reserve currency was British, or French, or Dutch, or further into ancient history, Greek or Roman. Similarly, there was a time before the adoption of gold when more primitive forms of money were dominant. The idea of a fiat currency like the US Dollar being untethered to gold is itself a recent phenomenon that seemed unthinkable half a century ago. In the future, it seems likely that the global monetary order could change in ways that would be unthinkable to us today, with digital currencies such as Bitcoin playing a significant role.

Market Size

As a decentralized store of value, it is most natural to consider Bitcoin's market size relative to gold, whose aggregate value is estimated to be ~\$9T (May 2020) between central bank reserves (17%), private investment holdings (22%), jewelry (47%), and other miscellaneous forms (14%). Some but not all of this value is addressable by Bitcoin.

Over time, the market demand for assets like gold and Bitcoin could expand to exceed ~\$9T, especially given the prevailing direction of global monetary policy. According to the IMF, total international reserves reached ~\$13T in 2019 between gold (11%), foreign currency reserves (86%), and IMF-related assets (3%). If foreign governments (some of whom already bristle at their dependence on US Dollar FX reserves) begin to adopt Bitcoin as a complement to existing gold holdings, the market size for Bitcoin could expand significantly.

Beyond complementing gold's investment demand, Bitcoin may also address broader store of value markets indirectly. Consider, for example, people who hold fiat currencies with eroding credibility such as the Argentine Peso or the Turkish Lira, but who may have difficulty accessing US Dollars or gold. Or consider various collectibles like art or gemstones, some of which are owned primarily as stores of value. Or consider the empty NYC apartment that is owned by a foreigner interested in storing value outside his or her native country. Bitcoin could plausibly address subsets of these behaviors more effectively.

Deferring a precise estimate of market size, we believe it is clear that Bitcoin has significant headroom if it continues to gain broader acceptance.

Risks

Although it has come a long way in 11 years, many risks remain for Bitcoin:

- **Crossing the Chasm:** Bitcoin has gained credibility with early adopters, including some large institutional investors, but it remains niche relative to incumbent monetary assets like gold. There is risk that Bitcoin never achieves the broad acceptance that its proponents hope it will. Of course, therein also lies the opportunity. If Bitcoin were already a broadly accepted store of value, then it would likely be worth orders of magnitude more with relatively little remaining upside.
- **Volatility:** Bitcoin has been (and continues to be) quite volatile relative to US Dollars. There is risk that this volatility limits adoption or prevents investors from considering Bitcoin as a credible store of value. For better or worse, this volatility may be inherent to the process of Bitcoin adoption as natural swings in investor confidence (as faced by any early-stage upstart) are reflected in Bitcoin prices. Bitcoin's bubble-like adoption process exacerbates this effect. As Bitcoin matures and becomes more broadly accepted as a monetary asset akin to gold, investor confidence and Bitcoin prices should stabilize.
- **Regulation:** Bitcoin is a new currency and payment rail that sits outside of existing systems, posing a potential challenge to existing regulatory frameworks. Similar to early Internet regulation, there is hope that governments pursue nuanced regulation(s) that allow innovative use-cases to prevail. However, there is risk that regulation is onerous and ultimately hinders broader Bitcoin adoption. One mitigating factor is that Bitcoin is a global, decentralized network like the Internet, which is difficult to control for any single government, although governments can plausibly limit access to Bitcoin in various ways.
- **Technical Risk:** The Bitcoin codebase and network have been battle-tested for over a decade, but it continues to evolve and there remain some open questions about how the system might behave in the long run (for example, when the Bitcoin supply approaches its asymptote and miners must be compensated primarily with transaction fees rather than block rewards).

- **Competitive Risk:** Other cryptocurrencies could compete with Bitcoin, as could digital fiat currencies sponsored by governments. Relative to other cryptocurrencies, Bitcoin has a strong first-mover advantage in acceptance, security, and credibility that will be difficult for competitors to overcome. Relative to digital fiat currencies, Bitcoin remains differentiated in its scarce, gold-like nature. Digital US Dollars or digital Renminbi would still be subject to local monetary policy decisions, although they have the benefit that they are currency units people already know and use.
- **Unknown Unknowns:** We must acknowledge that a digital monetary asset such as Bitcoin has never existed before. We are in uncharted territory with more uncertainty than is typical.

Conclusion

Bitcoin is a new monetary asset that is climbing an adoption curve. Although it is not yet a broadly accepted store of value, Bitcoin has great potential as a future store of value based on its intrinsic features.

Since monetary assets do not arise frequently, Bitcoin is likely to challenge our ordinary intuitions, and it has stirred (understandable) controversy in the investment world.

Therein lies the opportunity, of course. We believe Bitcoin offers a compelling risk/reward profile for patient, long-term investors willing to spend the time to truly understand Bitcoin. We hope this paper provides a helpful starting point.

About the Author

Matt Huang is co-founder and Managing Partner at Paradigm. Previously, Matt was a partner at Sequoia Capital focusing on early-stage venture investments including leading the firm's cryptocurrency efforts. Matt was the founder and CEO of Hotspots, a YCombinator company acquired by Twitter in 2012, and angel investor in companies such as ByteDance and Instacart. He purchased his first Bitcoin from MtGox in 2012. Matt holds a B.S. in Mathematics from MIT.

Twitter: [@matthuang](https://twitter.com/matthuang) LinkedIn: [Matt Huang](https://www.linkedin.com/in/matthuang)

Acknowledgments

This paper benefited from the feedback and contributions of many:

- Fred Ehrsam, my partner and co-founder at Paradigm, and our colleagues Alana Palmedo, Arjun Balaji, Charlie Noyes, and Dan Robinson.
- Michael Abramson, Alfred Lin, and Kevin Kelly of Sequoia Capital. I'm grateful to them and the rest of my former colleagues at Sequoia Capital for their open-minded interest in Bitcoin circa 2014-2018.
- Wences Casares of Xapo, and member of the Board of Directors of Paypal and Libra
- Pete Briger and Michael Hourigan of Fortress Investment Group
- John Pfeffer of Pfeffer Capital, and formerly of KKR
- Micky Malka of Ribbit Capital

- Nick Shalek of Ribbit Capital, and formerly of the Yale Investments Office
- Steve Lee of Square Crypto, and contributor to Bitcoin Core development
- Peter Palmedo of Sun Valley Gold
- Tyler Cowen of George Mason University and Marginal Revolution

Important Disclosures

The content of this paper is provided for informational purposes only. Nothing herein constitutes investment, legal, or tax advice or recommendations. This paper should not be relied upon as a basis for making an investment decision and is not an offer to provide advisory services. It should not be assumed that any investment in the asset class described herein will be profitable and there can be no assurance that future events and market factors would lead to results similar to any historical results described in this paper. The asset discussed herein is not representative of all assets in which Paradigm invests. Any projections, estimates, forecasts, targets, prospects and/or opinions expressed in this paper are based on the subjective views of its author, are subject to change without notice and may differ or be contrary to views expressed by others. Certain information contained in this paper has been obtained from third-party sources. While such information is believed to be reliable for the purposes used herein, Paradigm has not independently verified such information and makes no representation or warranty, express or implied, as to the accuracy or completeness of the information contained herein.

Bitcoin Mining's Three Body Problem

By Leo Zhang on Anicca Research

Posted June 1, 2020

“越透明的东西越神秘，宇宙本身是透明的，只要目力能及，你想看多远就看多远，但越看越神秘。”——刘慈欣 《三体》

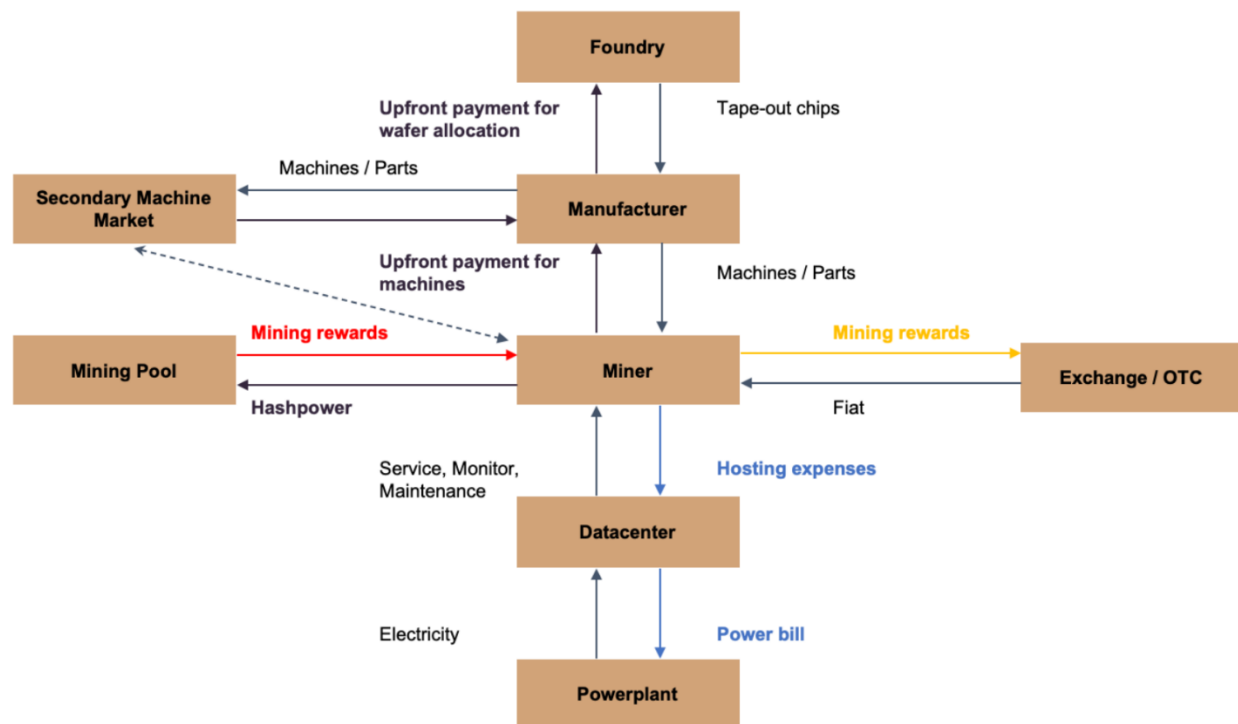
Bitcoin mining is a complex phenomenon that connects hardware and software, the energy and financial markets. Invisible rules govern every aspect of it. The performance of an individual operation is determined by various external factors that are often hard to quantify and almost impossible to forecast.

From a macro perspective, we can identify three principal forces that drive the mining industry as a whole: the emission schedule, the climate cycle, and hardware iteration. Each influences a different component in the miner's profit calculation:

Mining profit

= Mining Revenue - Mining Expenses

= (Block Reward + Fees) * Price * the Miner's hashrate / global hashrate - (Electricity Expense + Hardware Depreciation)



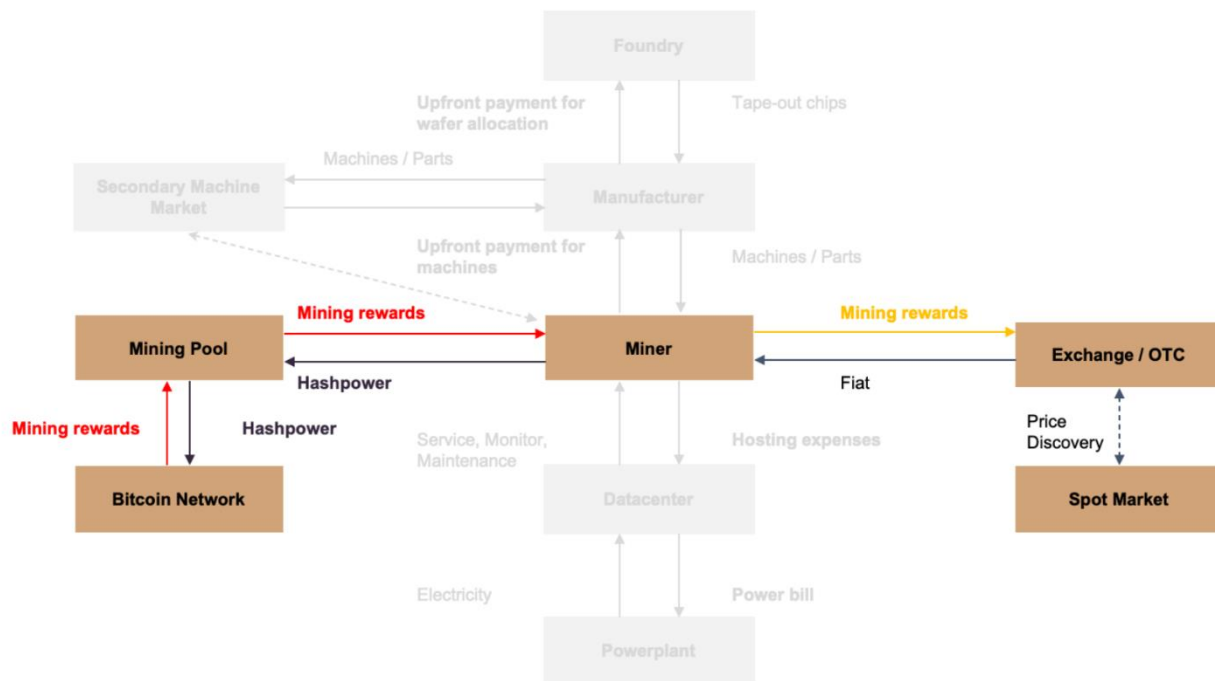
- **The emission schedule** drives block reward (revenue).

- ***The climate cycle*** indirectly drives the industry-average electricity expense (operating expense).
- ***The hardware iteration*** drives the miner's hashrate, energy efficiency, as well as hardware depreciation (capital expenditure).

When the first halving occurred in 2012 most people were mining with PCs and GPU rigs at home. Distribution of hashpower was scattered around the world. The dominant force in the market was just the block reward decrease. As the mining cost-of-production doubled, a noticeable amount of hashpower dropped and temporarily switched to the more profitable Litecoin. By the time the second halving took place in 2016, commercial ASICs were already available and industrial mining facilities were put in business.

Long before the third halving transpired in this May, market commentators engaged in heated discussions on possible outcomes. Some echoed that the price will grow exponentially due to the supply shock. Others speculated that 20-30% of the network hashrate would disappear. Because the timing of the halving block overlaps with a transition in the climate cycle and hardware upgrade from 16nm to 8/7nm, all three forces were moving in conjunction.

The Emission Schedule



Bitcoin is the product of hashpower. The industry wouldn't exist without incentivizing miners to continuously invest in hardware and burning electricity to augment Bitcoin network's settlement assurance. In absence of a vibrant blockspace market, the block rewards are their primary source of revenue. Over the years, the value of the rewards has significantly grown due to Bitcoin price appreciation, which in turn nurtured the mining business into a billion-dollar industry.

![[2020 June-December implied rewards based on 6.25BTC per block and Jan-May price. (Source: [blockchain.info](https://assets/images/2020/m6/lz3.png))](/assets/images/2020/m6/lz3.png) _ 2020 June-December implied rewards based on 6.25BTC per block and Jan-May price._ (Source: blockchain.info)

Unlike most physical commodities, Bitcoin has a well-defined quadrennial emission reduction schedule mandated by its protocol. Everyday a fixed supply of new coins gets created, and a varying percentage of that gets redistributed to the rest of the Bitcoin economy. Since miners are the only natural suppliers of Bitcoin, and the largest cohort of consistent sellers, profit margin is a key factor in determining the supply side dynamic.

Intuitively, reducing block reward by half immediately doubles every participants' cost-of-production. Some older generation machines may become too inefficient to operate. Consolidations tend to happen during these times. Miners with access to competitive power sources will purchase these machines in bulk at dirt cheap price, and the machine secondary market becomes far more active.

A miner is a bi-variate call option in physical form. The complexity in pricing and difficulty in transporting goods makes the machine secondary market opaque, illiquid, and highly reliant on insiders. But the poor price discovery at times brings great arbitrage opportunities for resourceful miners. For instance, in late 2018 Bitcoin price experienced a steep decline down to the \$3,000 level. A noticeable percentage of the hashpower dropped, spawning a wave of *"mining death spiral"* headlines. Some miners were able to scoop up large quantities of the Antminer S9s that were temporarily flushed out. In just four months, Bitcoin price propelled into a frenzy bull market. Not only have these buyers made a handsome profit off of the coins they mined, the resale value of the machines also increased by 3x. This demonstrates that unprofitable hardware still have option value.

Machine price is as volatile as miners' daily revenue



(Source: proprietary data, courtesy of Jinping Gou)

These consolidation activities change the hardware market composition. The market composition tells us how much energy the overall mining activities are consuming. There are a lot of naive attempts at calculating a "price floor" at which miners would stop selling. Every miner's entry time, amount of capital, cost basis, and risk tolerance is different, hence the industry-wide cost-basis is actually a very wide spectrum. Nonetheless, there will be selling at every level. To assess the entire network's selling pressure,

we need to understand the exact composition of machines. This data is rather challenging to collect since no single party in the industry has access to the entire transaction flow of machines and their energy cost. The *Blockware* team is one of the latest to try to do this by surveying individual facilities. In the halving opus published in March, they estimate network's hardware composition as the following:

Layer	Electricity Rate (kWh)	S9 Percentage of Network	S17 Percentage of Network	Total Percentage of Network	S9 Shutoff: BTC Breakeven Price	S17 Shutoff: BTC Breakeven Price
1	Below \$0.025	4.50%	0.50%	5.00%	\$ 2,568	\$ 982
2	\$0.030	5.63%	1.88%	7.50%	\$ 3,852	\$ 1,473
3	\$0.040	9.75%	5.25%	15.00%	\$ 5,136	\$ 1,964
4	\$0.050	7.50%	7.50%	15.00%	\$ 6,420	\$ 2,455
5	\$0.055	6.00%	14.00%	20.00%	\$ 7,062	\$ 2,700
6	\$0.060	3.00%	12.00%	15.00%	\$ 7,704	\$ 2,945
7	\$0.065	1.25%	11.25%	12.50%	\$ 8,346	\$ 3,191
8	Above \$0.07	1.00%	9.00%	10.00%	\$ 9,631	\$ 3,682

Next Gen. Mining Rigs Keep High Electricity Rate Miners Competitive:
A Layer 8 Miner (\$0.075 Electricity Rate) running S17's has a lower Bitcoin Breakeven Price than a Layer 2 Miner (\$0.03 Electricity Rate) running S9's. The S17 Layer 8 Miner is better positioned to survive and mine for the long-term than the S9 Layer 2 Miner.

Source: Understanding Bitcoin Market Participants - Vulnerabilities in the Price of Bitcoin Driven by Miners

Post-halving the network hashrate dropped to ~94 EH/s from the ~109 EH/s level in March. Assuming all machines that left the network were the S9s in the bottom categories, we can update the composition table:

![*Antminer S9i specs (13.5TH/s, 1,310W) at \$21 per unit. Antminer S17+ specs (70TH/s, 2,800W) at \$1,232 per unit. *Linear depreciating over 18 months for S9i, and 36 months for S17+.](/assets/images/2020/m6/lz6.png) _Antminer S9i specs (13.5TH/s, 1,310W) at \$21 per unit. Antminer S17+ specs (70TH/s, 2,800W) at \$1,232 per unit._ **Linear depreciating over 18 months for S9i, and 36 months for S17+.

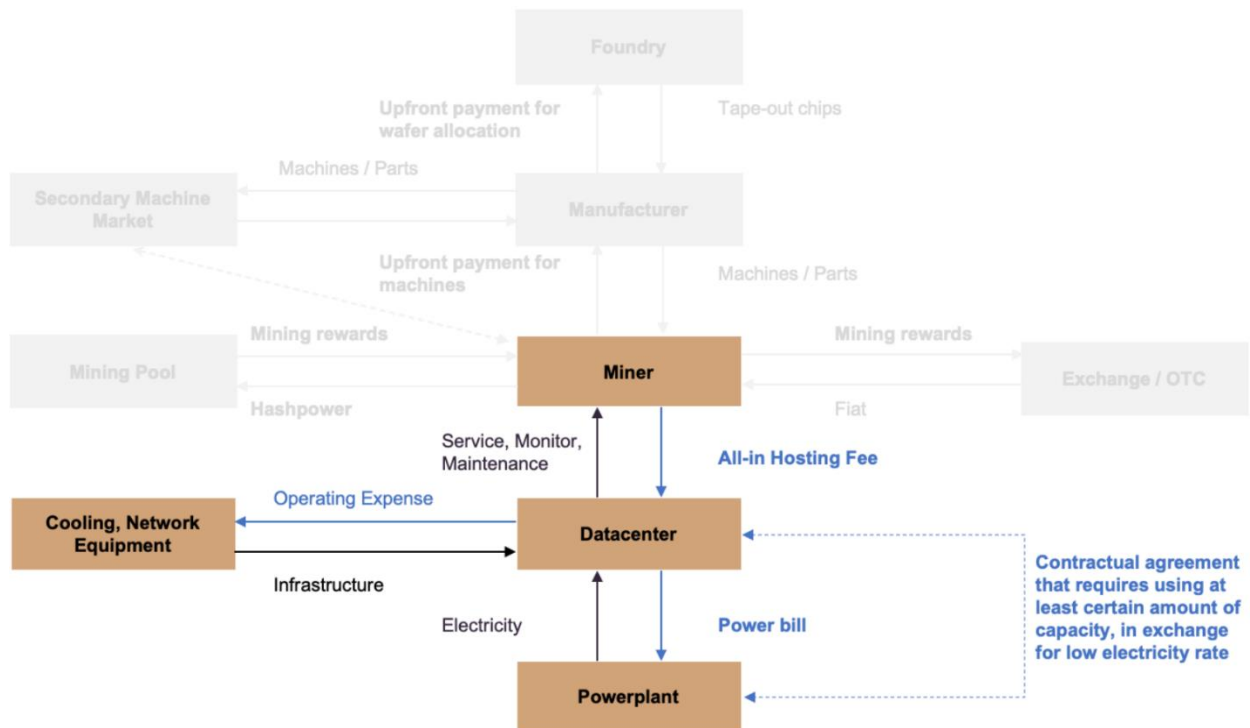
Using the data above, we can calculate a rough weighted-average selling pressure at various price levels, as a percentage of the global daily trading volume:

![Showing a relatively tight price range since global trading volume changes greatly as price moves. *6.25 BTC per block. Transaction fees not included. *Global trading volume of \$1.14Bn on Bitwise.](/assets/images/2020/m6/lz7.png) _Showing a relatively tight price range since global trading volume changes greatly as price moves._ _6.25 BTC per block. Transaction fees not included._ **Global trading volume of \$1.14Bn on Bitwise.

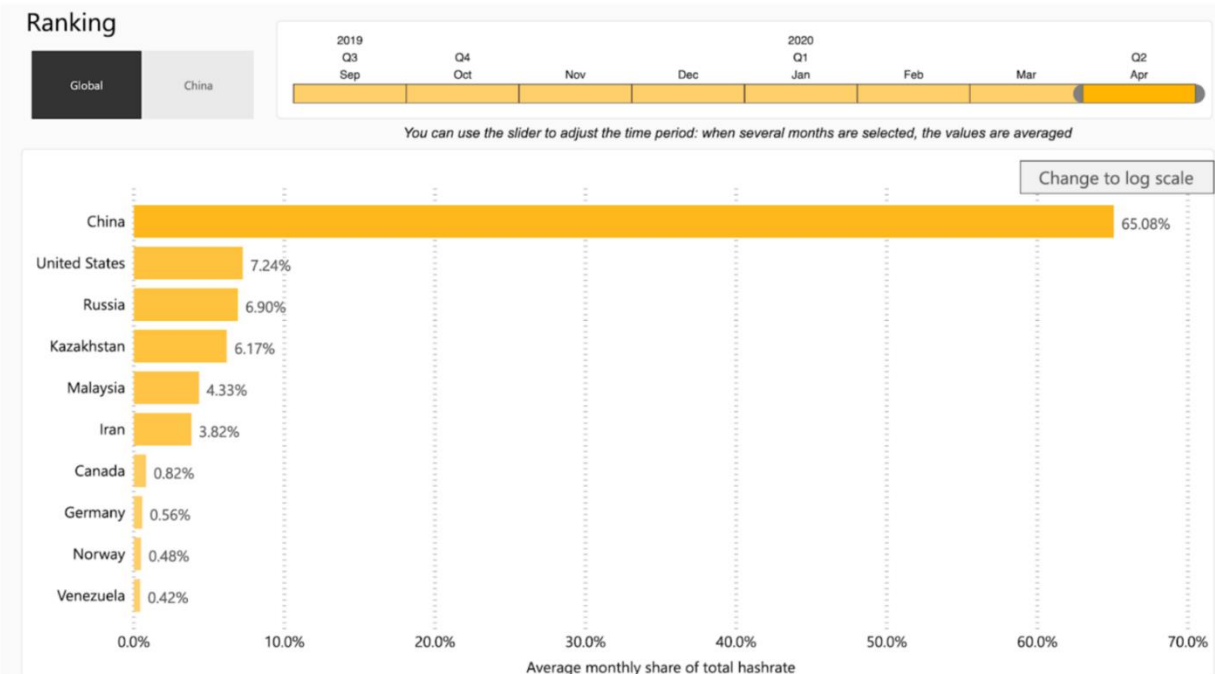
Note that this analysis is for illustrative purposes only. Here all old generation machines are represented by S9 and new generation machines by S17. Needless to say, miners purchase machines from multiple manufacturers, and same generation machines from different manufacturers have very different specs. In reality the variance of market composition is much larger. In addition, this analysis is a static snapshot. Hardware composition is highly fluid, machines are actively switching hands as the market seeks a new post-halving equilibrium. The upcoming flood season in Sichuan also has a drastic impact on a majority of the miners' electricity cost. As more miners employ financial instruments such as collateralize lending, futures, or even hashpower markets, the network's miner selling pressure will be partially mitigated or delayed.

A takeaway from observing how the mining composition evolves over time is that hashpower is “not fungible”, in other word, **every unit of hashpower is unique**. One TH/s of hashpower today is produced at a different cost-basis from that of yesterday.

The Climate Cycle



The Climate Cycle is the byproduct of the geographical concentration of mining operations. Over the years, the Bitcoin mining industry inadvertently benefited from a massive over-investment in hydropower in southwest China. Excess cheap electricity, massive power capacity, cheap labor cost, and physical proximity to manufacturers make it an ideal location for mining. It is estimated that over 65% of the world's hashpower is concentrated in these provinces.



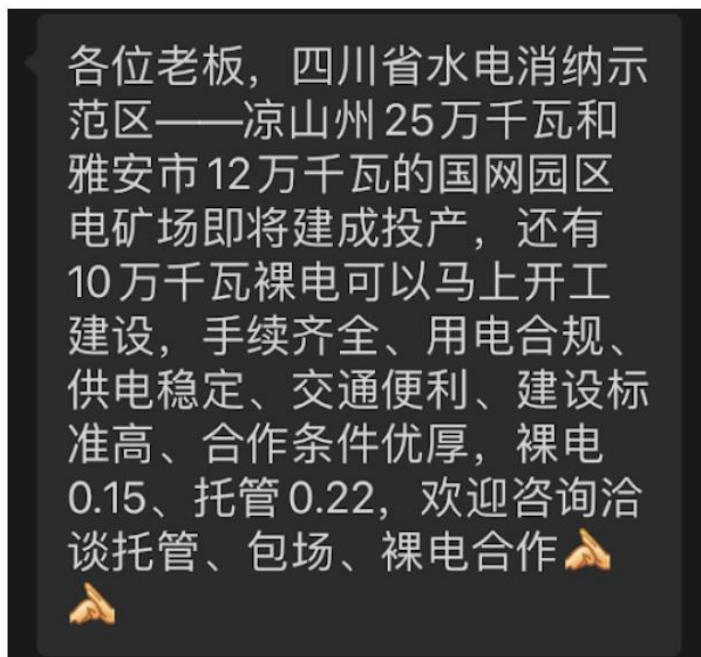
(Source: *Bitcoin Mining Map, Cambridge Centre for Alternative Finance*)

May-October is the flood season in Southwest China. It is also a festival period for mining businesses as the large supply of surplus hydro capacity significantly cuts down miners' operating expenses. For small-medium scale miners, the flood season can reduce the cost by as much as 40%. For large miners who own proprietary facilities, the flood season electricity cost is practically negligible. Over 80% of the miners in Xinjiang, Inner Mongolia will migrate in flocks to Sichuan, Yunnan, and Guizhou to take advantage of the discount, and they move back or sell their equipment after the dry season arrives in November.

The thriving mining industry is a boon to the local power plants business. Many converted or constructed their facilities into data centers to host miners.

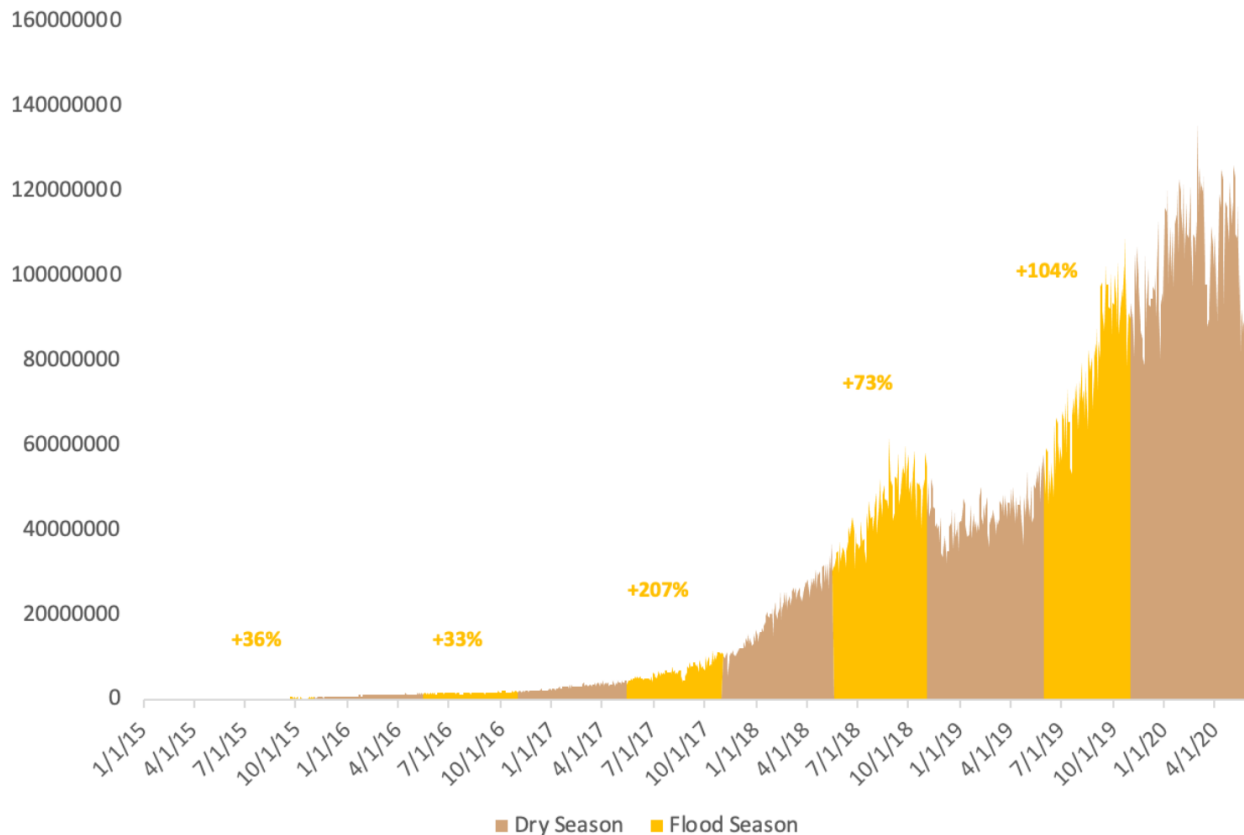
Example of hosting ads in Sichuan hydropower zone. Rough translation:
 "(...)100 MW capacity can start construction immediately (...) Bare electricity 0.15 RMB per Kwh, all-in 0.22 RMB per Kwh"
 (Source: Wechat group)

Gradually, the industry structured itself around these climate patterns. Like ancient rituals, every year before the flood season arrives, major mining conferences get organized in Sichuan's capital Chengdu. Some facilities are only open to external



customers during the flood season. Manufacturers plan their new product release right before it arrives. Miners race to source the latest and greatest machines in bulk.

Hashrate growth during flood seasons:



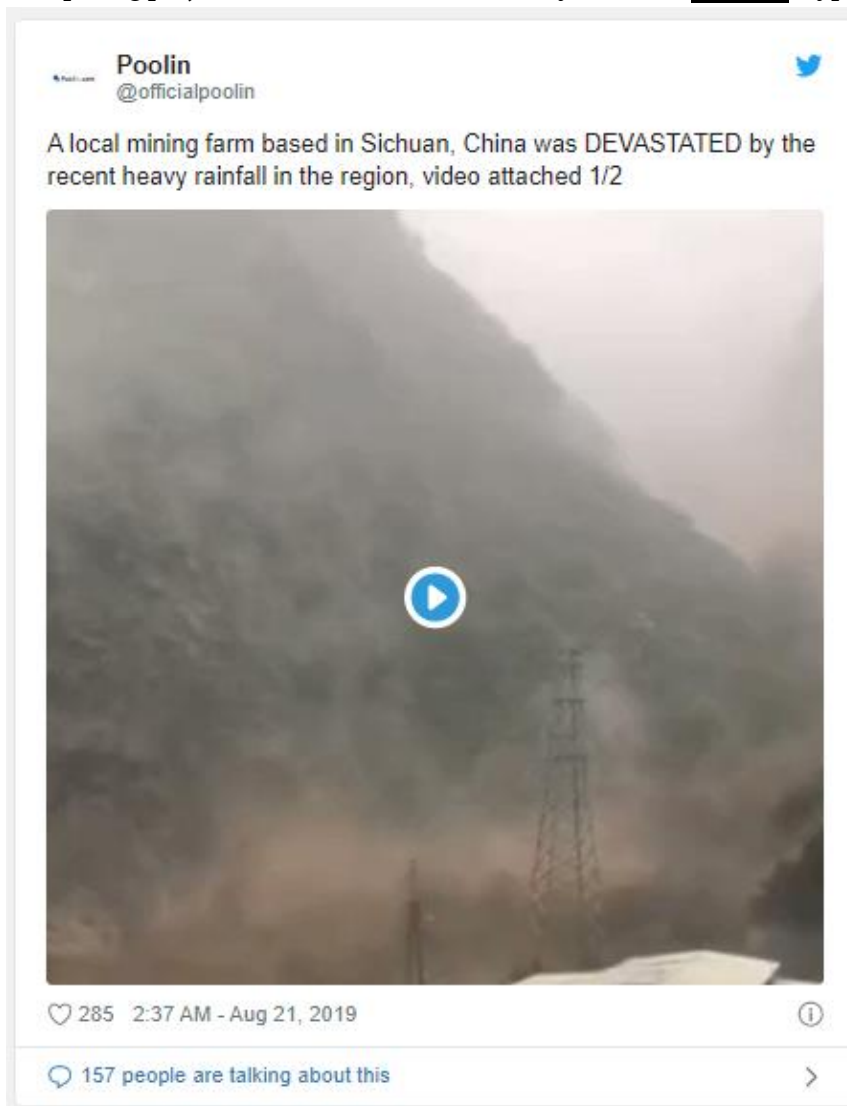
(Source: coinmetrics.io)

At the beginning of 2020, due to general macro uncertainties, investors and miners reverted to a mode of cautious response. The production of new machines temporarily halted due to supply chain shock from COVID. After the Halving, more machines left the network, leaving the supply of hosting capacity greater than the demand. Many facilities in Sichuan and Yunnan areas are having trouble finding clients. Their desperation further reduces average electricity prices. Compared to last year's 0.24-0.26 RMB / KWh all-in cost, this year's average can be as low as 0.10-0.20 RMB / KWh.

The impact from block reward halving will be partially absorbed by the lower power cost. Many facilities had to sign contracts with power plants that promise a minimum usage of electricity. In order to attract business, some of them are offering "joint-mining" programs, where the miners pay de minimis monthly cost, and split the mining revenue with the facility owner. Effectively transferring part of the market risks to the hosts themselves.

However, this doesn't mean low operating expense is absolutely guaranteed. While hydropower facilities are cheaper during the flood season, they are generally located in extremely remote areas. The power supply and internet connectivity may not be as stable. Sometimes they even risk getting flooded:

Another risk is that local government policies change from time to time. Prior to 2018, most of the local officials had no clue what mining is. The facilities report their activity as data centers for big data or cloud computing projects. In 2018 a committee led by the PBoC dictated cryptocurrency mining as a “false



innovation”, citing that mining is extremely wasteful and must “cease in orderly fashion”. Some mining operations did indeed shut down under the pressure. But in late 2019, the National Development and Reform Commission (NDRC) removed mining from a list of activities to be eliminated. Note that the NDRC also oversees the energy industry. Massive amounts of hydropower squandered during flood season is a longstanding issue. The officials are beginning to realize that Bitcoin mining is a highly effective way of transforming excess local capacity into a global digital commodity.

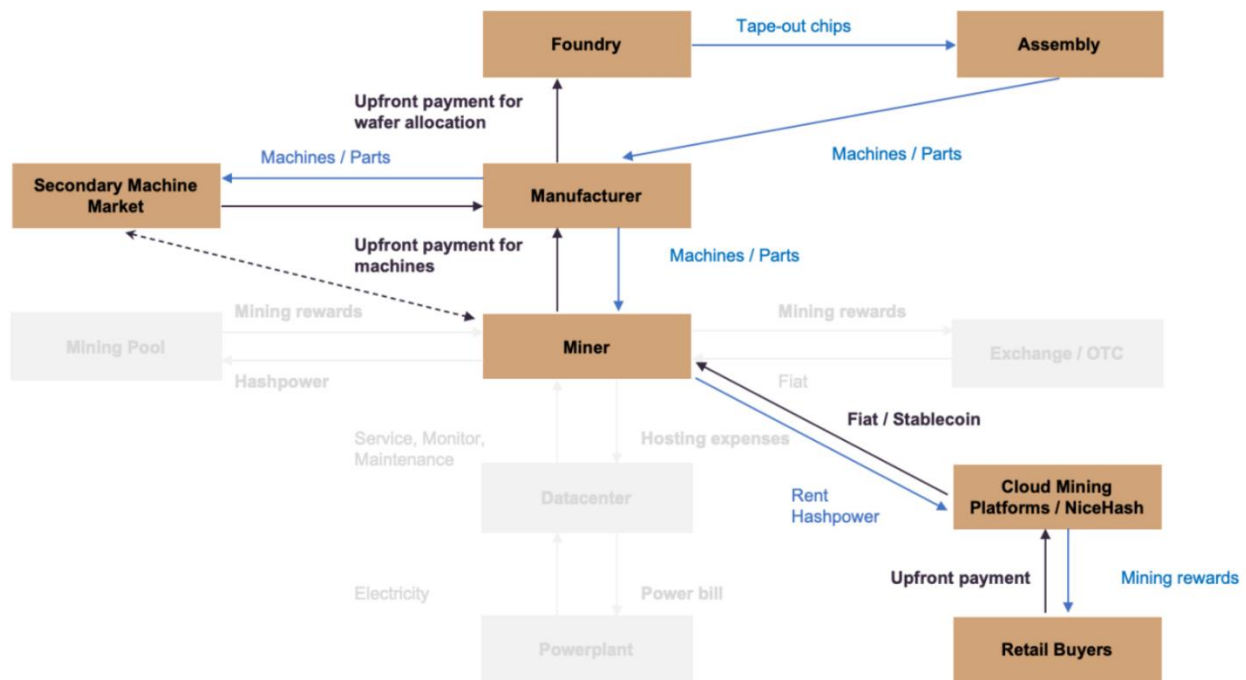
A few months ago, some cities in Sichuan announced a joint-venture program called “Hydropower Consumption Demonstration Zones” to

support the development of the “blockchain industry”. Unfortunately, despite more facilities opened for business, this year’s rain volume hasn’t been as great as expected. At the time of writing, electricity generated by hydropower plants is being transferred to other parts of Sichuan for residential use as the summer heat kicks in.

Last week, a county in Sichuan issued another notice that orders hydro power plants to halt accepting mining businesses. Although insiders on the ground do not expect the order to be enforced, it shows the complexity of the flood season energy scene. **It’s not a magic switch that turns on and off to immediately cut down miners’ electricity bills.**

The Climate Cycle is a rather unique phenomenon during this stage of cryptocurrency mining. If mining operations migrate to more diverse locations in the future and become less concentrated on a single power source, this cycle will cease to play such a significant role.

Hardware Iteration



Manufacturers are constantly in an arms race to produce the leading product. For a long time Bitmain's Antminer S9 dominated the market. According to the [IPO documents](#) the company filed in 2018, Bitmain machines occupied ~74.5% of the ASICs on the market. But in the past two years, competitors such as MicroBT's Whatsminer and Canaan's Avalon are rapidly eating into Bitmain's market share.

In 2017, Whatsminer sales accounted for ~7.2% of the network hashrate. In 2018, ~9%, and in 2019, ~35%. The shoebox miners are commodity products. While there are qualitative factors that can help a manufacturer stand out, such as customer service, delivery time, and supply chain management etc., the competition forces manufacturers to relentlessly focus on two key metrics: **unit price and efficiency**.

The efficiency is measured by Joule per Th/s. The lower the metrics is, the less energy it consumes to compute a hash function. Each generation of mining hardware is defined by its improvement in efficiency.

![*As of May 31th, 2020 *Based on 6.25 BTC block reward, 15,138,043,247,082 difficulty, \$9,500 BTC price](/assets/images/2020/m6/lz14.png) _As of May 31th, 2020_ **Based on 6.25 BTC block reward, 15,138,043,247,082 difficulty, \$9,500 BTC price

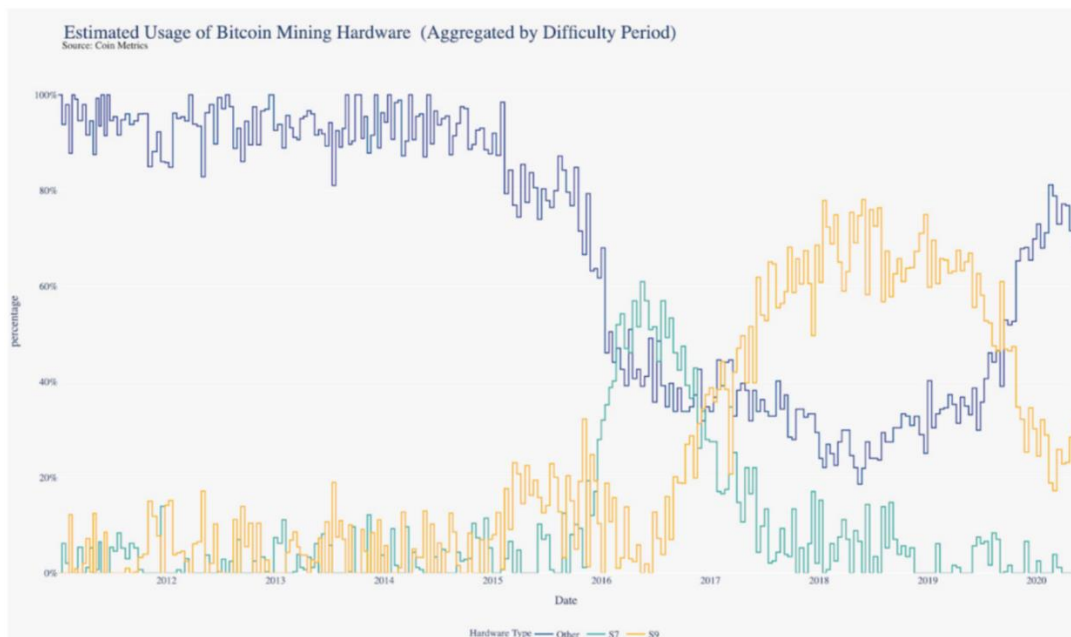
Improvement in machine efficiency has a significant impact on earnings. Using the current Bitcoin difficulty, and average price of an used Antminer S9i (\$21 per machine, 97.0J per TH/s), we can calculate the approximate **days to breakeven** at various price levels:

Electricity Price per KWh									
	\$ 0.025	\$ 0.030	\$ 0.040	\$ 0.050	\$ 0.055	\$ 0.060	\$ 0.065	\$ 0.070	\$ 0.080
\$ 4,750	Never	Never	Never	Never	Never	Never	Never	Never	Never
\$ 6,650	421	Never	Never	Never	Never	Never	Never	Never	Never
\$ 8,075	94	293	Never	Never	Never	Never	Never	Never	Never
\$ 9,025	62	112	Never	Never	Never	Never	Never	Never	Never
\$ 9,500	53	85	Never	Never	Never	Never	Never	Never	Never
\$ 9,975	46	69	Never	Never	Never	Never	Never	Never	Never
\$ 10,925	37	50	183	Never	Never	Never	Never	Never	Never
\$ 12,350	28	36	73	Never	Never	Never	Never	Never	Never
\$ 14,250	22	26	40	97	333	Never	Never	Never	Never

The **number of days** to breakeven of a new Antminer S19 Pro (\$2,407 per machine, 29.5J per TH/s) :

Electricity Price per KWh									
	\$ 0.025	\$ 0.030	\$ 0.040	\$ 0.050	\$ 0.055	\$ 0.060	\$ 0.065	\$ 0.070	\$ 0.080
\$ 4,750	824	950	1371	2463	4093	12114	Never	Never	Never
\$ 6,650	494	537	650	823	949	1121	1370	1759	4082
\$ 8,075	380	405	466	549	603	667	748	851	1174
\$ 9,025	330	348	392	449	485	526	574	633	796
\$ 9,500	309	325	364	412	441	475	515	561	686
\$ 9,975	291	305	339	380	405	434	466	504	602
\$ 10,925	261	272	298	330	348	369	392	419	484
\$ 12,350	225	234	253	275	288	302	317	334	375
\$ 14,250	191	197	210	225	233	243	252	263	288

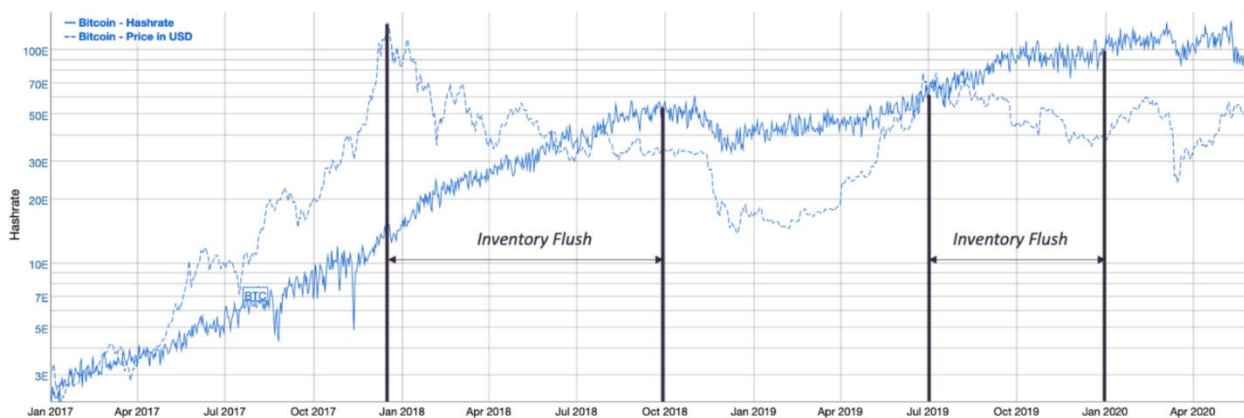
Under most circumstances, S9s are not profitable, but miners with access to extremely cheap power can still operate them at a profit. Comparing the two tables above, we can see at sub \$0.04 / KWh, it is faster for the miner to breakeven on S9. Thanks to cheap power sources, machines don't necessarily retire right away when the new generation hits the market. The team at *Coinmetrics* put together an estimated usage of Antminer S7 vs. S9 over time based on nonce distribution. As we can see, Antminer S7 usage doesn't just monotonically decline with the popularization of the S9s:



(Source: Coinmetrics' state of the network: Issue 51)

As discussed in **The Emission Schedule** section, resourceful miners can strategically take advantage of older generation machines. Such arbitrage opportunities usually appear when hashrate is relatively high and Bitcoin price relatively low. Although the value of hashpower is largely dependent on Bitcoin price, there is a disparity between hashrate and price due to the hardware market's delayed reaction to movements in the financial market. Manufacturing customized chips incurs non-recurring engineering costs. The miner manufacturer and its supply chain partners amortize expenses over the number of chips manufactured. In many cases the foundry requires the manufacturer to pay in full-upfront for a wafer reserve order, unless the manufacturer is a long-term client with massive orders.

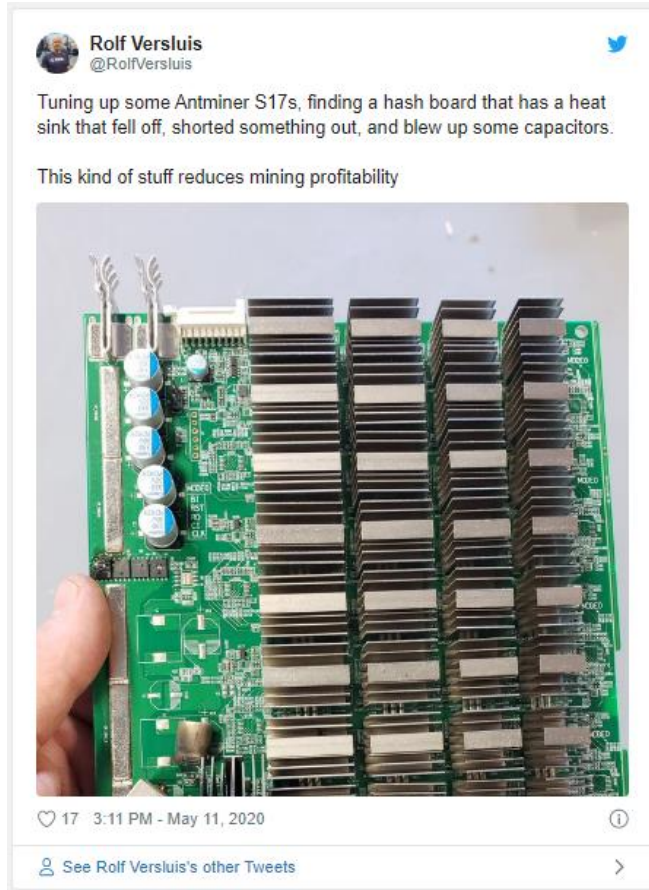
The cycle time of a wafer order is typically 12-13 weeks. The time gap makes it extremely challenging for manufacturers to make forward-thinking business plans. In late 2017, many manufacturers didn't have enough inventory to sell to the market during the bull market, and subsequently misjudged how much longer the market was going to rally. The manufacturers (including Nvidia), over-estimated the amount of orders in 2018, and had to gradually sell inventory at a loss during the second half of the year.



(Source: [Bitinfochart](#))

Once the market finishes upgrading from 16nm to 7nm machines, the backend process arms race will stop for a long time. The average lifetime of the new machines is prolonged from the previous 2 years to 3-4 years. Failure rate of equipment becomes significantly more important. In practice, it will be considered one of the key valuation metrics, along with unit price and efficiency.

Frequent mechanical failures decrease the miner's hash output, and quickly build up the maintenance expense long after warranty ends. High failure means upkeep will eat into a significant % of the revenue. For instance, the Antminer S17 series has a ~30% failure rate due to low quality thermo design. The heat sinks easily collapse on neighboring heat sinks and short-circuit the entire hashing board. This issue is



rather expensive to fix, and hence making the S17s a terrible product despite it is based on an advanced backend process.

Advanced machines means higher upfront capital expenditure, which in turn pushes mining to industrialize even more. Soon more data centers will customize their infrastructure to tailor mining-specific requirements. Flare gas mining, immersion cooling, and in-house monitoring solutions are starting to emerge.

In the meantime, should we be concerned that industrialization will further centralize the mining game? Hardware manufacturing is a reproduction process that actively eliminates the need for genetic mutation. At its current state, it benefits from standardization and centralized management. Industrialization is unstoppable in mining. Decentralizing mining is better focused downstream on the distributing ownership of hashpower voting, such as Stratum v2.

After a decade of barbaric growth, the mining industry is at crossroads. The entanglement of the three forces produces unpredictable short-term variances, but over the long-term as Bitcoin integrates deeper and wider with the rest of the economy, mining will become more competitive and resource-intensive. In the past miners only needed to focus on keeping expenses as low as possible. Going forward, the thinning profit margin will force the miners to be more conscious about cash flow and risk management. Two major trends will shape the industry in the future: **industrialization** and **financialization**.

Anarchy and Monarchy: A Natural State

By **Yuri de Gaia**

Posted May 1, 2020

What can be further apart from each other than Anarchy and Monarchy? In this article, I argue that these concepts are not only mutually exclusive, but complimentary.

When I discovered Bitcoin in late 2012, the event sent me on a fantastic journey of a lifetime. Not only did I learn about money, but I also studied the ways current political regimes operate in the world. I cannot say I have become an initiate in political science, but the limited knowledge I have, combined with an intuitive understanding of certain principles of Nature, led me to believe that we are terribly off course.



This is one of the reasons that made me write How to Scam the Planet,

Part 2: Democracy. However, it is mostly an exposé of the shortcomings of a particular mode of government that is widespread today. I did not offer a solution to the problem, nor may I provide a concrete one in this article. But this time, I will attempt to bring the issue closer to home.

Anarchy

In the natural course of my becoming, Bitcoin opened my eyes on many issues that persist today in the world. Besides the utterly fraudulent monetary system, there was another big discovery. Although it is connected with and affected by money, it certainly deserves an independent exploration. The issue is that of Government.

You can imagine the journey of a young, easily impressionable guy in his mid-twenties:

1. It looks like Government is not what it seems;
2. Government is cancer;
3. We must abolish all Government.

Thus came about my acquaintance with Anarchy, followed by the the study of its political implementation, Anarchism. From Merriam-Webster:

Anarchism : a political theory holding all forms of governmental authority to be unnecessary and undesirable and advocating a society based on voluntary cooperation and free association of individuals and groups.

As emotions reigned over reason at the time, I quickly attached a label to myself: an *Anarchist*. It was a time of pride and mental satisfaction. How could it not be? After all, I had swallowed the red pill and learned about the Matrix, while the rest of the world were asleep! I was a black sheep among the *sheeple*!

It was not long before I realized that even among anarchists there were constant infightings as to what Anarchy actually is. To some, it was just soft *libertarianism*, to others—*classical liberalism*, yet some others proclaimed the ultimate goal of a *stateless society*. Even though I leaned towards the latter, there were disagreements as to how that type of society would be managed. A free market? A communist utopia? A mixture of the two?



Flavours of anarchism

Delving into Austrian economics at the same time, my choice was clear: the world must rid of the State, and all the human relations must be voluntary and based on the principles of *laissez-faire* markets! My label got an upgrade: an *Anarcho-Capitalist*, also known as *Voluntaryist* (the black-and-yellow section in the circle).

Did it end there, though? It did not. I am a person who engages in constant refinement of character and knowledge. A lifelong process! “Change” is my middle name. To me, it is natural. Because if change ever stops, it means I have learned everything there is to know, perfected every area of my earthly life. Impossible.

How have I upgraded my knowledge to date?

Hierarchy

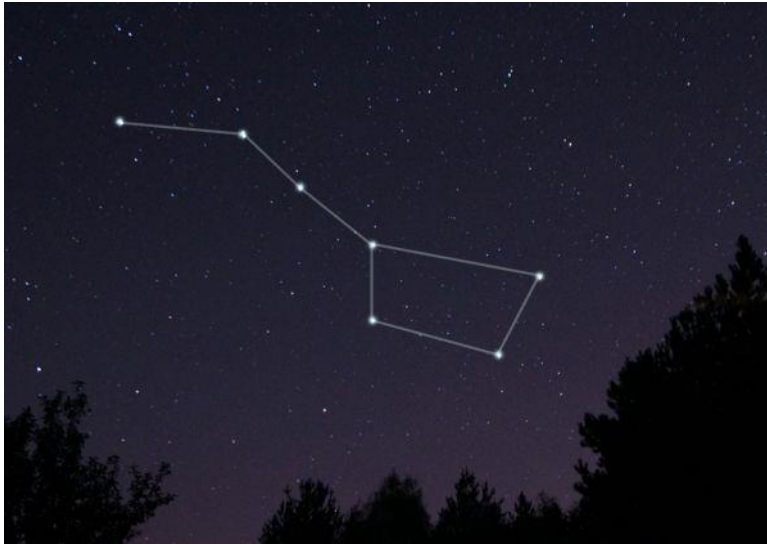
As I went deeper into the study of Nature (including human nature), political affairs and economic relationships, the realization dawned upon me that I was quite naive in my thinking. Not a rare occurrence, if you ask me!

At first, I believed that anarcho-capitalism meant not just the absence of Government, with capital G, but of any form of government whatsoever. Big, medium, small, unlimited or limited. But the study of the workings of Nature clearly reveals certain truths to the questioning mind:

- Everything in the Universe tends to self-organize;
- Hierarchy is natural order.

Let me cover both.

Spontaneous Order



the Cosmos, we conceive orderly patterns, such as constellations.

But Nature does not need the human mind to help her order things. It is what she does in her eternal dance of Becoming.



more often used for physical changes and biological processes, while “spontaneous order” is typically used to describe the emergence of various kinds of social orders from a combination of self-interested individuals who are not intentionally trying to create order through planning.”—[Wikipedia](#)

In economics, the phenomenon has been treated by many scholars, but the most famous example is that of *the invisible hand* introduced by the father of the science, Adam Smith.

“By preferring the support of domestick to that of foreign industry, he intends only his own security; and by directing that industry in such a manner as its produce may be of the greatest value, he intends only his own gain, and he is in this, as in many other cases, led by an invisible hand to promote an end which was no part of his intention. Nor is it always the worse for the society that it was no part of it. By pursuing his own interest he frequently promotes that of the society more effectually than when he really intends to promote it.”—Adam Smith, *The Wealth of Nations*

While the world seems like a chaotic place, one must understand the relationship between Chaos and Order. Our human mind likes to differentiate things because it makes it easier to fathom certain concepts. However, the reality is that Chaos and Order are one and the same thing, only with different degrees of such differentiation. The latter is simply part of and flows from the former.

The illustration below makes it more apparent. Out of the seeming Chaos of

Metaphysics aside, let us take a look at the concept of *spontaneous order*. Wikipedia can help with the term:

“Spontaneous order, also named self-organization in the hard sciences, is the spontaneous emergence of order out of seeming chaos. It is a process in social networks including economics, though the term “self-organization” is

When there is no centralized plan of action, no clear rules or guidelines, people tend to organize naturally to keep themselves safe and sound as well as make social interactions pleasant (despite what The Purge portrays). Anti-social behaviour is quickly shunned, and such individuals are ousted. A great example is provided in the video below that shows how, absent a functional traffic light, individuals tend to self-organize.

Suddenly, road rage is gone; drivers become more attentive and aware of their surroundings; polite gestures are the norm; eye-contact increases. Indeed, excessive traffic control is but one example in which, for the sake of safety, too many restrictions create more problems than what a naturally occurring order would achieve. As Justin Quinn rightly affirms in The Praxeology and Ethics of Traffic Lights:

“What this also demonstrates is yet another example of how government decivilizes people. The Austrolibertarian is aware of a plethora of government interventions into the free conduct of human beings, done in the name of safety, that either make us all less safe or simply create more daily annoyances.”

But does it mean that if we suddenly cancel all laws, regulations and rules, a beautiful lawless utopia will come about, with people dancing euphorically in circles and singing *kumbaya*?

Hierarchy as Natural Order

As mentioned, humans tend to self-organize if there are no clear rules. On what principle is such organization based? The answer is simple and natural: *inequality*.

Due to the characteristics of matter, there is no and cannot be such a thing as *equality*. Matter is variable, highly plastic, so even seemingly identical twins are different. Whoever perpetuates the myth of equality is either an ignoramus or a dangerous liar with malicious intent.

Just like in the animal kingdom, a faster cheetah has a higher chance of survival and procreation, Man also possesses an array of qualities that make or break certain aspects of his life. Physical characteristics and mental aptitude are the main differentiators. A taller man is a better basketball player by default; a smarter man has a higher chance of business success. This inequality makes the playing field uneven, with better performers finding themselves in higher positions. Even two physically and mentally identical individuals may have differing levels of success in life due to one of them possessing a stronger resolve to level up and the other one being lazy. *This is a law of Nature, and there is nothing you can do about it.*

As a result of this Law, *hierarchy* is inevitable. Someone will always be at the top, and someone at the bottom. This natural order of things can be seen throughout history in every corner of the Earth, at every level of society. The father is usually a family's decision maker, with the wife and the children being followers. A village has elders, old and wise men and women, whom the rest view in high regard. Even a circle of friends often has an unproclaimed leader. When such relationships are formalized, we get governments, companies, non-profit organizations, religions, cults.

I cannot speak precisely about the distribution of inequality in society due to my ignorance of statistics, but it would not be wrong to state that the vast majority of the population are followers and very few are leaders; most people are poor or in a fair financial situation while a small minority are truly rich; there are a lot of lazy individuals and very few men of action, and so on. Moreover, such conditions are natural. It is true that, in some cases, especially when it comes to monetary wealth, things could be a lot better absent certain factors, but the tip of the scale would not be turned against natural order.

So, how do we reconcile the two themes of this article: Anarchy and Hierarchy?

A World of a Thousand Kingdoms

Ancapistan

My initial naive assertion about Anarchy was that the ideal anarcho-capitalist world is a stateless world in which all human relations are voluntary and contractual. Money and reputation rule; there are no kings, princes, presidents or Soviets to decide on public matters. All the landmass is divided among private individuals, and all the services are provided by private contractors. Everybody is responsible for his life and actions. *Praxaology*, you see. If this sounds like a wonderful utopia, there is a reason for that: it is.

The utopian world of Ancapistan, as described above, ignores the very basic Law of Nature—that of Hierarchy and Order. It treats well another natural law, however, the Law of Cause and Effect (praxaology), but you cannot nitpick to fit your narrative. This makes you ignorant at best and malicious at worst.

Are we stuck with the current State then?

The State, Reimagined

The current State apparatus is overrun by parasitic redistributors of resources. These Parasites (marxists, communists, socialists, rent-seekers, etc) are the reason why the structure of the State has become akin to cancer: its deadly cells grow out of proportion and contaminate the healthy tissues of the society's body until the organs responsible for basic life support are no longer functional.

By changing a few elements, however, the cancer may fall into remission.

The **first element** is *the right of the individual to self-determination*. So-called “human rights” are, of course, a social construct—they do not exist in Nature. But neither do other “legal” aspects of life. *Forced citizenship* is one of them.

Today, we live in a world of passports, visas and strict border controls. Applied differently, these tools may be beneficial. Unfortunately, at present, they are used not to keep undesirables outside, but to keep the people *inside*. Modern states are farms, and the farmers are the Parasites at the top. What if citizens could choose to leave their country easily, without a hassle? Things would be a lot more different.

“Governments will ultimately have little choice but to treat populations in territories they serve more like customers, and less in the easy that organized criminals treat the victims of a shakedown racket.”—James Dale Davidson, The Sovereign Individual

It is quite straightforward: a State’s well-being depends on the well-being of its citizens. If citizens leave, the State suffers. Therefore, it must do everything it can to attract and keep citizens, not alienate them.

The **second element** is *governance*. One of the Parasites’ modern devices, *democracy*, helps them greatly in achieving their goal of domination. All wrapped in the “greater good” package, of course:

“As you can see, almost any method used to create a subservient class of followers is wrapped around the idea of helping them, saving them from the evils of the world as well as from themselves.”—How to Scam the Planet, Part 2: Democracy

What democratic institutions lack is *skin in the game*. Another excerpt from my essay:

“The question of responsibility is a loaded one. When you know that your time is limited, you have a sense of urgency to take advantage of all the powers given to you and act frantically, without much regard for the future. The result is squandering, more wars, silly laws and regulations. You, however, are completely devoid of any personal responsibility.”—How to Scam the Planet, Part 2: Democracy

There is no need to re-invent the wheel here. The solution is as Lindy as it can get: *monarchy*. Wait, did I just suggest that we return to the middle ages and undo all the progress we have achieved?

Unless you really think that an office of constantly rotating Parasites with no sense of responsibility in control of an animal farm that bears the name of your country can be considered progress.

But there is one more element. The **third** is *extreme localism*.

If before, empires grew due to conquest of new territories, today’s State apparatus grows by conquest and subjugation of its own people. More often than not, individual countries remain of the same size, but may unite into super-states like the European Union if the Parasites higher up in international organizations have their way. And therein lies the problem, of course: central control is efficient only up to a certain scale. Countries with vast territories are extremely difficult to manage while small states normally have fewer management problems and higher stability. The famous examples of Singapore, Hong Kong and Liechtenstein provide curious case studies.

Therefore, having a small but efficient state is preferable. This is precisely my argument for future citadels, independent city-states that treat their citizens more like customers rather than livestock.



Yes.

Sovereignty All Around

So, what does our State look like in the end, after we have applied the above-mentioned changes? It is a citadel-like micronation or city-state, which:

- is governed by an efficient central body with a head of State, preferably a *monarch*. In our case, a monarch is more of a *descriptive* term, however, than prescriptive. It can be a Prince advised by a Council. Or a Chairman, assisted by a State Council. Or a CEO surrounded by a Board of Directors. Your choice, as long as there is *clear hierarchy* and *leadership*.
- allows for its citizens' unconditional exit from the State, no strings attached. Citizens must be able to vote with their feet if living conditions turn against them. In other words, they are *sovereign individuals*. In this regard, having options is, of course, necessary. That is why a market of living together must develop.
- is small in size. A compact territory is important due to the fact that the larger the territory the weaker the control over its parts by the leader. The ruler must experience the conditions of the life of his citizens by *living* in them. The citizens must have access to their ruler. Should a country become lucky with a larger landmass, it must be broken into smaller, largely autonomous units. Even Liechtenstein, a small principality of only 160 km², allows for the right of secession of each individual community.

Closing the Circle

It has been less than ten years since I stumbled upon the concept of Anarchy. I find it curious how my thoughts have developed in light of new knowledge, experience and deliberation on the topic.

My current understanding of things can be summarized in this tweet.

I am sure that I will learn something new in the coming years that will refine my understanding even further. However, the current state of affairs in my brain is close to *actionable knowledge*. That can only mean one thing: the time to act on it is here.

By decentralizing the world into thousands of independent states while centralizing control in each individual unit in the hands of the leaders with skin in the game, we may create better, more *natural* conditions for everybody on the planet.

Shall we?

The State vs. Bitcoin

By **Steve Barbour**

Posted March 15, 2020

- The sustainability of censorship resistance -

***Foreword:** As with freedom and oppression, Bitcoin and State money may exist in a perpetual tug of war between ideals. Where State money relies on compulsory participation, Bitcoin offers completely voluntary entry and exit and thus represents the antithesis of State money. In this essay I will explore the mechanisms in which Bitcoin may resist State attack.*



Notes to the reader:

- The term 'Bitcoin' with a capital 'B' refers to the Bitcoin network or economy, while the term 'bitcoin' refers to the unit of money.
- Please refer to the definitions section at the end for clarifications

Introduction

Bitcoin's ability to resist censorship has a necessary security assumption in that honest mining is more profitable than dishonest mining¹. For this to hold true censorship must meet adequate resistance by the honest economy to ensure that dishonest behavior and censorship is not sustainable. This may be achieved by depleting the attacker's investment capital by either minimizing their mining reward or maximizing their mining cost. While it is not possible to prove one way or another whether dishonest mining can be overcome, we will outline some of the factors that may give honest miners an edge to resist censorship and support the sustainability of honest mining.

Bitcoin

Bitcoin is engineered money. Its design is unique in that any interested participant is able to join and leave consensus² on a voluntary basis without having to receive permission from any authority. It offers superior monetary properties over legacy State monies. For example, bitcoins are impossible to counterfeit or arbitrarily debase and are very difficult to confiscate. There is no other money today that

offers such freedom, so it's no surprise there are many people interested in protecting its value proposition, though others feel threatened by it.

Sound engineering must consider not just steady state conditions, but also the upset conditions. A properly designed system must anticipate the unlikely but catastrophic scenario and build in appropriate safety factors to prevent disaster. A bridge may average fifty vehicles crossing at any given time but it still must be designed for many hundreds of vehicles stuck bumper to bumper in traffic, or for the thousands of pedestrians who may congregate. We cannot afford to have the bridge collapse and kill everybody when an upset condition rears its ugly head.

As engineered money, what exactly are the upset conditions in which Bitcoin was designed to mitigate? What are the worst case scenarios with the greatest impact? Is Bitcoin engineered to resist catastrophe?

Censorship Threats

A bitcoin miner may gain a majority of the network hashrate at any given time, given enough external capital investment. If a single bitcoin miner, or a colluding cartel of smaller miners, gain over 50% of the total network hashrate then they become the network majority and gain the option to censor the network completely.

A majority miner may choose to censor in the following ways:

1. Deny blocks and block rewards to the minority miners
2. Deny merchant transactions and fees
3. Reorganize history and attempt double spends

A majority miner may simply choose to mine honestly rather than upset the integrity of the network with censorship, but how would you even know if a majority miner existed? It is trivial for a miner to hide their hashrate among many different pools or to solo mine. Mining is by nature and necessity anonymous, so the possibility of a majority miner persists as an ever present threat to network trade.

Possibly most concerning to some is the fact that each of these methods of censorship represents *valid* behavior which no bitcoin node on the network would reject. There is no state, now or in the future, in which the risk of censorship can be eliminated altogether, but it can be resisted.

Denials of Service

There are plenty of good reasons that we could consider as to why a majority miner might decide to stay honest but we will not be contemplating them here. Instead we will assume a majority hashrate, once achieved, will attempt to upset the economy in the most disruptive manner possible. This is the upset condition that the network must resist and may indeed be the censor's objective. Let's explore the censorship threats listed above.

1. Deny block rewards

A majority miner may choose to build selfishly on top of his own blocks and to exclude any of the honest miners' blocks from the strongest chain. This means the dishonest majority would be censoring all competing hashrate, earning 100% of all block rewards while the rest of the honest minority would earn nothing. This could be achieved with even a simple majority of 51% of network hashrate. In such a case any honest blocks that are mined on the network would lose the race to the majority miner and go stale, thus wasting the energy and capital consumed by the honest minority. The majority would have complete control and have the ability to tax the minority miners up to and including 100% of the block reward. To resist censorship the honest minority must either increase their hashrate to overtake the censoring majority or they must reduce it in order to preserve their capital and live to fight another day.

It is notable that the censor may choose to tax honest miners less than 100% and to allow some arbitrary percentage of honest blocks to confirm. Doing so may be in an effort to enforce a white market mining regime under a State mandate, where a tax is enforced on the economy. This may seem far-fetched but the reality is this is what the State does today; they do not tax 100% as that would invariably kill the economy and likely spark a revolt. The parasite does not want to kill its host.

2. Deny trade

Majority hashrate also gives the censor the ability to choose which UTXOs are allowed to move with a white list or a black list. The censor could also arbitrarily tax merchants by increasing the minimum fee levels to confirm their transactions. Any honest minority blocks that allow a low fee to confirm could be made stale by the censor. The censor could also decide to only allow a white-list of transactions through, presumably a list of UTXOs in which the owner has passed through a proper KYC process mandated by the State. This may be a State objective³ as a mechanism to control the money and enforce a 'Statecoin'.

The worst case scenario for merchants is the majority censor could ban trade altogether and mine empty blocks exclusively. This would be a complete denial of service attack on merchants and the Bitcoin network in general, not allowing any trade to occur on the network at all. The downside of such an attack for the majority miner is that they would not be earning any transaction fees and the fee pressure supporting honest miners, discussed later, would increase substantially. Such behaviour would absolutely require an external subsidy, which only the State could provide by consuming taxes brought in externally from increased taxation or seigniorage.

3. Double Spend

A majority miner can not only keep people from participating, but they can also trick them into believing their transactions have settled, opening up an opportunity to steal from them.

If a majority miner has enough of a hashrate advantage over the minority of honest miners then they can mine on top of previously confirmed blocks in which transactions have previously settled. In doing so they can mine a new chain in secret and reveal the chain to the network once they surpass the tip of the chain of the honest minority, which 'resettles' previously confirmed transactions. If the majority miner had made a transaction that was confirmed in the chain tip that gets resettled then they can re-spend their

coins again on the newly mined chain causing the merchant who accepted their coins originally to lose the balance. The end result is the merchant had sold their goods in return for coins that disappear – a theft.

Double spend behavior, while theft, is *valid* behavior and even anticipated by the system⁴. The network has no choice but to accept such behavior in order to maintain consensus rules, otherwise a new consensus model would be in place which negates the value proposition of Bitcoin altogether. The ‘DAO fork’ on Ethereum, where a social consensus was used to over-rule the Bitcoin consensus property, is an example of tossing out the value proposition that Bitcoin offers.

The censorship threats listed above are not meant to be an exhaustive list, only to outline some of the more serious attack vectors in Bitcoin.

Censorship Objectives

An obvious risk of censoring the Bitcoin network is the assumed loss in value of the coin and in the mining hardware of the attacker, as presumably the economy reacts negatively to censorship. Some people have referenced this loss in value as a ‘security cost’ to attacking the network and a strong preventative incentive against an attack. However, this is not necessarily a reasonable assumption to make.

The potential depreciation of the hardware and coins due to censorship may or may not matter to a censoring majority depending on his or her objectives. Indeed, the censor may not even own any hardware or coins at all, any person with a gun can walk into an industrial bitcoin mine and take over the hashrate. Many men with guns, e.g. an army, can do so at minimal cost and capture or destroy all mines they can identify. All that is required is the word of law to co-opt all identifiable bitcoin mines within a given jurisdiction. Therefore, relying solely on lost value of coin or of the hardware as a defense against censorship is an error – the censor may wield powerful resources.

Who is Motivated to Censor Bitcoin?

Prior to discussing the mechanisms of censorship resistance let’s discuss who would want to censor bitcoin in the first place. Who would want to shut down a network offers greater freedoms of trade and prosperity to anybody that participates? We will assume that the entity who is most motivated to shut down the Bitcoin network is the entity that profits the most from doing so. Considering that we have not yet seen a single profit-driven miner censor the network in the first 11 years of operation – the easiest years to attack it, mind you – it is increasingly unlikely that we will see a profit driven miner attempt to censor it any time in the near future. Not to say they won’t try eventually. That being said, not all bitcoin miners are seeking on-chain profits, the greater risk comes from the miner who seeks to preserve their off-chain profits – the State.

State Money

The ‘State’ is an organizational framework based upon an aggression enforced dominance hierarchy that begins with the control and issuance of ‘State money’. State money is a money that is not produced by any free market, voluntary or competitive means but instead issued and enforced via aggression and law. In this way, State money is unnatural, unlike monies which are produced by people in a voluntary and competitive manner – gold mining for example.

The State is made up of government, institutions, businesses and regular working class people like you and I. Indeed, as members of society, we *all* play a role within the State and we are each vying for higher positions and leading roles within the dominance hierarchy. Not all State actors are equal, the higher you are in the hierarchy and cheaper you can acquire State money the more disproportionate the advantage you have. We see the disproportion manifested in the centralization of wealth in society today – “It takes money to make money”, as they say.

A monopoly on money issuance is the backbone of the State and those responsible for it are at the very top of the dominance hierarchy. Using the American State as the example, at the top sits the US Treasury and the Federal Reserve (central bank). They acquire money at the lowest cost and lend it out to those on the next level down the hierarchy. This may include investment banks, hedge funds, or other institutions. Eventually the money flows to commercial and retail banks followed by businesses and finally individuals, but each step down the hierarchy the cost of money goes up. The further you are from the top of the hierarchy, the longer it takes you to acquire the money and the more you are disadvantaged by the increasing prices of goods caused by the inflationary nature of the State money. This concept is described by the Cantillon Effect, units of inflationary State money are worth less tomorrow than they are worth today.

At the top of the State hierarchy money is not acquired through any competitive free market means, it is acquired through arbitrary issuance and enforcement via aggression. It is a fiat money. New units of fiat money are issued at negligible production cost and its value is accrued from the dilution of the remaining money that is already out circulating on the market, held primarily by those at the base of the hierarchy. In this way, the issuance of State money is a tax on the holders of the existing monetary base. This is known as seigniorage.

Anti-State Money

Bitcoin does not need to rely on an aggression enforced hierarchy, instead money can be produced by anybody on a voluntary basis. It is based on market competition and all actors must suffer a cost to produce it (mining investment) or to acquire it by other means (trade).

The antithesis to State money, Bitcoin has a deflationary nature and the further away you are from the money issuance in time the more you are advantaged. People are motivated to hoard bitcoin because its purchasing power tends to increase over time. This ensures that any prospective investment has to out-compete the market rate of return of simply hoarding bitcoin, which is in stark contrast to the incentives behind State money in which hoarding is punished. In essence Bitcoin represents a reversal of the Cantillon Effect and is therefore a threat to State money and the State itself.

Bitcoin also benefits each State actor disproportionately depending on their position in the State dominance hierarchy. The individual who is furthest down the hierarchy is most advantaged by Bitcoin's success relative to those further up the hierarchy in the same way that they are most disadvantaged by State money. An investment bank is disadvantaged relative to the individual, but is advantaged relative to a central bank. Generally, someone less wealthy, who has trouble accessing low interest rate loans, is advantaged relative to someone with better interest rates at their disposal. The top of the dominance hierarchy, who by definition have the lowest cost basis for State money, are the most disadvantaged by

Bitcoin's success — they simply have the most to lose and furthest to fall if State money collapses. As bottom-up money Bitcoin is inherently anti-State for these reasons.

Money is Power, Power is Money

As a parasitic organizational framework, the State exists to extract taxes from the economy to subsidize its own existence. Controlling the money is the easiest way for the State to enforce this objective, including taxation via seigniorage (a politically correct term for counterfeit).

The State does not want to lose its control on taxation so it will likely attempt to control Bitcoin. It is natural for the State to have this objective just as it is natural for any organization to resist that which threatens its growth or survival. The State is not by any means 'evil', it is simply an organization of people that has found success by leveraging aggression. In some ways it is the final manifestation and natural progression of mankind's tribal nature. Remember, the State is an organization framework, not specific people — there's nobody to blame here.

The State may attempt to destroy Bitcoin altogether in order to preserve the utility of State money or it may simply try to control it and attempt to turn it into Statecoin. Since Bitcoin is really just an idea and may not be possible to destroy, we can probably expect the latter. The best way for the State to control Bitcoin and enforce their objectives, as described in the censorship threats above, is by gaining majority hashrate.

Is Censorship Feasible?

The true cost to gain a majority hashrate and censor Bitcoin is a function of how well honest miners are distributed and hidden. Let's look at the two extremes:

Extreme #1 — Distributed Hashrate: *A network of hundreds and thousands of well distributed, anonymous miners, each having less than 1% of the network hashrate.*

If the network consists of many independent miners, each with relatively equivalent hashrate and each mining with relative anonymity, then it becomes rather costly to acquire a majority hashrate and censor the network. In such a scenario the hopeful censor must invest his own capital to acquire a majority hashrate with no option of co-opting the existing miners and destroy competing mines since they are well hidden and well distributed. After all, if a mine cannot be identified then it cannot be bought, co-opted, or destroyed.

To reach 50+ percent of the network hashrate in this scenario would require an enormous capital investment and would also require a massive advantage on low cost energy supply. Presumably, because the network is well distributed precisely because of the lack of energy arbitrage opportunities, low cost energy may not even be an option. This might indeed be what the future of bitcoin mining looks like, as energy arbitrage opportunities continue to tighten.

When the censor is successful and gains majority hashrate he has now sunk a ton of capital in ASICs, farm build-outs, and in the coin. If he decides to censor the network and there is a market drop in price due to the censorship scare, then he loses a significant percent of his capital investment due to the depreciation

of his hardware and coins. A prospective censor would much prefer a cheaper, more feasible option to censor the network.

Extreme #2 — Centralized Hashrate: *A network with a few dozen large 100+ MW industrial mining farms dominating the network by accounting for over 80 percent of the hashrate.*

The bitcoin network today looks more like this scenario than the previous one, albeit probably not as extreme. In this example the hashrate distribution may consist of a mix of hobbyist and small commercial scale miners that make up an insignificant minority, and a few dozen massive industrial bitcoin mines that collectively dominate the network hashrate. The large mines might be located in different countries, but they are so large in size they are impossible to hide. Immense power consumption generates heat that can easily be spotted from satellites, among other surveillance means.

A State ban on mining comes to pass, likely as a wartime measure (which do tend to have the interesting characteristic of permanently shrinking human rights and liberties), and multiple States collude with each other and take control of several large mines within their respective jurisdictions. Laws are written and Bitcoin is banned or only allowed under strict KYC and AML laws and mining licenses, among other regulatory approvals.

Under a regulated regime, all of the large mines comply since they cannot hide and failure to do so is a crime. The smaller mines continue as before, hidden on the black market and circumventing the costs of compliance. In some cases the owners of the large mines decide they do not want to participate under the new regime and accept discounted buyouts for their interests in the mines to those who are willing to comply. In other cases the mines are simply taken over by force on the basis of illegal mining. Regardless, in this way and others the State gains control of majority hashrate with relatively little resistance or upfront capital cost.

Threat Avoidance

In the animal kingdom we observe the survival instinct when facing a predator — the decision of fight or flight — but a greater defence yet is avoiding the threat altogether. If the predator cannot identify the prey which is camouflage with its environment, the decision does not need to be made at all. Like a chameleon, remaining hidden requires no energy input and is therefore an optimal threat avoidance strategy. It is therefore the ability to mine covertly that best protects the miner from aggression, in the same way that anonymity is the best defence against any violent act — you cannot attack someone you cannot identify.

Any entity with enough capital can become the majority miner, whether they build it out themselves or buy and take over existing mines. For the State who can call upon legal aggression, it is even easier. There can be no doubt that obtaining majority hashrate is feasible, so the question is whether or not censorship is sustainable.

“It is not the size of the mine that matters, it is whether or not you can hide it.”

-Sun Tzu, maybe

Mechanics of Censorship Resistance

Censorship is anticipated by the system, it was designed precisely to anticipate a dishonest miner attempting to gain control ⁵. However, we have not yet experienced a censorship attack on the network by a majority hashrate so we can only speculate as to the sustainability of honest mining. What stands in the way of a dishonest majority confiscating all future block rewards? What kind of strategy might a censor employ to attack the bitcoin network?

Censorship Optimization

If a majority miner censors an honest miner's block by not building upon it, then the honest miner's work ends up wasted. This is because the proof of work completed by the honest miner, whose block was censored (made stale), is not included in the strongest chain. The result of censorship of honest blocks is longer block times and a network Difficulty adjustment downwards to compensate.

As an example, if a censor gains control of 85% of the total hashrate and rejects all blocks from the remaining honest 15%, then the difficulty will adjust down 15%. The censor may choose to reject only a subset of honest blocks – perhaps only the blocks that do not provide an approved signature under a 'white list' regime – or he may choose to blacklist all honest blocks entirely.

Notably, the majority miner only needs just over 50% of total network hashrate to blacklist all other honest blocks entirely and earn 100% of rewards. Let's call this the 'minimum majority rule'. Therefore, if a dishonest majority is interested in complete censorship of the network then **any investment beyond 50% by the majority censor ends up being a waste of capital and energy**. Our majority censor with 85% of total network hashrate would be burning 35% of their hashrate and energy for no reason, which would lessen their ability to continue censoring by depleting their capital.

Since we have assumed a sustainable attack must also be profitable, one could expect the censor to choose to optimize accordingly and limit their hashrate investment to the minimum majority hashrate. In this case they still earn 100% of rewards but have preserved capital by not burning the extra energy for no extra reward. If the honest minority of miners manage to find some lucky blocks and outpace the censor, presumably he can simply bring on more hashrate to deny their blocks and win the race.

In fact we would expect the censor to only broadcast blocks at a rate that honest blocks are found, thus continuing to make them stale but not increasing the Difficulty for no good reason. The censor is better off shelving all excess hashrate beyond the minimum majority and using it only to overtake honest blocks, if he wants to censor optimally. Therefore if honest hashrate increases or decreases for any reason, then so will the censor's hashrate in order to optimize to the minimum majority requirement. At any given time, under an optimized censorship regime, all honest hashrate is being matched by the censor. The censor is even able to automate censorship and ramp up or down hashrate as needed. Honest hashrate has no means of colluding to mine in secret because this would be dishonest behaviour and would result in coordination problems which proof-of-work consensus was invented to solve, defeating the purpose.

The only choice an honest miner has to resist a censorship regime is when to mine and when to go offline. By mining, an honest miner forces the censor to increase their hashrate by at least as much, but doing so

can only be expected by an honest miner if a reward is obtainable. **Mining ‘ideologically’ implies mining at a loss and doing so is an error because it wastes capital and prevents the ideological miner from mining profitably in the future.** Once made aware that his blocks are being censored, an honest miner may decide to go offline until such a time that resuming is profitable, such as in response to fee pressures discussed below

Honest mining is required to overcome censorship, but the honest miner cannot be expected to mine at a loss, it is by definition unsustainable. Since the honest miner cannot affect the magnitude of the mining reward, which is a function of trade, he must attempt to mine the reward or to go offline and live to fight another day.

A censor is not interested in a healthy economy and so he must be forced to abandon censorship by running out of the capital required to sustain his censorship regime. The Bitcoin economy may accomplish this by forcing the censor to mine at a loss, which can be achieved by minimizing his reward and maximizing his cost. Censorship must not be rewarded if it is to be resisted, so what are the resistance mechanics provided in Bitcoin’s design?

Censorship Resistance Mechanism – Difficulty Adjustment

If a majority miner optimizes censorship by maintaining a minimum majority hashrate then it results in Difficulty drop equivalent to the censored hashrate. Previously we noted that the censor does not want to mine dishonestly at 85% hashrate because the 35% did not contribute to any further reward. However, by optimizing to the equivalent honest hashrate (which is 50% of total network hashrate at any given time) the difficulty necessarily adjusts downwards up to the maximum of 50% due to the same amount of honest hashrate being censored. This decreases the cost to mine a block and will entice more honest hashrate to come online in order to chase cheaper blocks.

Indeed, if the Difficulty adjusts downward enough then even older hardware that was previously ‘obsolete’ and too costly to mine economically (e.g. high electricity prices) may also attempt to come online if the risk to reward ratio is great enough. This is comparable to the case where the bitcoin price increases at a rate faster than the Difficulty, less efficient mining hardware becomes profitable again.

Censorship optimization also results in the maximum Difficulty reduction and therefore provides the largest possible incentive for more honest hashrate to come online, increasing the cost to sustain censorship. The effect is somewhat similar to how State mandated production cuts in the oil and gas industry cause the price to increase and in turn incentivizes more investment into new production.

Here we have identified how the Difficulty Adjustment mechanism optimizes the price of blocks to maximally incentivize honest mining.

Censorship Resistance Mechanism – Fee Premium

If a majority miner is not accepting transactions from merchants then the censored merchants must either increase their fees or not transact at all. If a merchant cannot move their bitcoins then they effectively have no value for the duration in which they are being censored. We can deduce that, due to personal time preference, a merchant who is being censored will be willing to pay a higher confirmation fee proportional to the duration in which they are being censored, up to the theoretical maximum in which the fee is the entirety of the transaction.

If the merchant chooses to wait and simply 'hodl' then they are denying a reward to the censor for blocking their transaction, however this is clearly the censor's objective. While the censor does not earn a reward to offset their mining costs, the merchant is suffering the cost of not being able to use their bitcoins in trade.

Inevitably all coins must be spent, so the merchant must eventually choose to increase their fee. The increased fee level will either entice the censor to mine the transaction or it will drive up honest hashrate who look to earn the fee. The fee premium either gets mined and breaks censorship or it increases the cost of censorship, in both cases the censor loses.

In the Difficulty Adjustment Mechanism we discussed what happens when a majority censor prevents honest miners from finding blocks — it results in extended block times and an eventual downward Difficulty adjustment. It turns out that the increase in block times also ends up driving up the fee premium to get into a block, presumably due to the market's time preference and desire for rapid confirmation and settlement.

By censoring transactions and honest blocks the censor has effectively enabled a fee premium to honest miners. Honest miners always seek maximum reward and will attempt to mine the fee premium that the censor refuses. Therefore, the fee premium is an incentive to honest mining and increases the honest hashrate. As shown, this has a net effect of increasing the cost basis of censorship and **therefore a majority miner cannot censor a merchant without incurring a loss.**

Here we observe how the Fee Premium Mechanism results in a cost to the censor and incentivizes honest mining.

Censorship Resistance Mechanism — Confirmation Preference

Earlier we discussed how a majority dishonest miner can attempt to double spend merchants and steal their goods and services. However, merchants are not helpless against this threat because they can protect themselves by changing their confirmation preference.

We often say in Bitcoin that zero-confirmation transactions are unsafe. This is true because a zero-confirmation transaction can be double spent even without majority miner reorganizing the chain because the transaction was never confirmed in the first place. We also say low confirmations are unsafe because single block reorganizations are a relatively frequent occurrence and a fundamental risk due to the probabilistic nature of bitcoin mining.

The more confirmations a merchant prefers the safer they are from a double spend. A merchant's confirmation preference should rely on the value of the trade that is being conducted or the risk potential of a double spend.

For example, a small value transaction such as a movie ticket purchase might be OK to accept 1 confirmation because the likelihood of a double spend attempt on such a low value transaction is pretty much negligible and not worth waiting the extra time for more confirmations. However, if a majority miner is actively censoring the network and causing frequent block reorganizations then the merchant may prefer more confirmations beyond the average reorganization depth before giving over the goods. In this way a merchant can continue to trade during a period of high risk. Notably, once merchants are made aware of censorship and change their confirmation preference the costs of continued double spend attack increases proportionally. Realistically, a merchant's confirmation preference is subjective based on the value of the trade, the anonymity of the purchaser (legal recourse may be an option if the thief can be identified), and the threat level of an active majority miner.

Here we observe how the Confirmation Preference Mechanism results in an increased cost to the censor.

Conclusion

Bitcoin was designed as a tool for people to use to resist censorship. As a tool, it cannot offer any guarantees against a majority miner choosing to censor the network because the censor is always able to subsidize their operation with external capital or co-opt existing mines. However, it does provide the mechanisms required for honest miners to overcome censorship, we just cannot know if the censor has the resources to continue mining at a loss indefinitely. Since the State is the most likely censorship threat, all we can say is that they would have to consume taxes at a rate equivalent to their losses. It remains to be seen whether or not people would tolerate such behavior, as it would require off-chain resistance.

Satoshi Nakamoto understood what his design represented and wisely chose to enter consensus anonymously. Bitcoin is the antithesis of State money, the evidence to which Satoshi engraved in its genesis block — a political statement against widespread financial corruption within the State. We may expect to see the State attempt to control Bitcoin, or perhaps we, as actors within the State, will find a peaceful way to transition to better money.

Whether we find a peaceful transition or not, we can help others follow Satoshi's example by building the tools that merchants and miners need to share the risks associated with resisting censorship. Together, honest action and honest intent may overcome and deplete the resources of the censor and quell the upset condition.

Acknowledgements

I would like to thank Eric Voskuil whose work on cryptoeconomics — a compilation of which can be found in the Libbitcoin Wiki⁵ — was the source material and much of the inspiration for this piece. If you enjoyed this perspective on Bitcoin's security model please consider contributing to the Libbitcoin Institute.

Definitions

AML: Anti money laundering, a State regulation.

Block Reward: The sum of bitcoins from the block subsidy and transaction fees in each mined block.

Difficulty: A protocol variable that controls the frequency of block times due to a changing hashrate.

Dishonest mining: To reject one or more valid transactions or blocks; to censor.

Honest mining: To accept all transactions and build on top of all valid blocks.

KYC: Know your customer, a State regulation.

Majority miner: A miner who controls > 50% of hashrate.

Merchants: People who use bitcoin in trade and pay confirmation fees to miners.

Miners: People who produce confirmations in return for the block reward.

Minority miner: A miner who controls < 50% of hashrate.

Stale block: A valid block that is mined but is not included in the strongest chain.

The State: A set of people who profit through aggression in lieu of voluntary trade.

UTXO: Unspent transaction output; A merchant's bitcoin balance.

Bitcoin and the intolerant minority

By Hasu

Posted June 5, 2019



Someone on Twitter asked me about the thesis that an intolerant minority can defend Bitcoin. I've long had some thoughts about this, so it was time to write them down.

I think the concept of the intolerant minority is frequently misapplied in Bitcoin. Bitcoin is less defended by an intolerant minority than it defends *against* an intolerant minority.

Most people in most systems are indifferent as to what happens. They are the tolerant majority. Then there are special interest groups pulling the system in different directions. These groups most resemble intolerant minorities.



The process by which the special interest group moves the tolerant majority is often invisible to the untrained observer, but it exists. Lobbying is one example. Lobbying has a bad connotation, but special interest groups are nothing bad; they are a prerequisite for ANY change to occur.

In Bitcoin, there are groups that support larger blocks, smaller blocks, better privacy, or expressive scripting language, even KYC on a blockchain (to name a byzantine proposal). Some are better organized and resourced than others. Some operate overtly, others covertly (e.g. via funding some proposals and people and withholding funding from others).

These groups can neutralize each other (e.g. a smaller-blocks and a bigger-blocks movement), at least until a more permanent split occurs.



This is a deliberate oversimplification - in practice, some from the majority might favor LEFT, while others might favor RIGHT. But there's not enough momentum in either direction to cause a change.

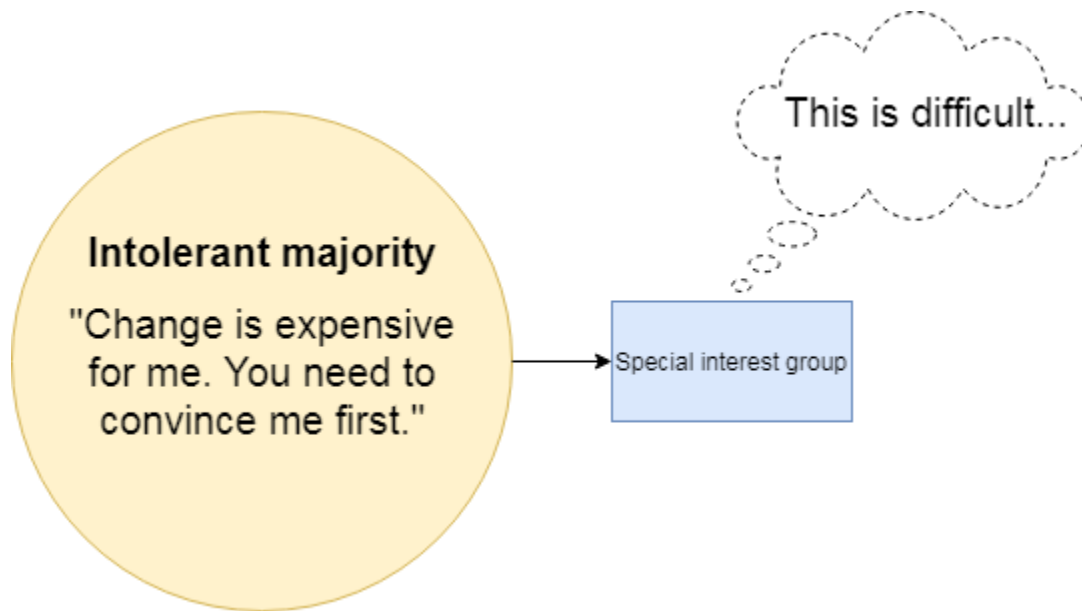
More commonly a system's governance is eventually captured by one or two special interest groups (watch this happen in most real-world systems).

So the first insight is that intolerant minorities lead to CHANGE, not prevent CHANGE in a system. Only when two special interest groups neutralize each other perfectly the result is no change.

When a sufficient number of people from the otherwise-tolerant majority disagree with a special interest group, they can branch into their own special interest group. Then, the course is determined by a battle of the special interest groups.

Bitcoin is designed to resist change by making it cheaper for the MAJORITY to be intolerant. It does this by automating the detection and rejection of transactions and blocks that don't abide by the social contract.

The rules can still be changed, but it takes more explicit buy-in from the majority.



Intolerance of the majority exists on a gradient. The more intolerant it is, the larger special interest groups need to be. Even this is not all positive: It's super hard nowadays to get any change into Bitcoin, even ones that have many supporters and very little opposition (Schnorr, CTV...).

But if the majority stops using these tools (self-custody and full nodes), Bitcoin's endgame is the same as in any other system:

its rules determined by the battles of small special interest groups; its credible neutrality lost.

A Peaceful Protest - Opt-Out, Buy Bitcoin

By Adam Pokornicky on New Money

Posted June 8, 2020.

I came to Bitcoin from a unique perspective back in 2012, looking for something better after watching bankers destroy our economy then receive bailouts and bonuses for their noble work. The Federal Reserve(the Fed) had just begun its unprecedented experiment in printing money and quantitative easy, and I had grown cynical towards a crony form of capitalism that was normalizing bad behavior by rewarding failure and underwriting wealth extraction from the poor and middle class to the rich through money printing and easy money policies.

Article 1 of our constitution, explicitly gives the power to print money to Congress. Controlling the money supply is indeed our government's job. However, for those unfamiliar, President Woodrow Wilson signed the Federal Reserve Act into law on Dec. 23, 1913, three years after a bunch of shady bankers like J. P. Morgan, William Rockefeller, and their associates, went on a fake secret hunting trip to Jekyll Island off the coast of Georgia where **they conspired to create a central banking cartel** for private bankers that would later come to control the issuance of the U.S. money supply.

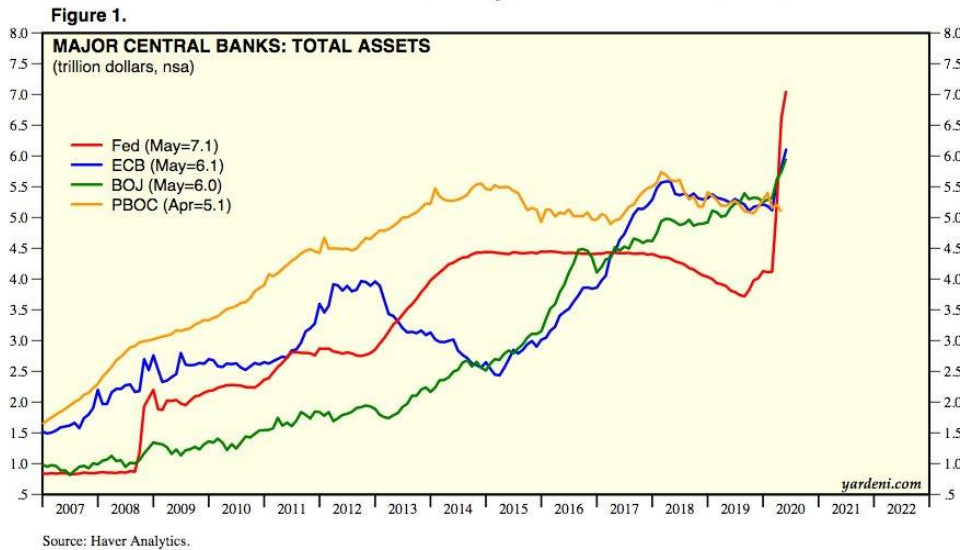
The Federal Reserve was sold to the public with a promise to end the threat of recessions and depressions but the fact of the matter is that most people have little understanding of what it actually really does. There is no mention of a central bank in any of America's founding documents because the founders of our country knew what would happen to the economy and the workers in this country if control of the supply of money was put in the hands of a few "trusted" bankers. Thomas Jefferson once said:

"If the American people ever allow the banks to control the issuance of their currency, first by inflation then by deflation, the banks and corporations that grow up around them will deprive the people of all property until their children wake up homeless on the continent that their fathers occupied."

If this doesn't sound familiar then you've either been in a coma or have been living under a rock for the past decade. In past issues "**What is Money**" and "**The Cantillon Effect**", I've described how printing money works, how it decreases your purchasing power while greatly benefit the rich and powerful who are closest to the money created. (re: NOT YOU!).

As a quick reminder, let me describe to you one way that the Federal Reserve is inherently oppressive to the workers in this country. Every time the Fed creates money and pumps it into the economic system, the value or purchasing power of each dollar you own goes down because the money supply is inflated. Each dollar in existence gets diluted by all the new dollars created. For example, since 2008, the US federal reserve has expanded their balance sheet from .8T to 7.1T. In actual terms, this means they have "inflated" that fiat monetary base supply of currency by 21.9% ANNUALLY over that 11 year period of time.

Total Assets of Major Central Banks



How is this oppressive? The money goes straight into the hands of the people holding assets giving them more wealth and power to encumber us while only a trickle comes down into the lower-income sections of the economy where a majority of the population exists. This phenomenon is called the **Cantillon Effect** which I described in a recent post as the uneven expansion of the amount of money. Under our current system of modern central banking, money is created and injected into the economy through the credit route and first affects financial markets. **Cantillon explained that the first ones to receive the newly created money see their incomes rise whereas the last ones to receive the newly created money see their purchasing power decline as consumer price inflation comes about.**

In the case of a monetary expansion, the ones who profit from it are the ones who are closest to the money. “Close to the money” in this case means everyone who can access the money right at the beginning, i.e. big companies, banks, hedge funds, ultra-wealthy individuals, etc. They get loans and make investments. Prices then start to rise on goods and services that are absolute essentials to life (ie. Healthcare, Housing, Food, Education) even though the majority have not profited from the increase in money at all. In sum, the purchasing power of those furthest away from the top drops the most. The result is a redistribution from the poor to the rich.

Where does this inequity show up the most? Specifically in the wealth gap between black and white Americans. Of the 1.2 million households in the top 1 percent, 96.1 percent are white. While there are many factors at play that have relegated Black Americans to second-class status, with far fewer opportunities to achieve good health, political influence, prosperity and security than other Americans, the magnitude of this problem is highlighted by the significant gap in median wealth held by Black families (\$17,000) and White families (\$171,000)—a ratio of 10 to one.

American Inequality Didn't Just Happen. It Was Created.

Economist Joseph Stiglitz wrote in a recent book the following which touches on many crucial points regarding the system and economy we find ourselves trapped in:

“American inequality didn’t just happen. It was created. Market forces played a role, but it was not market forces alone. In a sense, that should be obvious: economic laws are universal, but our growing inequality—especially the amounts seized by the upper 1 percent—is a distinctly American “achievement.” That outsize inequality is not predestined offers reason for hope, but in reality, it is likely to get worse. The forces that have been at play in creating these outcomes are self-reinforcing.”

“Inequality is the result of political forces as much as of economic ones. In a modern economy government sets and enforces the rules of the game—what is fair competition, and what actions are deemed anticompetitive and illegal, who gets what in the event of bankruptcy, when a debtor can’t pay all that he owes, what are fraudulent practices and forbidden. Government also gives away resources (both openly and less transparently) and, through taxes and social expenditures, modifies the distribution of income that emerges from the market, shaped as it is by technology and politics.”

The perversion of our system didn’t occur overnight but the mutation likely began in 1971 when the U.S. dollar was taken off the gold standard, severing the relationship between money backed by something and money backed by nothing. This is when the country began its long transformation from an industrial empire to a financial one, where asset inflation, rent-seeking, and debt-serfdom subjugate Americans in their own country in a gross form of Financial Feudalism.

Debt Serfdom and How the Wealthy Use Debt

My good friend Michael Krieger wrote about “Financial Feudalism” in a post earlier this year, where he broke down how Debt is the primary weapon used against the masses.

Krieger went on to describe how most people understand the societal effects of excessive debt from a basic level where individuals in the bottom half of our population essentially have no choice but to borrow in order to participate in the economy as constructed because the cost of so many things has been inflated way beyond the capacity of most people to purchase them outright. Because wage growth is woefully struggling to keep up with the soaring costs of fundamental things such as shelter, healthcare, and higher education, it requires many to take on debt defensively, just to get by and avoid falling down the socioeconomic scale.

As a result, he notes, “rather than empowering people, it **turns them into modern-day indentured**

servants endlessly stuck on a hamster wheel with little to no hope of getting off. This is not an accident, it’s a tried and tested tool which, when combined with incessant mass media propaganda, is an effective way of creating a submissive, confused, and desperate underclass.”



Michael Krieger
@LibertyBlitz

Americans have been conquered by the ruling class not via the sword, but via debt. Debt is the primary weapon used against the masses.

I call it financial feudalism and will be writing about it today.

February 17th 2020

111 Retweets 397 Likes



Michael Krieger
@LibertyBlitz

The oligarchy uses debt offensively (to increase wealth and power), while the masses must use debt defensively (to survive). If more people understood precisely how the game is rigged at the highest level (financial system) we might get somewhere.

February 17th 2020

57 Retweets 166 Likes

He continues to explain how for wealthy individuals, the opposite occurs. If you are fortunate enough to own your home, have a high paying job, enough savings that you have an investment portfolio, can pay for healthcare premiums, vacations and/or pay for your kid's college in cash without making a dent, then debt becomes something else entirely. Debt's no longer an anchor holding you down, instead, it becomes a tool to increase wealth in the form of leverage.

Krieger masterfully explains how the opposite occurs for the wealthy and how a large portion of wealth inequality over the past several decades can be traced back to this systemic interclass weaponization of debt. If you are wealthy and connected, you have virtually unlimited access to cheap debt, just as the private bankers on their fake hunting trip designed it. This access is used to make leveraged bets on all sorts of stuff, but primarily real estate and financial assets such as stocks and bonds.

He concludes by showing the gross juxtaposition of the haves and have not, describing how most Americans either struggle to earn enough income to get by a week-to-week basis while other white-collared cubicle monkeys strive to earn extra income to diligently add to their 401k. Meanwhile, bankers and hedge fund managers who have taken on massive leverage to amplify such bets made generational fortunes while creating nothing of value as their corporate executive counterparts use access to extremely cheap debt and financial engineering to consolidate their competition, buy back stock and reward themselves through generous stock option plans while looking at their employees as a line item between revenue and profit.

If it's not clear by now, **Central Banking is nothing more than socialism for billionaires**, policies that are enforced on us by unelected officials whose decisions implementing central economic planning have no accountability and zero public debate. Why aren't our politicians doing anything about it? Well, at this point it should be pretty obvious. With the DC political class being captured by big money from billionaires and corporations who benefit from central banking, politicians have no incentive to do anything that benefits citizens at the expense of the overlords that fund their existence. You, of course, will get a few breadcrumbs along the way like the mirage of voting every 4 years or a \$1200 check to keep you in check while the overclass continues to loot away and consolidate wealth and power.

With wealth inequality expanding and income inequality continuing to get worse, it's no secret that the wealthiest, typically white people, are getting wealthier while blacks and Hispanics continue to lose the little relative wealth they have. According to an analysis by Prosperity Now and the Institute for Policy Studies, the racial wealth divide is hollowing out America, particularly for persons of color, with **black households expected to have a net worth of ZERO by the year 2050**.

While the murders of George Floyd, Breonna Taylor, and Ahmaud Arbery highlight the racial injustice and police brutality black Americans live with every day, systematic inequality as a result of structural racism seen through housing policies, education, employment discrimination, the drug war, decriminalization, and debt-serfdom creates a damaging cycle of wealth inequality that is failing them, only to be compounded by central banking that keeps all of the above in place while literally stealing their money.

A Peaceful Protest: Plan B, Opt-Out for something better

When a system oppresses you and fails you in so many different ways, the most natural forms of push back are through protests, civil disobedience, strikes, and boycotts.

It is the latter that I believe offers individuals, especially the black community and those who believe that #blacklivesmatters, a non-violent and effective way to push back against the state and the system that oppresses it by boycotting it with their money. Bitcoin doesn't see color. Its messaging system heuristics don't care nor can care if you are black, brown, female, or fabulous. Its apolitical nature doesn't see algorithms or names, leveling the playing field for anyone involved. It gives every single individual the pure ability to interact with the protocol to leverage the network to succeed and make it work for you.

Opting out of the money of the State and the oppressive structures it supports is a powerful form of boycott. Embracing a new form of system and doing it with your money is a peaceful protest. The focus of any boycott or strike is to pressure bad actors to change behavior. If you don't want to protest violently, you can accomplish it through your actions with your money.

While protests around the country have galvanized support across the nation for wholesale changes to the violent and unchecked force the police use towards black people and the very citizens that pay them to serve and protect, there is an increasingly large number of the population that is so broken, agitated and destitute from decades of economic inequality and economic hardship that want to use this moment to be heard too. While riots are the voice of the unheard, for any successful change to happen, we most certainly cannot allow destruction and violence by opportunists and looters derail the message. We must constantly be thinking about non-violent and effective ways to push back and rise up against a system that is rigged with the deck stacked against them. Watch this short clip from the #BlackLivesMatters rally in LA over the weekend

If you are tired of politics going round and round and feel stuck between elections cycles and division driven by media and political class or the binary choice of burning it down or having the military babysit us un curfew and Marshall law, what do you do?

By buying Bitcoin, you can voice your displeasure and cripple the money printing machine which gives power to the bad guys and actively steals it from you while distributing it to other people at an extraordinary rate that we can't do anything about. By buying Bitcoin you are funneling money into something that stands for something better. This reduces the potency of the USD, the weapon of inequality, through an alternative system that operates in a different away. This is exactly what we need to do.

As a community, Bitcoiners are effectively united in a global movement or boycott against state-controlled money. By owning Bitcoin and having a stake, you are naturally participating in a peaceful vote



against the dominant financial system by moving your money away from it. Your vote and your protest become meaningful ways to fight a broken, corrupt, destructive system. The price of Bitcoin going up in value creates a price signal that something is wrong. And if that money goes up as more people join the movement, you end up building wealth in the process.

While profit motive certainly drives many towards Bitcoin, I can tell you first hand there is something far deeper and more fundamental that drives Bitcoiners too – *“the possibility of building a parallel, reliable financial system which is functional, open, and independent of governments or unaccountable corporations.”* (Nic Carter, A Most Peaceful Revolution)

If the internet was a country, its currency would be Bitcoin

Thanks to Bitcoin, we now have a non-sovereign, hard-capped fixed supply, decentralized, free-market global currency that anyone can participate in. No one controls it and no one can print it. With Bitcoin, you are taking back power because you know the rules of the protocol and you understand the inflation rate. You are taking back control because now you are the one that can spend it without permission. It's money that's the antithesis to the money that is oppressing and has undeniably made the most progress towards the separation of money and state. The idea of stateless money that anyone can choose to participate in, is one of the most extraordinary creations in human history, offering possibilities for us as humans that never existed before.

While you can be certain governments and their banker overlords won't be giving up their money printing addiction any time soon and the resulting power and control that comes with it, we finally have other options and can choose to opt-out while still be able to pay for things and conduct global transactions. Why does this matter? While people spending and transacting is currently not being censored by the state, it could change down the road. If you're an activist, caught in protest, or associate with groups the government deems hostile, you can quickly become a persona non grata and be cut off from society, similar to Wikileaks in 2012. This makes Bitcoin even more valuable as censorless free speech money in a world where free speech has become more threatened and civil liberties continue to be cracked down on.

Anyone can buy Bitcoin right away. You don't need to be rich or flush with extra cash to buy Bitcoin and get off zero. Because Bitcoin can be divided into 100mm micro-units called Satoshis, you can get started with as little as a \$1 and can continue to save and stack sats(a term for stacking small units of Bitcoin) over time. But opting out and getting off zero is critical. From a technology aspect, the more people adopt Bitcoin there will eventually be a threshold or “Tipping Point” out there somewhere where we can leave that old system behind and have control of the money. Once we have control of the money, we can decide amongst ourselves how to allocate it and better our communities and lives around us. **Fix the money, fix the world.**



Mining for the Streets

By **Diverter “No ID” BTC**

Posted June 8, 2020

Download the original *Mining in the Streets* report PDF.

Simple Guide for Acquiring Bitcoin Without KYC/AML Using ASIC Mining

Introduction

For years the narrative that has been pushed regarding Bitcoin mining is that it's a fool's game, better left to the professional mining farms and big players due to shrinking profitability. This guide aims to show that this is overly simplistic and narrow-minded in its view. In fact, as ways to acquire BTC without going through the dangerous KYC/AML verification process shrink, mining becomes more and more intriguing for the average user. By having the ability to create an account with no real verification required, you can simply hook up ASIC miners, plug them into a mining pool, and begin receiving payouts for your provided hashpower directly into your personally controlled Bitcoin wallet without providing any KYC/AML identifying data to be scraped.





The Skinny on Mining in 2020

We are all aware of the perils of attempting to mine Bitcoin profitably. Between the new hardware that is incrementally released so that you never seem to have the newest version, to the huge mining farms that pop up and fire tons of hash at the chain. It is very important to understand the difference that proper hardware plays in this calculation.

For a solo, or as I like to call it “Garage Band Miner”, it is imperative that the miner purchased be relevant for some time to come. What the home miner wants to keep in mind is to be able to recoup the funds paid to purchase the machine (ROI), and have the machine then still be able to run, and preferably still be producing BTC near or above profitability levels if possible.

It is here I must stress the marked difference in mentality to be taken when entering into this task- Home mining is not a business model. The most profitable Bitcoin miner on the market today, even with free electricity, will net you ~\$10 per day in USD profit at current BTC prices, and cost upward of \$3,000 USD to obtain. If BTC price were to quadruple overnight, that profitability would likewise go up if the hashrate remained the same. As we know, however, that won't be the case. At \$100k BTC everyone that has ever owned a miner will have it fired back up, which then causes a difficulty increase, and profitability stabilizes. What most don't understand is the dynamic ability of the difficulty adjustment makes mining a near perfect mechanism for balancing the market.

So if you plan to begin Bitcoin mining as a business, I sincerely hope you have millions of dollars to get started. If you plan to begin mining as a way to acquire BTC without KYC/AML regulations, and to help maintain the security of the network that you have time and value invested in at the same time, the barrier to entry is much lower. **Knowing the difference between these two is paramount to having a good experience with Bitcoin mining.**



Infrastructure Needs

During mining, electricity is expended and miners rewarded with BTC in the event that a block is “found”. **Thus, the first critical need for mining is an energy source.** This available energy source is also one of the considerations needed when buying your miner.

Most miners require 220 volts (V) electricity to operate at maximum efficiency. There are some miners that, with a proper firmware upgrade, may be able to operate at 110V and achieve normal hash power, but that requires some technical knowledge of the miner, and generally uses a higher number of watts (W) to generate. Some S9’s, for example, may be able to run on 110V, but in the 6.25 BTC subsidy epoch, these miners are generally less profitable at \$0.04/kWh than an S17 at \$0.07/kWh. Having said that, *if in a situation where electricity is essentially free*, they can be useful and have a very low barrier to entry. S9’s can be purchased for <\$50 now due to their limits.

In the US, many residential buildings are not equipped with 220V outlets, but rather use the standard 110V. There are exceptions of course, but for the most part 110V outlets is what you will see. If you wanted to run a larger miner in these conditions, my advice would be to **have a licensed electrician install the 220V outlet and be done with it.** The price tag on this usually runs around \$200-300, depending. I advise against the DIY attitude in this matter, for safety reasons; but understand it can be and is done by some users. I’m sure guides can be found for such things, but as I don’t recommend I won’t be linking.

A 110V-220V converter will not supply the miner with the necessary efficiency in most cases.

- Know your electricity infrastructure beforehand. Visit [here](https://bitmain.com/en/faq/faq-antminer.html) for specifications of various Bitmain Antminers to understand the electrical requirements (Volts & Amps).
- The second critical infrastructure requirement is steady internet access and ethernet connection. You need ethernet cable connection on each miner, if running more than one. The good thing is

ethernet cable can be run for a good deal of distance, so miners do not necessarily need to be in close proximity to the router.

- In addition, these miners are very loud machines, often reaching decibel (db) levels between 60-90db. To set a miner up in the bedroom of your apartment would be like having a conversation while standing near a jet engine. Intolerable. There are ways to mitigate much of the noise, which we will discuss later.
- The final infrastructure piece to keep in mind is the heat generated by the miners. If you have ever been in a dedicated server room, you know that the heat given off by a running computer chip is immense. ASIC miners are no different, and most miners come equipped with intake and exhaust fans designed to help feed air over the working chips to keep them cooled. So, a miner set up in your bedroom will sound like a jet engine and have your entire room feeling like a sauna in short order. This is unacceptable for most.

Infrastructure requirements likely the largest barrier to entry. Make sure you have them covered before buying a miner. If these requirements are not able to be overcome or are economically infeasible, it may be necessary to look into hosting options.

Miners, Miners Everywhere

Your choice of miners depends on your infrastructure abilities and electricity costs. I generally recommend buying new, as longevity of operation is key to achieving ROI, and a miner you buy second-hand may have been run in excessive heat for extended periods, run in especially dusty, humid, or oxidized areas, or otherwise generally abused. The last thing you need is to spend your sats on a piece of equipment that runs for a week then leaves you with a nice looking conversation piece, or just shows up DOA.

However, some of Bitmain's S17 line have had a litany of issues, and repair or return from Bitmain is expensive in shipping alone, nevermind the fact that many people claim to have received back either the same miner they sent in or an equally bad machine.

I can only speak to my personal experience, which is with the S17 PRO 50Th/s model. I absolutely love them. *There is a Telegram group for the growing number of dissatisfied customers of the S17 line, linked [here](#).*

It is worth bearing in mind many factors come into play, such as different facilities and temperatures, setups, etc. From what I have been able to gather, there are far less complaints with PRO model Antminers in general, and I haven't noticed any for the particular 50T model I run. **Several complaints seem to come from the S17+ models.** *Point being, buying a slightly used S17 model from a reputable dealer known to put accurate grades on equipment is probably not a terrible idea for the time being.* This can at least let you know it shouldn't arrive dead and likely runs without issue.

Hopefully Bitmain rights the ship with the S19 model; but if they don't, **MicroBT** will continue to take market share as long as they produce even decent quality miners.

*For a single, Garage Band Miner, there is one miner on the market today that I can confidently recommend. That miner is the **Bitmain Antminer S17 PRO 50Th/s edition**.*

You will note there are several versions of the S17 model, which as mentioned before, Bitmain strategically releases with slightly higher hash rate on each successive miner in an effort to FOMO you into buying new again. If you are paying attention though, as with anything, you find the signal in the noise. **This machine runs on 220V electricity, and will net you a true average of ~51.5th/s at a power consumption of ~2000W.**

This is remarkably efficient. For comparison, the soldier of SHA-256 mining, the Antminer S9, nets the miner 13.5Th/s at power consumption ranging from 1150W-1400W. **So the 50T model provides nearly 4x the hashing power on less than 2x the power consumption.**

That isn't even the most beautiful part of the S17 for the home miner. This version has several settings:

- **Normal-50Th/s @ 1945W**
- **Turbo-Listed up to 62Th/s @ 2250W, actually averages around 57Th/s daily**
- **Low-36Th/s @ 1296W**

For those times when BTC rises sharply in price and the difficulty adjustment hasn't recalibrated yet so you throw every hash you have at it-**Turbo**. To make it through those brutal "crypto winter" bear markets, or for those with high energy costs-**Low**.

The specific numbers for the S17 PRO 50Th/s model can be found [here](#). The efficiency of this miner, coupled with a reasonable price, make it an excellent choice in my opinion. MicroBT Whatsminer M20 and M30 lines have come out swinging back against Bitmain dominance. They generally run a bit higher on energy consumption, but overall Joules/Terahash efficiency remains competitive if not better than Antminer.

The average price for electricity is measured in kilowatts per hour (kWh), and in the US the average is ~\$0.13/kWh. At Bitcoin prices below \$10,000 USD, this makes mining unprofitable at "normal" difficulty and hashrate levels. But that's precisely the problem with the blanket claims often seen regarding the "cost of production" for BTC. The cost of production is dynamic, and varies depending on a variety of factors, including electricity cost, hash rate (which then determines difficulty settings), the amount of transactions producing miner fees, and more. **It is virtually impossible to apply some blanket number to say "Bitcoin mining is profitable above \$X.xx".**

However, we can use mining profitability calculators, of which there are several, to help determine what things look like in reality. I will use [cryptomining.tools](#) which is a site by Scott Offord a Bitcoin mining proponent for many years. So, what does profitability actually look like with the S17 PRO 50th/s model?

Below are the results on today's metrics of price, network hashrate, and difficulty, in normal mode, in USD amounts per day **NOT including mining fees** (Subsidy=6.25 BTC):

Electricity Earned Cost Profit

.07/kWh	\$4.36	\$3.28	\$1.08
---------	--------	--------	--------

Electricity Earned Cost Profit

.09/kWh	\$4.36	\$4.22	\$0.14
11/kWh	\$4.36	\$5.16	\$-0.80
13/kWh	\$4.36	\$6.10	\$-1.74

You would mine around .000453 BTC per day, equivalent to around \$4.36 If your electricity cost is \$0.09/kWh, you would pay around \$4.22 USD per day to run the miner. What does that really mean? It is the equivalent of going into CashApp with \$4.36 and buying the .000453 BTC, except when you back out of the app you aren't broke—you still have \$0.14 remaining. **So while BTC price is \$9,625, you will have paid an exchange rate of \$9,315.** **_You bought at ~3% discount_**.

Looked at another way, you essentially have set up an account on Swan Bitcoin and requested to purchase \$30 of Bitcoin per week in their "Savings" plan. You've obtained .003171 BTC at a cost of \$29.54. You pay your electric bill in USD, you receive BTC. **This is, for all intents and purposes, Dollar Cost Average (DCA) buying.** **_This way though, you have avoided the KYC databases_**.

This may seem like too rosy a picture to paint, so let's look at it from more of a "worst case" type scenario. Difficulty has historically risen in Bitcoin, and in my opinion, is likely to do so for the foreseeable future. The all time high difficulty to this point was ~16.55T. Difficulty rises when more hashpower joins the network, resulting in blocks being mined on average less than 10 minutes apart over a period of 2016 blocks. Conversely, difficulty drops if hash leaves and blocks take longer than the 10 minute target.

Let's assume then that difficulty will be at least as high as 16.55T, and sticking with the worst case let's assume there are no transaction fees to be awarded. Using instead only the subsidy of 6.25 BTC per block and electricity cost of \$0.13/kWh on the mining calculator again we can find what price Bitcoin needs to be in order for the S17 PRO 50Th/s model to be at least break-even. Quick glance might lead you to believe we need all time high prices to breakeven if we're at all time high difficulty and only half the subsidy amount as the last 4 years; but you'd be wrong.

We find that we see break even levels—essentially buying KYC-free at spot market value in a DCA manner—~\$16,225. However, leaving all variables the same but switching the S17 PRO 50Th/s model over to "Low" power mode efficiency, we find that BTC price only need reach \$14,785 to see breakeven. In such a case, the miner would be mining extremely close to the USD equivalent amount of BTC used in the earlier example of \$30/week, since low power at 16.55T difficulty mines ~.001897 BTC @ \$14,785, or ~\$28.05.

Lots of numbers, lots of "what-ifs", and plenty of opportunity to lose the signal in the noise. So let me get you back on solid ground.

Where Do I Even Begin

You may have heard of the cutthroat, competitive, and secretive nature of mining—and it's not entirely untrue if you are speaking about large mining companies or even pools. However, you'll find the community of miners much more receptive and willing to help, as long as you are willing to help yourself.

If you come in expecting to be spoon-fed every little thing to do, have your million questions answered now, or with some sort of idea that you don't have to earn your stripes then you will indeed likely have a rough journey.

Outside that, it's fun and exciting to help others further their Bitcoin journey, and miners are no different. These are bitcoiners, many of them have been for several years. They are also business people, with little desire to waste time and effort on, well, assholes. So don't be one.

In trying to stay off KYC databases, you also want to avoid having your name and information stored with a company such as Bitmain, much like you wouldn't want your info to be held by Coinbase, for example. Luckily, there is a thriving peer-to-peer (P2P) market setup you can leverage to obtain a miner (or 4 😊) without having to hand over too much information to do so.

I feel it's important here to note the distinction between non-KYC and anonymous.

****_Buying something without doing full KYC does not necessarily mean remaining fully anonymous. In my opinion, the most important thing is to keep your name, photo ID, date of birth, social security number, and bank account information off an easily requested database of users, such as one necessarily held by the most used Bitcoin exchanges today._****

Often these exchanges are favored for their convenience and ease of use. I'll skip the whole no KYC only spiel, and assume if you are still reading it's because you understand why it is important.

When dealing in P2P type markets, the trade-off for being able to maintain pseudonymity or not having to do KYC is that the possibility of fraud can dramatically increase. There are ways to mitigate these risks, such as the use of reputation systems and requiring vendors, but not buyers, to complete some sort of verification that may be leveraged against them in the case of fraudulent activity. Such is the case with my favorite-and recommended-market for buying a new generation ASIC Bitcoin miner.

I recommend Hardware Market on Telegram, which can be found [here](#). I encourage all to read the pinned message in order to best avoid being scammed.

**** I do not recommend buying a miner from ANYONE if they are not verified on Hardware Market ****

*There is a command that can be given as **!toprep** which reveals a list of verified sellers .*

You can likely also simply scroll through until you find the list as requested by another, so we don't spam the chat. This means they have undergone KYC essentially, and their info will be handed over to proper authorities in the case of any scam behavior. They have reputation scores to help show the most reputable based on the number of successful interactions and the *quality* of those interactions.

Ads get posted by different sellers and/or the companies they work for, and the miners are listed as new/used, often with grades. They denote whether shipping is included or not, where shipped from, there is often video evidence of the miners hashing, etc. In addition, the group is very well moderated by respectable members of the community and I have witnessed some disputes be worked out and resolutions

amenable to all parties be reached in the end. Everything does not always go perfectly, but this group and its verified members do a wonderful job of doing the best they can to operate smoothly and efficiently.

I recommend this group because it is easiest to branch off into individual companies or sellers from there, since it acts as a sort of central hub. **I do not recommend Ebay for buying miners**, as the setup is not good from a privacy standpoint, and you run a very real risk of receiving a seriously beat up miner. Example of dust filled Ebay miner shown below.

As a quick example, I will pick on Kaboomracks for a bit. Their marketplace can be found [here](#) and the pinned message outlines why they feel buyers should consider them. You will often see them place ads similar to this:

81 qty Antminer S17 Pro 50T for Sale

Used in Excellent Condition, A

\$1299 each all-in which includes domestic shipping includes built-in Bitmain APW9 power supplies no minimum order size ships from Ohio, United States Contact Sales: t.me/kaboomracksNick #kb00737 #used #sha256 #usa June 2nd, 2020 Miners for Sale → t.me/kaboomracks ❄️❄️

It is advised to scroll for ads for miners you would like to buy, rather than post a “Want To Buy” (WTB) ad in Hardware Market. The reason is simple-scams.

Posting a WTB order is open season for scammers to DM with very similar looking profiles to verified sellers

If you send your BTC to these scammers there is no customer service recourse to be pursued. If you scroll for ads until you see one you like, you can click on the links in the ad or the poster themselves to open up a chat that you know is with the correct person. This is because every ad posted in Hardware Market must only be done by verified sellers, and any ad attempted to be posted by an unverified seller is quickly removed, and the poster receives a warning. After 3 warnings, they are banned. Can also click the name of the verified seller directly from the /toprep list. These are the tradeoffs of working around regulations, and it's on us to make them work.

Say you wanted to buy one of the 81 S17 PRO 50Th/s miners at an all-in (shipping to your door in US, in this case) price of \$1,299. Kaboomracks accepts BTC as payment, so you do not have to give over your banking information or reveal your account at all. They will ask of you (as most all sellers will for their own records) some very basic, vanilla information such as your “Name” and “Company Name” or the like.



There is no need for them to verify this generic information, so no need to panic and reveal everything about yourself. There is no “selfie” to submit, no singular honeypot to be mired in. As for the shipping address, this is where your personal threat modeling comes even more into play.

KYC free != Anonymous

If State agents try hard enough in situations such as these, it is likely one may be deanonymized using a shipping address. If that is a concern, I leave it on your own research to find ways of setting up P.O. Boxes or having them set up in different names, or having it delivered somewhere other than your home address. In my opinion, it is very likely enough to keep name, DOB, SSN, bank info, and photo ID off an exchange database. Only supplying a shipping address provides a certain amount of deniability, requiring far more work than sending a single subpoena to an exchange and rounding up 1 million users at once. That part is on you to decide, I advise not making it too difficult, and instead aiming to keep the lowest hanging fruit out of Big Brother’s face. **If you have concerns about these things, have a frank conversation with the verified seller about your issues.** As I said, dealing with fellow bitcoiners generally makes explaining these things much easier than telling Joe Schmoe why you value your privacy. These guys get it.

Once you order and receive the miner, and have verified it is the miner you ordered in the condition advertised, you and the seller will post a final message in a chat group specifically used to increase/decrease reputation. The seller will claim to make a deal with your Telegram username, you will reply to that message with a simple “Confirmed”, and that’s that. You are now ready to mine on.

Hello? Is This Thing On?

Now the fun begins. Let’s assume you are mining at home. Let’s also assume you have a significant other (though I feel like many in this space need only pull a plug and deflate theirs) and are interested in both mining and keeping the spouse. The other assumptions being made are that you have 220V 20A power outlet and a router to connect ethernet to the miner.



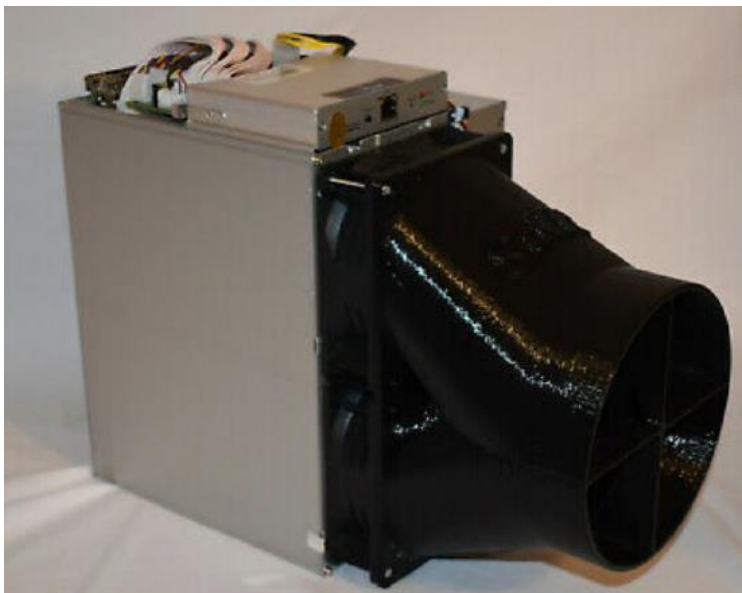
Many new gen miners have two (2) plug in needs for 220V power cords.

They have built-in Power Supply Units (PSU) but need two cords plugged in to operate, not just one, as you can see from the picture on this page. **Further, it is important to note these miners rarely, if ever, come with power cords that are compatible with US power outlets.** I suggest universal adapters, which can be bought for a few dollars usually on Ebay or Amazon to ensure you have the right gear when the

miner arrives. Generally compatible power cords and multi-outlet extension cords are found in Hydrofarms equipment pages, if not able to simply find them in Hardware Market or related channels themselves. They have the CN style outlets, and sell for around \$15-25, example of where to start [here](#).

If you don't have a sufficient amount of CAT-5 ethernet to extend from the router to miner placement, might want to go ahead and pick some up as well. The rest of the supplies needed will really depend on your personal placement of the miner.

Do you have a room that can be kept cool enough to allow your miner to operate? **The cooler you are able to keep your miner, the quieter it will be.** It needs to be above freezing to prevent issues, but if you are able to provide cool enough air for the intake fans to blow over the miner, and able to relieve the exhaust heat as well, the fans don't have to work nearly as hard to keep it cool, and thus move slower and quieter. One way to help mitigate the noise through heat reduction is through the use of 3d printed duct shrouds that can be applied to the outside of exhaust (or intake) fans, attaching flexible ducting, and directing the heated air to a different area. This may sound difficult, but it's actually quite easy. Sellers on Ebay like the one [here](#) offer these shrouds for cheap prices, and they are well made. Will need a bit of cleanup of the rough strands before applying, but work great.



Whatsminer and Antminer may not be compatible, so be sure to check on your miner's specifications before ordering. Usually either be 120mm or 140mm, but check each miner before ordering. Flexible ducting can be picked up or ordered for around \$10-20 online or at Wal-Mart, takes nothing more than a screwdriver to mount it all, *mounts right on the miner using existing screws and holes, no scary drilling or extra parts to worry over.*

Depending on your situation, you may need to go even a step further. Might want to keep your miner(s) "on ice" to try and keep sound low and the spouse happiest. Insert the cooler as a possible sound barrier.



There are some sellers on Ebay offering pre-built coolers, generally they have been custom fitted for S9 miners, so only have a single intake and outake. This can likely translate pretty easily to Whatsminer single-tube ASIC's, or may require some modifications to work for Antminer double-tube miners. *To DIY the entire thing is not a very difficult or costly endeavor, so if going with a cooler, I say just go for it.* Can grab a normal, 38-48 quart cooler from Walmart for \$20-35 in most areas. It is helpful to have a small, hand-held drill with a circular bit, but even to buy all from scratch—cooler, drill, bits, ducting, and don't forget some soundproofing foam—still very likely looking at less than \$100-150 and less than a days work to put all together. Not bad to maintain a happy home. Doing this all yourself works fine, it doesn't have to be perfect. **It's a very simple concept; cool air in, hot air out.** The further you can easily get the hot air out, the better. Remember, we're talking about a miner or two,

not a farm.

There's no investigation coming into the massive electricity use of your home, no heat signature changing dramatically, and no need for professional installation help. It can look as crude as you like. *If it gets cool in and hot out, **mission accomplished.***

Once you have your setup in place, you will need to use ethernet to connect from router to miner. You will need a computer on the same internet connection in order to be sure to find the IP address of the miner. It is a simple process to configure the miner, takes only a couple steps, and is detailed here as well as any of several YouTube video guides. Very "n00b" friendly setup overall. If you do run into problems, again there are several places to reach out to fellow miners for help, including on Keybase .

Pool Selection

Mining pools are ways for many miners from geo-diverse locations to "pool together" their hash rate in an effort to increase chances of winning a block. I won't spend much time on pool types, as it's easy to



understand and a personal choice as to which pool you want to trust with your hash.

I will say this—mining pools have gone and do go broke, and there is a chance you do not receive payout for hash if that happens.

Usually this happens if an FPPS type pool hits an unlucky streak and does not have the Bitcoin required to pay out. Pools such as Slush, running a different type of pool where miners are only paid if/when a block is found, run less risk of going bust. *However, if no blocks found, no BTC earned*, unlike FPPS pools like Poolin for example, where contributing miners get paid from the pool coffers *regardless of the number of blocks found*. There are tradeoffs to each, and it is fiercely competitive. Find more opinions about this subject [here](#) and learn about different pool types [here](#).

Hosting Services

Now we reach a portion with which I am a bit unfamiliar, but I realize may be a necessity for many would-be miners. As a result of too high electricity or simply infeasible infrastructure abilities, hosting services are becoming more widely used and viable options.

My advice concerning hosting boils down pretty simply to this: ***Don't skimp on cost at the expense of reputation.*** If it costs a cent or two more in kWh to host, but is with a reputable host that is far less likely to “take the money and run”, pay the little extra.

Again, we are in a highly unregulated market, which many of us ask for. That means responsibility is transferred more to ourselves to police bad actors and make good decisions. That said, to think you'll get out of Bitcoin without ever having been scammed is likely a foolish dream. Keep the amount low, learn, and spread the knowledge to others.

I'm going to give a bit of info relayed to me by an outstanding (*and criminally underfollowed*) bitcoiner in [CrazyK](#). You may have seen his amazing luck in winning a brand new MicroBT Whatsminer M30S 88Th/s a short time ago. His situation did not allow for him to mine at home, and so he explored hosting options with [Blockware](#). They offer hosting services for new gen miners, as well as the sale/host package deal, for which they offer better kWh cost deals.

CrazyK reached out to Blockware about hosting a single M30S and they were able to accommodate him. The electricity cost was quoted at \$0.067/kWh, and would likely be lower if more miners were hosted or if the miners were bought from Blockware themselves. **Blockware does not actually provide the hosting.** Another company does that, and there is a fairly lengthy, and rather one-sided, contract involved. ***This is going to be necessary for hosting, since you are empowering a trusted 3rd party with control of your machine and hash.*** Luckily for all, CrazyK is planning to do a more detailed write-up on his overall experience, especially regarding hosting. I'm looking forward to that myself. I'll leave many details to him, and paint with a broader brush here instead. There are one-time setup fees, and then ongoing monthly electricity cost, which must be paid in full upfront. The electricity cost then, using M30S specs and the \$0.067/kWh rate, is ~\$180/month. *So the recurring cost for this contract, which is for one year, is that \$180 upfront monthly.*

- *Using current network stats, the M30S in an FPPS pool should mine an average of ~.023929 BTC/month, which at current exchange rate is ~\$230. This means someone hosting a single M30S at these rates is essentially DCA “stacking sats” at a rate of \$57.50/week auto buy, at an exchange rate of 1 BTC=\$7,522. Instead of paying an extra fee on top of spot market value to auto-DCA, you can do it at a hefty discount.*

Sounds too good to be true? It kinda is, seeing as not everyone gets a free machine which is valued at over \$2,000 dropped at their door for free (I'm not at all jealous) But the bigger point is the fact that his experience has been pleasant to this point, and hosting is an actual, viable option if you can't or don't want to go through the trouble of hosting your own machine. Can find out about hosting services using Scott Offord's cryptomining.tools site.

A couple of parting shots about hosting single or small numbers of miners: Some hosting services don't like taking single customers, so check around. *Get a knowledge of how miners work and the fluctuation in hashrate before you get involved*, in order to keep from being the guy that emails to his hosting service 4 times a week asking why their 88Th/s machine is only showing up as 75Th/s when they just checked it. Can watch an actual S17 PRO 50Th/s model running on Poolin (one of mine) [here](#).

As with anything, do not see magic dollar signs and rush into something without understanding all costs involved. That is a sure way to end up disillusioned and “mad at Bitcoin”. Tradeoffs and incentives matter more than most people understand, it pays to learn as much as you can before making any moves.

Are We There Yet?!?!?

Let me bottom line this thing for you. **Bitcoin mining is NOT a get rich quick scheme.**

In fact, I would argue that beginning mining for yourself requires the *most* bullish sentiment of all. To mine, you must put forward a not-so-insignificant amount of upfront money, be it BTC or USD, with the expectation that you will recoup those expenses at some point in the future—much like buying bitcoin. The difference being, you can't just wake up on a Thursday having ‘lost faith’, jump on CashApp and sell all your BTC for USD, turn and walk away.

Investing in mining equipment, infrastructure, and even hosting contracts means it's virtually impossible to just walk away. It is the ultimate test of time preference. If your initial miner purchase takes 2-3 years to make a ROI and be truly profitable, is it worth it? Why not just buy bitcoin and hold it instead? Wouldn't you end up coming out better that way? This [report](#) throws a big wrench in that argument. Past performance is not indicative of future returns, of course.

We are in the beginnings of a new deployment cycle, with the M30S/M30S(+) and S17/ S19 PRO hitting the street now. Their life cycles are still TBD—so the gamble persists. Twitter leaders would have us follow the Stock-to-Flow model predictions, with varying targets between \$55,000-288,000 per 1 BTC within the next 2 years. If so, mining profitability likely sees a spike, newcomers FOMO in chasing a dream, and (by then) ‘seasoned’ vets have piled sats up regularly the whole time. In addition, the fact you've been able to avoid full KYC compliance sets you up for the ability to avoid something else as well—capital gains taxes.

If buying through 3rd party centralized exchanges that are willing and in most cases obligated to turn over the holdings and tax liabilities of users, defunding the government becomes much harder. If looking to cash out from years of HODL'ing when BTC hits \$288k, you must understand how much bigger (and thus how much more important and scrutinized by government) Bitcoin will be. **How much more interested in holders identity and tax liabilities will the State likely be?** How willing, and more importantly how *able*, are you to resist attempts to compel disclosure and pay huge taxes on those gains?

Will the % of gains lost to taxes be more or less than the premium you may have paid to acquire those BTC in a non-KYC fashion? And if not so much interested in gains, but more so in taking power from the State, how much are you able to contribute to the security and decentralization of the Bitcoin network? What kind of future do you see for Bitcoin and bitcoiners in an adversarial environment?

The time to strike is upon us, immediately post-halving coinciding with new miner life cycles beginning and chips perhaps approaching uncertainty principle levels. Each bitcoiner must decide for themselves the depth of their interest in BTC; just be sure you're actually doing that.

Don't fall victim to the narrative pushers that would have you believe mining is "too hard", "too expensive", or "better left to the big players". Sounds an awful lot like the same thing bankers and governments tell the masses about fiat money and economics now, doesn't it? Don't let me influence you—that's not my job. I just want the knowledge to be out there for anyone to pursue for themselves. And I certainly don't want the DM's from people that spent too much on a shitty miner and now hate Bitcoin and the asshole that inspired them to buy!

I do want adversarial thinkers, narrative challengers, and fighters. This Bitcoin thing was founded and secured by such minds, and it's my opinion if Bitcoin continues to succeed, it will be because of the next wave of these minds and their contributions; both in software and code they push *and* in security and hardware run by users. Click the links, find some resources, and decide for yourself. Help is out here in the form of guides and personal interaction if you know where to look. I hope I have at least provided a bit of illumination for those paths.

Stay adversarial, frens.

Additional Links

- [Mining Calculator](#)
- [Difficulty Calculation Site](#)
- [Twitter Profile](#)
- [Keybase Profile](#)
- [Telegram](#)



Bitcoin: Reform or Revolution? Part 1

By Solairis

Posted June 9, 2020

>You will not find a solution to political problems in cryptography.

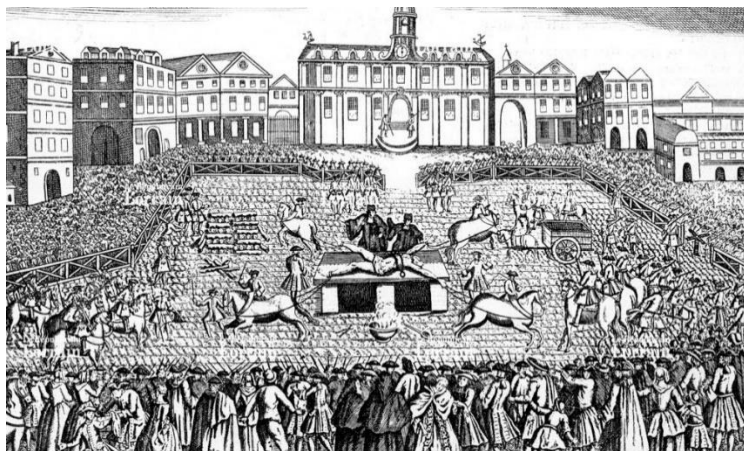
Yes, but we can win a major battle in the arms race and gain a new territory of freedom for several years.

Governments are good at cutting off the heads of centrally controlled networks like Napster, but pure P2P networks like Gnutella and Tor seem to be holding their own.

-Satoshi Nakamoto, The Cryptography Mailing List.

“The day will be hard,” said Robert-François Damiens the morning of his execution in consequence of having tried to assassinate King Louis XV of France. He was condemned to be “taken and conveyed in a cart, wearing nothing but a shirt, holding a torch of burning wax weighing two pounds;” then, “in the said cart, to the Place de Grève, where, on a scaffold that will be erected there, the flesh will be torn from his breasts, arms, thighs and calves with red-hot pincers, his right hand, holding the knife with which he committed the said parricide, burnt with sulphur, and, on those places where the flesh will be torn away, poured molten lead, boiling oil, burning resin, wax and Sulphur melted together and then his body drawn and quartered by four horses and his limbs and body consumed by fire, reduced to ashes and his ashes thrown to the winds.”

You may or not like Michel Foucault’s political career or ideas, but what is indisputable is the novelty of his exhaustive work in deciphering power relations. In his book “Discipline and Punish” he begins by describing the martyrdom of Damiens. Foucault quotes the testimony of several people and it seems that the execution was much crueller than was dictated.



The execution of Damiens

Nowadays the justice system applied by the state may seem kinder in comparison to thunderous and sadistic practices of the 16th century. Many who appreciate this transformation would attribute it to an enlightened position of greater humanization and progress. Foucault disagrees.

Let’s start with Damiens. Why was his execution so violent and excessive? Yes, he attempted to kill the King, but to us, the punishment seems beyond the measure of his crime.

It will be necessary to understand that punishment was and is not merely punitive retaliation, but a **political ritual**.

In the past, the laws were identified as the will of the sovereign. If you broke the law, you were basically rebelling against the sovereign's persona. And to do so, you were threatening the monarch's integrity by not respecting his or her law, thus it would have been necessary to exercise a symbolic and very public show of violence.

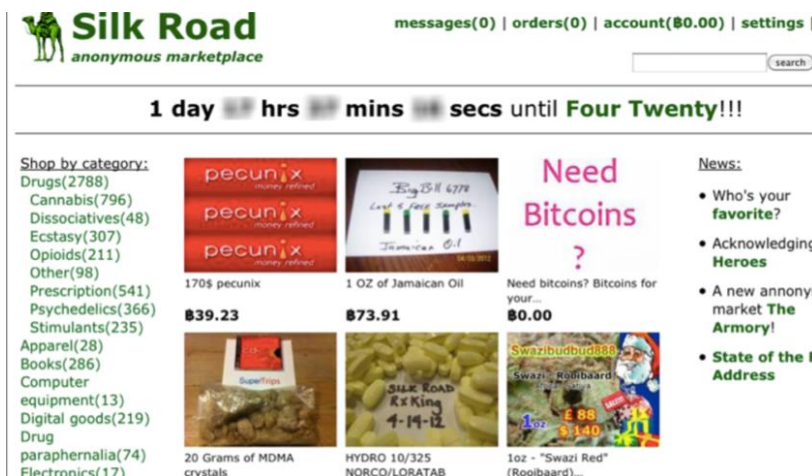
The problem is that while this symbolic show demonstrates the power of the king, it also demonstrates its limitations. Every time someone committed a crime the machinery of punishment had to be reactivated. The sovereign's power was great but inefficient.

There was always the risk that people would sympathize with the condemned and start riots and disasters in support of him or her, motivated again, by the irregular and inefficient execution of power.

The prison system developed in the age of enlightenment (now the law identifying itself with the Social Contract instead of the sovereign) made the exercise of justice more methodical and meticulous in its administration. A system that can be executed efficiently, in private, and with predictable consequences. However, the political ritual is not gone. There are thousands of cases that could be cited to exemplify this, but a very significant one was the double life imprisonment plus 40 years without the possibility of parole that Ross Ulbricht, founder of Silk Road, received in 2015.

For those that may not be familiar with Silk Road, it was an e-commerce website for voluntary exchanges, with emphasis on user security and anonymity. It was launched in 2011 and employed two key technologies: Tor and Bitcoin. Ross envisioned Silk Road as a free-market economic experiment, an open platform driven by its user community. He believed that "people should have the right to buy and sell whatever they wanted so long as they weren't hurting anyone else."

The guiding philosophy of the site was that it is no one else's business who you are or what you are buying and selling as long as the transaction is voluntary and no third party gets harmed. You could find all kinds of items on the site, both legal and illegal. Individuals could purchase drugs like Cannabis and mushrooms straight from small growers around the globe. However, things like weapons or child pornography were emphatically prohibited.



Silk Road's Home Page

Ulbricht, being an American citizen, knew he was doing something risky. There was no way to avoid a sentence against him. But why such an excessive exercise of power? It gets more intriguing when you look at the information liberated by the team advocating for Ross' release. Ross was only the founder of the site, and he wasn't

even managing it by the time the marketplace attracted more traffic and therefore more volume of money. Furthermore, it is presumed that “the prosecution’s forensic evidence was below amateur level”; besides having violated Ross’ rights to obtain this evidence, the judge precluded any mention of the corrupt agents at the core of the investigation, thereby hiding them from the jury.

Look, a character like Gilberto Rodríguez Orejuela, a former Colombian drug lord and leader of the Cali Cartel, only received a 30-year sentence despite having been guilty of part of the bloodiest drug war between Colombia and the United States in the 20th century. El Chapo Guzmán, the most wanted man after Bin LaDen’s death, received a single life sentence just last year. These are a few popular examples, however, there are many drug traffickers sentencing cases that can be quite questionable.

Since it appears that the precedents for punishment did not apply to Ross’ conviction, what were the prosecutors’ motivations for levying such an excessive sentence?

Well, in June 2011, Democratic Senators Charles Schumer of New York and Joe Manchin of West Virginia wrote to Attorney General Eric Holder and Drug Enforcement Administration head Michele Leonhart in a letter that expressed concerns about the Silk Road. Senator Schumer asked federal authorities to shut down the site and said this about Bitcoin: “It’s an online form of money laundering used to disguise the source of money, and to disguise who’s both selling and buying the drug.”

By September 2013, Preetinder Bharara, US Attorney in the southern district of New York, on the recommendation by Senator Schumer, started leading the prosecution against the notorious Silk Road’s “operator”.

Ross was arrested in October 2013 in San Francisco thanks to a joint investigation by the FBI, and several other US law enforcement agencies. Bharara made sure the case was brought to his territory in New York, rather than California.

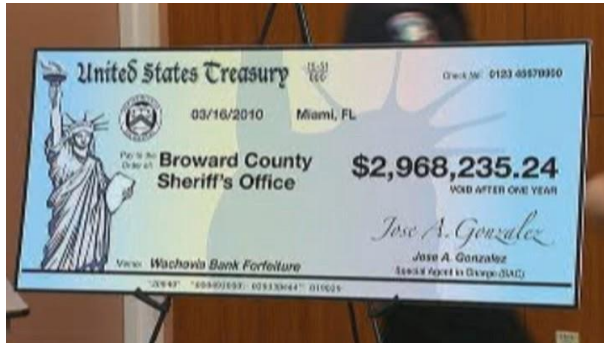
After being arrested and denied bail, one of the arresting agents threatened him that he [the agent] would recommend that the judge sentence Ross to life in prison without parole but pleaded guilty of many charges, including murder-for-hire and money laundering. Ross refused to do so.

In February 2014, congressional and financial regulatory hearings floated the idea of new regulations on Bitcoin that would treat it as a more or less traditional currency, subject to the same anti-money-laundering laws as any other form of money.

What bothered the people in New York, in addition to drug commercialization, was the potential use of Bitcoin for money laundering. Even though it is still the case that most money laundering occurs in traditional finance: Mexico’s Sinaloa cartel and Colombia’s Norte del Valle cartel laundered between them \$881 million through HSBC. The results? No senior executives were admonished or prosecuted. HSBC of America “only” had to pay a fine of \$ 1.9 billion dollars in 2012, representing 5 weeks of earnings, and they were allowed to continue operations, business as usual.

There was a similar and particularly scandalous case with Wachovia Bank (Acquired by Wells Fargo in 2008) back in 2004–2007. Some sources declared that \$380 billion were laundered for Drug Cartels. The largest violation of the Bank Secrecy Act, an anti-money-laundering law, in US history. The resolution? a

160 million settlement was achieved and no banker or individual was jailed, punished or brought to account over this grand scandal.



Wachovia checks to South Florida as part of the \$160M settlement.

February 4, 2015. “You sought... to put yourself above the law,” the Judge declared. [You asserted that you] were better than the laws of this country. (...) I make this judgement mindful of... the needs for the severest possible penalty to be imposed,” she stated before issuing her sentence to Ross. “There

must be no doubt that lawlessness will not be tolerated.”

And we already know how it ended.

Bitcoin is dangerous, but not dangerous in the same way as drug lords, terrorists or other violent offenders. These profiles are part of a convenient narrative used every time the government in turn needs to obtain public or specialized support to justify an extension of capacities or greater collection of resources that just prolongs the cycle of violence. Bitcoin is dangerous since it puts into question something very profound: the symbolic and material monopoly of money as we knew it. An entity that only belonged to the state and that had been hegemonized by the United States for just under a century as no other civilization had done in the history of humanity.

Senator Joe Manchin would comment “This virtual currency is currently unregulated and has allowed users to participate in illicit activity, while also being highly unstable and disruptive to our economy”. I don’t think the senators have thought that Bitcoin, just two years old when they denounced it for the first time, had the potential to overcome or rivalize the US dollar as the world’s reserve currency. But I think they did consider the existence of something like Bitcoin as a kind of heresy. And Silk Road, with the help of Bitcoin and Tor, conceived a different type of market removed from the controls of state taxation and regulation, thus they decided to exercise a symbolic show on Ross.

I mean, the money from the big cartels pay taxes thanks to the big banks, right?



“In such epochs where the highest values of life — our peace, our independence, our basic rights, all that makes our existence more pure, more beautiful, all that justifies it — are sacrificed to the demon inhabiting a dozen of fanatics and ideologues, all the problems of the man who fears for his humanity comes down to the same question: how to remain free?”

-Stefan Zweig, Montaigne

The Death of Socrates

The death of Socrates, caused by an unfair trial, some say, is one of the most important in Western history, only below Jesus. Despite not having formulated very complex ideas as Plato and Aristoteles did, he laid the foundations for a lifestyle that would change the way we see the world, forever.

Fearless of death and his own reputation. Socrates was a man that left no traditional idea unchallenged, asking difficult questions to the point of being quite annoying. And that's why he got killed, not on any whim, but because he represented a risk, a danger to the power structures in Athenian society.

Nietzsche said that the Greek aristocrats referred to themselves as "We, the truthful." Which means that they considered themselves as the bearers of the truth, and should not be questioned.

Some say that Bitcoin is apolitical. Maybe we can't get a Nolan diagram out of our pocket and ask Bitcoin to point out where it feels most comfortable. But what we can understand is that **Bitcoin is the Socratic Quest made software.**

A group of cypherpunks expressed through code: I don't trust in your institutions, I don't trust in your laws, I don't trust in your ability to follow those laws, I don't trust in your intentions, in your goals, I don't trust in your power to influence my wealth, property and life. I don't trust you.

Provocative ideas become something else when they do not only seek to be annoying or challenging but have an underlying intention of change.

The existence of Bitcoin evokes change? If yes, what kind of change?

Special thanks to Bitdov from Bitcoinherios, Giacomo Zucco, Auriol from Bitcoin Center Korea, Chelsea Palmer & Paul Shapiro for the review and editing of this essay.

Not trusting does not prevent us from resisting tyranny. #FreeRoss.

Bitcoin Has to Be for Everyone

By **Brian Harrington**

Posted June 12, 2020

#bitcoin has to be for everyone There is no alternative The legacy system is failing The world is literally demanding new solutions, everyone is frustrated w/ oppression

Look at what's happening with the autonomous zones, and talk of tax protesting, and talk of defunding institutions People know that voting and politicians are a joke, people know the current game is rigged

If you're even saying the word #bitcoin and you think you have zero understanding, the fact that you're saying it and interested for some reason is huge, you know there is something here And even more than that you know the current status quo is rigged

When you choose to believe #bitcoin is too complicated for everyone so only some will get it and only some will find it useful that doesn't feel like it's big enough then If that's your mindset I would challenge you to dream bigger

I don't think the revolution can half moon, like humans are either able to take back our wealth and time and labor from corrupt institutions or we can't?

The internet is for everyone, Jesus is for everyone, country specific revolutionary wars are for everyone in that country. Like that's how big #bitcoin is

If only a few people are able to secede and be free we are falling short of our potential If only we are going to get rich in USD and pay cap gains we are falling short of our potential

The ability to send value peer to peer digitally no middle men stealing your labor, time, and wealth is a completely gigantic thing that after 11 years still is not fully figured out

If you're a #bitcoin user and are feeling discouraged for not getting it or you have concerns about concentration of wealth in the new system or concerned with swapping one pair of elites for a new pair of elites Your position is valid

Your concern is valid I'm concerned with it too In the fight against tyranny we need everyone we can get The revolution is for everyone I want you to use #bitcoin I want you to take your wealth, labor, and time back from the people stealing it from you

I want you to join the fight I want you to join the revolution with me #bitcoin is for everyone I'm dumping the tea in the harbor, I'm not paying the tax anymore to a corrupt system Please join me Do it for yourself and do it for your family

#bitcoin is bigger than just a hot stock that might go up, it's bigger than just a way to make money It's changing the way labor and tax and commerce agreements between humans can be set up It's not a way to make money one time, it's a brand new paradigm shift

#bitcoin has the potential to defund oppression and set people free You can fully control your value after working for it rather than having it erode from fees and political decisions

Some people already live in this reality of earn, spend, and save with #bitcoin They report back that it is freeing and the friction to do it with more convenience is being eroded every day as more people switch over

Some people are holding #bitcoin and not living off it yet because their employers won't pay them in Bitcoin yet This is legitimately a problem, this is a current speed bump. People are aware and working on this

Whether you're living off #bitcoin now or waiting to live off it in future your participation is good and appreciated Both these actions improve the value of the alternative system that again literally must survive because there's no other option

This thread is an invitation Different people will say different things about #bitcoin in the same way they say different things about Jesus, the internet, and revolutionary wars You are invited and encouraged to participate in the Bitcoin parallel economy

#bitcoin is different than the legacy system in that cancel culture has a hard time existing on the network and in fact doesn't at all Some Third parties on top of Bitcoin still engage in certain types of cancel culture which is frustrating

At the core when using certain options BTC transactions are impossible to censor That's what makes it so radically different and what makes it for everyone

Even enemies can use #bitcoin at the same time and not have a way to censor the other person or take away their ability to transact

The world is desperately demanding this solution, we all have experiences of being treated unfairly by a banking or government third party #bitcoin fixes this

If you're stalled with your #bitcoin progress or you feel like after using it you may be being censored or not getting the full experience try a new wallet or a new exchange

Wallet software and exchange software is different than the #bitcoin software The developers of that software can set their own rules Sometimes those rules can be frustrating and it can feel like you're back in the legacy system

I have experienced this frustration It's hard to know what to do The frustration doubles when you ask for help and are told that maybe #bitcoin just isn't for you

I genuinely believe the opposite of that I think and believe if you're reading this right now that #bitcoin is for you and I think it's useful for you And I won't even say in the future, I believe it's useful to you right now

I believe #bitcoin can help you right now The reason is because the current value transfer system or banking system connected to the government is rigged That's an unfair game, the sooner you get out of that game the better

The legacy banking system tied to the government is a den of thieves These institutions do not promote your health and freedom, they promote your imprisonment Use #bitcoin and get away from them

Then vote with your #bitcoin and challenge products built on Bitcoin to be open and transparent and built for everyone

Sometimes it's helpful to see how others are using #bitcoin I think of my finances in three stacks 1. USD that I use for bills/taxes 2. BTC deposits w/ a Bitcoin bank called BlockFi 3. Samurai Wallet that I run this thing called whirlpool on before spending

1. USD is important because it's the current unit of account for the world, works best to be a good budgeter in USD so then you can lean into trying out different #bitcoin set ups without worrying about living off Bitcoin yet

2. Bitcoin deposits are important because I still like to have a banking type feel with some of my funds and the place I chose gives me the ability to get a USD loan if I need it in the future, added flexibility I like

3. My Samurai Wallet stack is the stack that is the most fun and the most active participating focus for me at the moment because it deals w/ earning and spending #bitcoin This is where when paired w/ a node you keep at your house, you become your own bank

When I do jobs for #bitcoin I get the funds sent to me using Samurai Wallet because it's the most private wallet at the moment When used correctly, others can't see the amount or who is paying me This is the opposite of the current banking system that mistreats their users

That's the way that I #bitcoin budget and I'm working on moving more commerce from bucket 1 to bucket 3 The more I can transact on things I need with Samurai Wallet instead of USD the less I will be paying institutions that don't have my best interest at heart

Bitcoin is for everyone, even enemies, and even people that have nothing in common except wanting freedom The incentives to work together on #bitcoin are more powerful than any other thing on earth right now looking to disrupt established institutions

Lots of people will argue about this, it's not rainbows and pancakes on the way to disrupting entrenched corrupt systems, I'm not laying out this thread naively thinking a lot of people believe this is possible So many #bitcoin users don't even believe this is possible

I think it's worth it to try and every sign I see points towards it being possible #bitcoin is a huge gigantic deal I want to invite you to look at it, touch it, use it, earn, save, and spend it It's not a toy, it's not a game, it's a revolution And the revolution is for you

Bitcoin is Antifragile

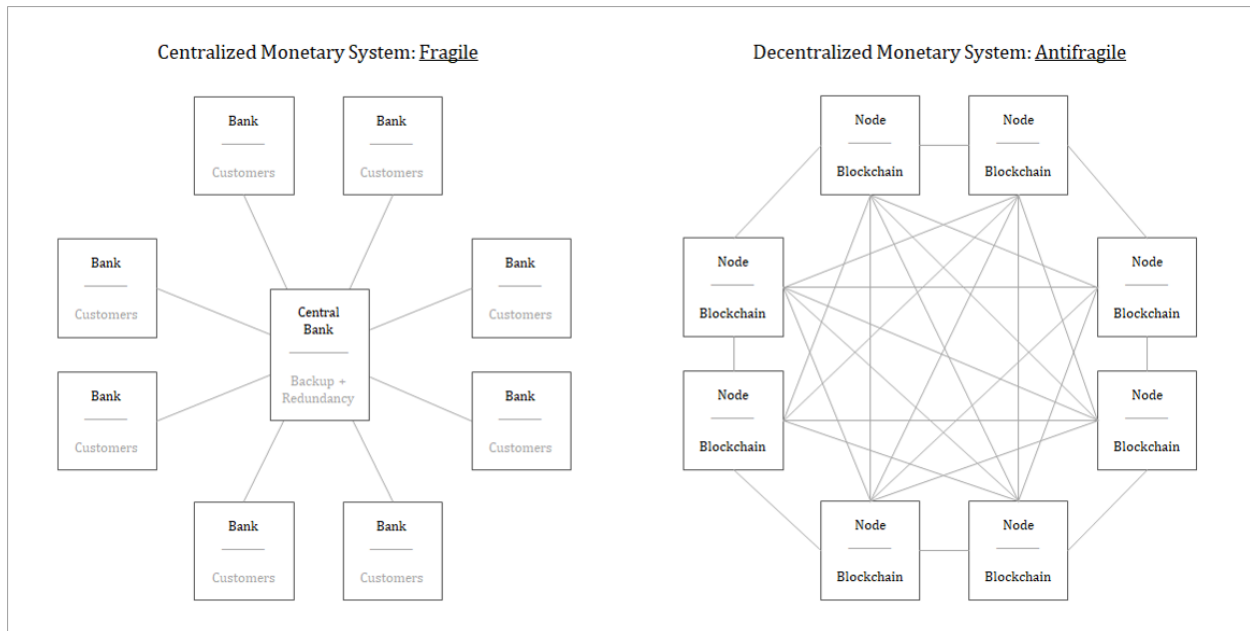
By Parker Lewis on Unchained Capital

Posted June 12, 2020

AUDIO VERSION BY BITCOIN AUDIBLE

If one thing is certain, it is that bitcoin is humbling. It humbles everyone. Some sooner than others, but everyone eventually. Individuals you respect may have called bitcoin a fraud or compared it to rat poison but if it hasn't been walked back yet, it will in time. For most everyone first considering bitcoin, the reality is that the proper context to evaluate it is practically non-existent, even for the most revered financiers of our time. Is bitcoin like a stock, bond, tech startup, the internet or merely a figment of everyone's imagination? At first glance, bitcoin admittedly makes very little sense. It is very reasonably believed by many to be one massive collective hallucination. There exist two fundamental problems. Almost everyone lacks the baseline to evaluate bitcoin because there has never been anything like it, and very few, prior to bitcoin, have ever consciously considered what money is. Every day, people evaluate whether to invest in stocks, bonds or real estate, or whether or not to buy a home or car, or whether to purchase some consumer good, or conversely, whether to save. While there are exceptions to every rule, practically everyone is unequipped to evaluate bitcoin because it does not fit any prior mental framework. It is like asking someone with no concept of mathematics what $2 + 2$ equals. It may be obvious to those that know math, but if not, it's unrelatable. To make it even more difficult, bitcoin is so abstract an application and so far from a tangible phenomenon, that it is like staring into the abyss. Bitcoin is both difficult to see and impossible to unsee once discovered. But often the path from one end of the extreme to the other is a journey, where the impossible first becomes possible, then probable and ultimately inevitable.

Eventually, some chord is struck or some dot connected. As the fog begins to lift, there naturally remains the idea that, while bitcoin is possible, it is surely subject to high degrees of chance and more likely to fail than succeed. It is perceived to be inherently fragile and risky. Many believe that bitcoin could vanish as quickly as it appeared on scene. At the beginning of the journey, it seems to live somewhere between an aspiring long-shot and just one unidentified silver bullet away from complete and utter collapse. Bitcoin is novel and it is often thought of as untested and unproven. Launched in 2009, bitcoin seemingly lacks permanence. It is not yet anchored in time. But on the other hand, bitcoin has been around for going on twelve years and has a total purchasing power (or value) of \$180 billion. Twelve years of operating history and hundreds of billions in value may still be an upstart, but it is far from untested and unproven. Instead, it is thriving in the wild without any central coordination, and it is the lack of central coordination that gives bitcoin its lifeblood; decentralization not only allows bitcoin to function, but it is also what causes it to gain strength rather than falter when stressed.



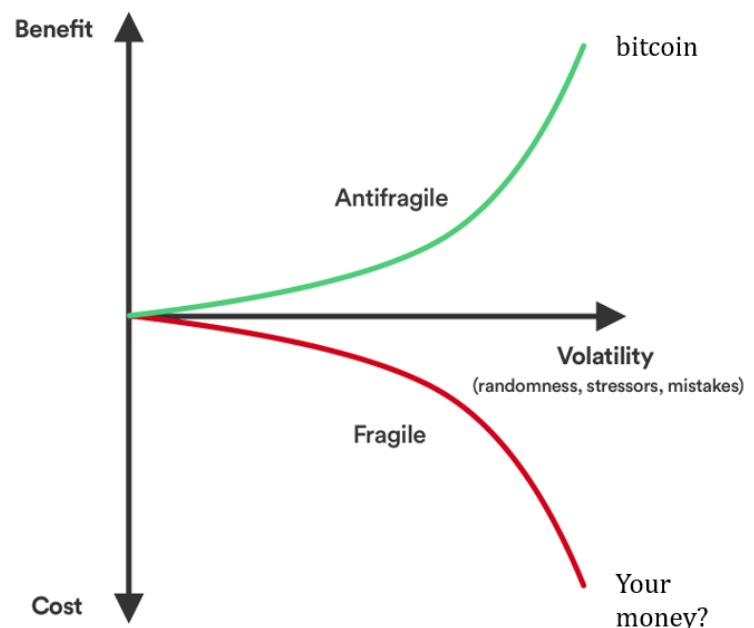
That bitcoin is natively digital and powered by computers running software capable of being shut down lends to the default impression that bitcoin is inherently fragile. The mental image of a computer network being unplugged creates the false sense that one day and suddenly, somehow bitcoin as a system could cease to exist when the opposite is true for the very same reason. That bitcoin both exists everywhere and nowhere, that it is controlled by no one, that anyone is capable of running the open source software from anywhere, and that hundreds of thousands of people do, relied upon by tens of millions (and growing) is what gives bitcoin permanence. With no single point of failure, bitcoin is practically impossible to stop because it is impossible to control, and it is a dynamic system that only becomes more redundant and further decentralized in time and with increasing adoption. In short, bitcoin is more permanent than risky because it is an antifragile system. An idea popularized by Nassim Taleb, antifragility describes systems or phenomena that gain strength from disorder, which is bitcoin to its core. There is no silver-bullet that kills bitcoin; there is no competitor that can magically overtake it; there is no government that can shut it down. But it does not stop there; each attack vector and shock to the system actually causes bitcoin to become stronger.

“Some things benefit from shocks; they thrive and grow when exposed to volatility, randomness, disorder, and stressors and love adventure, risk, and uncertainty. Yet, in spite of the ubiquity of the phenomenon, there is no word for the exact opposite of fragile. Let us call it antifragile. Antifragility is beyond resilience or robustness. The resilient resists shocks and stays the same; the antifragile gets better. This property is behind everything that has changed with time: evolution, culture, ideas, revolutions, political systems, technological innovation, cultural and economic success, corporate survival, good recipes (say, chicken soup or steak tartare with a drop of cognac), the rise of cities, cultures, legal systems, equatorial forests, bacterial resistance ... even our own existence as a species on this planet. And antifragility determines the boundary between what is living and organic (or complex), say, the human body, and what is inert, say, a physical object like the stapler on your desk. [...] The antifragile loves randomness and uncertainty, which also means—crucially—a love of errors, a certain class of errors.” – Nassim Taleb, Antifragile

Bitcoin is an adaptive and evolving system; it is not static. No one controls the network and there are no leaders capable of forcing changes onto the network. It is decentralized at every layer, and as a result, it has shown to be immune to any type of attack. However, it is not just immune to attack or errors, bitcoin actually becomes stronger as: i) external forces attempt to influence or coopt the network; ii) as individuals within the network make errors; and, iii) as a very function of its volatility, which is often perceived to be a limiting, if not critical, flaw. As bitcoin survives shocks and as individuals learn from errors and adapt to its volatility, bitcoin becomes tangibly more reliable; its demonstration of resilience and immunity causes trust to be reinforced in the network, which increases adoption and makes bitcoin more resistant to future attack or individual errors. It is a positive, self-reinforcing feedback loop. With every failed attempt to coopt or coerce the network, the bitcoin protocol hardens and confidence increases. Every time bitcoin doesn't die, that very event propels bitcoin forward, and in a fundamentally stronger state than previously existed.

Each exogenous shock to the network provides learnings that cause bitcoin to adapt in a spontaneous way, which can only be endemic to a decentralized system. Because bitcoin is decentralized and because it becomes increasingly decentralized as a function of time (and adoption), not only is there no single point of failure, but the increasing levels of redundancy ensure network survival and fortify it against future attacks. There is a positive correlation between time and the degree of network decentralization. Similarly, there is a positive correlation between the degree of decentralization and the network's ability to fend off more formidable attacks. Essentially, as the network becomes more decentralized over time, it also becomes resistant to threats it may not have been capable of surviving in prior states.

Separately, each error within the system is isolated to the responsible parties, and as bitcoin grows, each potential point of failure becomes less critical to the proper functioning of the network as a whole. Weak points in the network are sacrificed and the system strengthens in aggregate. The entire process is made more effective and efficient because it is never a conscious decision. It is simply structural to the system architecture. No one picks winners and losers. Decentralization eliminates moral hazard and ensures system survival at the same time. At all times, network participants are maximally accountable for their own errors. There are no bailouts. Incentives and accountability optimize for innovation and naturally drive toward consistently better outcomes in aggregate. It doesn't eliminate error, but it ensures that errors are productive, as the mere fact of survival affords that the network as a whole has the opportunity to adapt to threats and to immunize around them. Whether borne from exogenous shocks or internal



errors, bitcoin feeds on disorder, stressors, volatility and randomness, collectively a hallmark of an antifragile system.

Bitcoin Benefits from Disorder

The lack of social order in bitcoin may be its single greatest asset. There is no CEO of bitcoin nor is there a centralized authority that controls it. There is no person or organization to drag in front of Congress, whether to answer questions or demand action. In fact, there is no Congress or legislative body with any influence over bitcoin, preferential or otherwise. It does not mean that any individual or company is immune from influence; nor does it prevent any country from attempting to regulate (or ban) bitcoin, but disorder insulates the network from external threats. While Facebook's Libra is fundamentally plagued as a currency for reasons independent of government influence, the CEO and other top executives were quickly brought before Congress soon after its announcement to answer questions and with key legislators demanding the project be delayed, if not scrapped, over concerns of "national security" and other regulatory issues. It is not that CEOs and companies cannot coexist with government; instead, it is that the mere existence creates influence that could never exist in bitcoin at a protocol level, and the absence of which allows bitcoin to be viable as a currency.



"The root problem with conventional currency is all the trust that's required to make it work. The central bank must be trusted not to debase the currency, but the history of fiat currencies is full of breaches of that trust." – Satoshi Nakamoto (February 11th, 2009)

With no central counterparties controlling the network, bitcoin functions on a decentralized basis and in a state that eliminates the need for, and dependence on, trust. Its distributed architecture reduces the network's attack surface by eliminating central points of failure that would otherwise expose the system to critical risk. By being built on a foundation of social disorder and only in the absence of control is bitcoin able to function on a secure basis. It is the precise opposite of the trust-based central bank model. Bitcoin is a monetary system built on a market consensus mechanism, rather than centralized control. There are certain consensus rules that govern the network. Each participant opts in voluntarily and everyone can independently verify (and enforce) that the rules are being followed. If any market

participant changes a rule that is inconsistent with the rest of the network, that participant falls out of consensus. The network consensus rules ultimately define what is and what is not a bitcoin, and because each participant is capable of enforcing the rules independently, it is the aggregate function of enforcement on a decentralized basis that ensures there will only ever be 21 million bitcoin. By eliminating trust in centralized counterparties, all network participants are able to rely upon and ultimately trust that the monetary policy is secure and that it will not be subject to arbitrary change. It may seem like a paradox but it is perfectly rational. The system is trusted because it is trustless and it would not be trustless without high degrees of social disorder. Ultimately, a spontaneous order emerges out of disorder and strengthens as each exogenous system shock is absorbed.

For example, in 2017, there was a civil war of sorts that emerged in bitcoin. Many of the largest companies that provide bitcoin custody and exchange services aligned with large bitcoin miners that controlled 85%+ of the network's mining capacity (or hash rate) in an attempt to force a change to the consensus rules. This group of power brokers wanted to double the bitcoin block size as a means to increase the network's transaction capacity. However, an increase to the block size would have required a change to the network consensus rules, which would have split (or hard-forked) the network. As part of a negotiated "agreement," the group proposed to activate a significant network upgrade (referred to as Segwit - an upgrade that would not change the consensus rules) at the same time the block size would be doubled (which would have changed the consensus rules). With most all large service providers and miners onboard, plans were set in motion to effect the changes. However, a curve ball was thrown when a user-led effort prompted the activation of the Segwit network upgrade without changing the network consensus rules and without increasing the block size (read more [here](#)). The effort to change the network's consensus rules failed miserably and bitcoin steadily marched forward undisturbed. In practice, it often cannot be known whether bitcoin is resistant to various threats until the threats present themselves. In this case, it was disorder that prevented coordinated forces from influencing the network, and at the same time, everyone learned the extent to which bitcoin was resistant to censorship, which further strengthened the network.

Before Segwit2x Failure - Industry Executive



Editors Note: This is not criticism of Ted Rogers, but rather a recognition of leadership in articulating a perspective that changed following the Segwit2x hard-fork fail, helping to educate others.

After Segwit2x Failure - Industry Executive



This episode in bitcoin's history demonstrated that no one was in control of the network. Not even the most powerful companies and miners, practically all aligned, could change bitcoin. It was an incontrovertible demonstration of the network's resistance to censorship. It may have seemed like an inconsequential change. A majority of participants probably supported the increase in the block size (or at

least the idea), but it was always a marginal issue, and when it comes to change, bitcoin's default position is no. Only an overwhelming majority of all participants (naturally with competing priorities) can change the network's consensus rules. And it really was never a debate about block size or transaction capacity. What was at stake was whether or not bitcoin was sufficiently decentralized to prevent external and powerful forces from influencing the network and changing the consensus rules. See, it's a slippery slope. If bitcoin were susceptible to change by the dictate of a few centralized companies and miners, it would have established that bitcoin were censorable. And if bitcoin were censorable, then all bets would be off. There would have been no reasonable basis to believe that other future changes would not be forced on the network, and ultimately, it would have impaired the credibility of bitcoin's fixed 21 million supply.

That the most powerful players in bitcoin could not influence the network reinforced its viability, and it was only possible because of the disorder inherent to the system itself. It was impossible to collude or to coopt the network because of decentralization. And it did not just show bitcoin to be resilient, the failure itself made the network stronger. It educated the entire network on the importance of censorship resistance and demonstrated just how uncensorable bitcoin had become. It also informs future behavior as the economic costs and consequences are both real and permanent. Resources to support the effort turned into sunk costs, reputations were damaged, and costly trades were made. All said, confidence in bitcoin increased as a function of the failed attempts to control the network, and confidence is not just a passive descriptor. It dissuades future attempts to coopt the network and drives adoption. Increasing adoption further decentralizes the network, making it even more resistant to censorship and outside influence. It may seem like chaos, but really, social disorder was and will continue to be an asset that secures the network from unpredictable and undesired change.

Bitcoin Benefits from Stressors

Attempts to influence the network consensus rules may be the most acute stressor, as it is these rules that underpin the entire system and create order out of disorder, but bitcoin is consistently exposed to a myriad of smaller stressors that similarly strengthen the network as a whole and over time. There are many different forms of stress, but because bitcoin is exposed to stress on a consistent basis and of a wide variety, it forces the network to constantly adapt and evolve while also building its immune system from the outside in.

Type of Stressor	Example	Impact/Outcome
Consensus Rules	<ul style="list-style-type: none"> • Segwit2x Civil War • Bitcoin Cash Hard-Fork 	<ul style="list-style-type: none"> • Bitcoin proves to be censorship resistant • Bitcoin wins, strengthens
Government action	<ul style="list-style-type: none"> • Indian central bank banning banks ability to service bitcoin companies • China clamping down on exchanges and mining activities • U.S. Congress representatives calling for bans or restrictions • Bitcoin addresses being put on OFAC list 	<ul style="list-style-type: none"> • Network continues to function uninterrupted • Network adapts and immunizes threat • Bitcoin wins, strengthens
Competing protocols	<ul style="list-style-type: none"> • Bitcoin hard forks and copies • World Computer • Utility Tokens • Stablecoins • Facebook's Libra 	<ul style="list-style-type: none"> • Competing currencies fail • Bitcoin remains dominant <ul style="list-style-type: none"> • Market tests provide information • Bitcoin wins, strengthens
Company or service provider error	<ul style="list-style-type: none"> • Mt. Gox hack - stolen bitcoin • Bitfinex hack - stolen bitcoin • Binance hack - stolen bitcoin • BlockFi hack - stolen personal information • Hardware wallet vulnerabilities 	<ul style="list-style-type: none"> • Errors owned by responsible parties <ul style="list-style-type: none"> • No bailouts • Accountability eliminates moral hazard <ul style="list-style-type: none"> • Companies adapt or fail • Bitcoin wins, strengthens
Individual user error	<ul style="list-style-type: none"> • Individual exchange accounts getting hacked • Accounts being frozen or terminated • SIM Swaps • Bitcoin wallets being lost or stolen • Forgetting passphrases to private keys • Malicious browser extensions or malware 	<ul style="list-style-type: none"> • Errors owned by responsible parties • No bailouts - Accountability eliminates moral hazard <ul style="list-style-type: none"> • Individuals adapt or lose money • Bitcoin wins, strengthens

Each form of stress hardens the bitcoin network and often for different reasons. Whenever governments take action in an attempt to ban bitcoin or otherwise restrict its use, the network continues to function

unperturbed. China and India, countries with a combined population of 2.7 billion people, have both taken material actions to curb the spread of bitcoin. Despite this, the network as a whole continues to function without flaw, and bitcoin continues to be used in both countries. After the RBI (Central Bank of India) restricted the ability for banks to service bitcoin or cryptocurrency-related companies, the Supreme Court in India ultimately overturned the ban as unconstitutional. It sets precedent in more ways than one. First, that the central bank was overruled; second, that the ban was ultimately unsuccessful as people continued to find ways to access bitcoin; and third, that despite these actions, the network was unphased. Separately, China has taken measures to restrict the ability of exchanges to facilitate bitcoin trading and has expressed an interest in eliminating bitcoin mining. Similar to India, people continue to use bitcoin in China and the bitcoin network has been undeterred. Naturally, as government regulation in China has become more restrictive, miners have begun to look to more stable jurisdictions. Bitcoin mining in the United States (among other regions) continues to grow, and Peter Thiel recently backed a startup that is building out mining operations in West Texas. Regardless of the threat, bitcoin exists beyond countries (and governments). The network adapts to jurisdictional risks and continues to function without interruption. As network participants observe the failed attempts to inhibit bitcoin's growth and witness how it adapts, bitcoin does not merely remain static; it actually becomes more resilient through this process by routing around and immunizing each passing threat.

Cryptocurrencies

Cryptocurrency Virtually Outlawed in India as Top Court Backs Ban

By Upmanyu Trivedi and Rahul Satija

July 3, 2018, 4:10 AM CDT Updated on July 3, 2018, 5:55 AM CDT

Technology

Cryptocurrency Bourses Win India Case Against Central Bank Curbs

By Upmanyu Trivedi

March 3, 2020, 11:27 PM CST Updated on March 4, 2020, 1:41 AM CST

- RBI had barred banking services from using digital currencies
- Supreme court ruling on Wednesday struck down the RBI's curbs

CRYPTOCURRENCY

China says it wants to eliminate bitcoin mining

PUBLISHED TUE, APR 9 2019 5:38 AM EDT

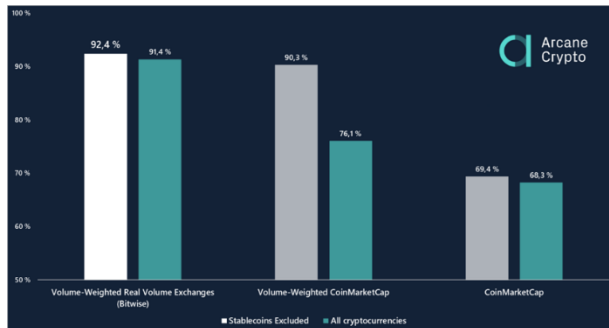
THE LEDGER • BITCOIN MINING

Texas Bitcoin Mining Startup Gets \$50 Million From Peter Thiel to Steal China's Crypto Crown

By JEFF JOHN ROBERTS
October 15, 2019 7:52 AM CDT

An entirely different type of stress comes in the form of competing cryptocurrencies. Since bitcoin was launched in 2009, there have been no fewer than a thousand competing digital currencies. While often (but not always) espousing different purposes and “use cases,” in each instance, every single one has in reality been competing with bitcoin as money. In many cases, the creators do in fact call out perceived flaws in bitcoin and how a particular competing protocol intends to improve on its “limitations”. Despite thousands of competitors, bitcoin accounts for ~70% of all cryptocurrencies in terms of market value, and when adjusted for liquidity, the estimate is closer to ~90%. Whereas one currency accounts for 70% to 90% of value depending on the metric, thousands of competing cryptocurrencies account for 10% to 30%. That is the market distinguishing between bitcoin and the field. Competition is inherently good for bitcoin. Not only does each attempt to create a better bitcoin fail, the repeated failures actually inform market participants that there is something which distinguishes bitcoin from the rest of the field. Even if the what or why is not immediately self-evident, the market provides useful information. Bitcoin does not just withstand the competition; it beats the competition. While bitcoin cannot be copied, that fact is more easily learned through market functions and market tests than any amount of reason and logic. Through

the failed experiences of competing currencies, bitcoin accumulates more human capital, and the network grows as a direct result. If bitcoin were never tested or challenged, it would not have the opportunity to benefit from stress. That it is constantly challenged and stressed through competition creates a more resilient network and a larger holder base.



Insight News

Bitcoin's reported market dominance is approaching 70%, but in reality it is above 90%

An analysis by Arcane Research shows how the real market dominance of bitcoin is way higher than what is traditionally reported.

While stress exposed to the network from external threats creates positive externalities, bitcoin also benefits from more regular and consistent stressors from within the network, typically arising in the form of malicious attacks or unintentional error. Attacks aimed at participants within the network, whether companies or individuals, occur practically at a constant clip. Each participant is maximally and independently responsible for the security of their bitcoin holdings, whether choosing to trust a third-party or whether taking on that responsibility directly. Many of the largest exchanges in the world have been hacked as have many individuals within the network. For those that have not, the threat always exists. As participants are compromised, hacked or otherwise have access to bitcoin restricted, it does not impact the functioning of the network, but like all stressors, the attack vectors directly cause the network to adapt and become stronger.



With numerous critical exchange failures, market participants increasingly shift to taking on the responsibility of holding their own bitcoin, independent from third-party service providers. The same is true in response to individual accounts at exchanges getting hacked. Not dissimilarly, as threats are identified for those that secure their own bitcoin, more secure wallets are developed and users opt toward more secure ways to safely secure their bitcoin by reducing or eliminating single points of failure. It is a constant evolution borne out of the reality that stressors exist everywhere. The network is not exposed to any critical failures because the entire network iterates through trial and error around the clock, with free competition and endless market opportunity incentivizing innovation. And, with each failure, everyone is on their own and personally accountable. The incentive structure dictates that everyone constantly seeks out better ways of securing bitcoin. Through this process of stress, the network very naturally and organically strengthens.

Bitcoin Benefits from Volatility

Similar to the benefit provided by consistent stressors, volatility tangibly builds the immunity of the system. While it is often lamented as a critical flaw, volatility is really a feature and not a bug. Volatility is price discovery and in bitcoin, it is unceasing and uninterrupted. There are no Fed market operations to rescue investors, nor are there circuit breakers. Everyone is individually responsible for managing volatility and if caught offside, no one is there to offer bailouts. Because there are no bailouts, moral hazard is eliminated network-wide. Bitcoin may be volatile, but in a world without bailouts, the market function of price discovery is far more true because it cannot be directly manipulated by external forces. It is akin to a child touching a hot stove; that mistake will likely not be made more than once, and it is through experience that market participants quickly learn how unforgiving the volatility can be. And, should the lesson not be learned, the individual is sacrificed for the benefit of the whole. There is no “too big to fail” in bitcoin. Ultimately, price communicates information and all market participants observe the market forces independently, each adapting or individually paying the price.



But information is not just communicated through price volatility. Volatility is also how bitcoin gets distributed and how the network becomes further decentralized. Every time a bitcoin is sold, someone else is buying. Consistently over time, the ownership of the network becomes more decentralized, and this occurs most acutely in bouts of volatility. In very tangible ways, the volatility strengthens bitcoin by decentralizing it and reinforcing that while tulips may die, bitcoin never does. As the network becomes more decentralized, it similarly becomes more censorship resistant and each individual within the network holds a smaller and smaller share of the currency (on average) resulting in a dynamic in which, over time, price is less exposed to the preferences of a few large holders. It is not to say that there do not remain large holders that can singularly influence price and volatility, but as a directional trend, the impact of any individual on price diminishes over time and often directly through the distributive function of volatility itself.

And when network participants, individually and as a whole, observe that bitcoin survives, even after extreme downside volatility, that mere fact strengthens confidence in the network. At some price, individuals were willing to step in and catch the falling knife. Through these episodes, bitcoin accumulates more human capital. The weak hands are shaken out and the strongest hands always survive (often in the form of new holders), causing the network to become more resilient and not merely remaining static or simply absorbing the disruption. Bitcoin actually feeds on the chaos. In the end, near-term volatility directly contributes to long-term stability. By maintaining a fixed supply with highly variable present

demand, the market performs price discovery 24 hours a day, 7 days a week. It is the intermittent stress that trains and hardens all individual owners and which prevents the network from being exposed to systemic risk. All while the opposite is true of fiat currencies. Central banks manage currencies to maintain short-term stability but ultimately, by suppressing volatility, imbalances accumulate below the surface leading to fragility and greater systemic shocks in the long-term, as has been witnessed with increasing regularity over the last two decades. The contrast between the two competing systems could not be more extreme and it is volatility in bitcoin that communicates information with the least distortion, and without which long-term stability would not be possible.

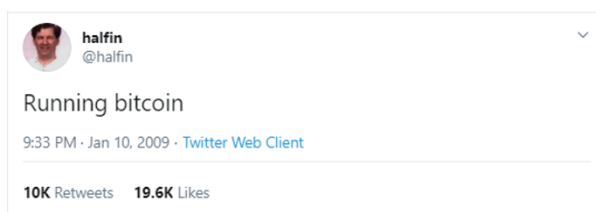
“Complex systems that have artificially suppressed volatility tend to become extremely fragile, while at the same time exhibiting no visible risks [...] Such environments eventually experience massive blowups, catching everyone off-guard and undoing years of stability.”

“Variation is information. When there is no variation, there is no information [...] there is no freedom without noise—and no stability without volatility.” – Taleb & Blythe, Foreign Affairs, May/June 2011 Issue

Bitcoin Benefits from Randomness

“Many of the greatest things man has achieved are the result not of consciously directed thought, and still less the product of a deliberately coordinated effort of many individuals, but of a process in which the individual plays a part which he can never fully understand. They are greater than any individual precisely because they result from the combination of knowledge more extensive than a single mind can master.” – Hayek, The Counter-Revolution of Science

Lastly, randomness. While most people recognize that there is intelligent design in bitcoin’s foundation, what is often missed is the randomness through which it evolved and that what it became (money) was largely a function of that randomness. Lightning was caught in a bottle; it was a result of thousands of people making thousands of independent decisions very early on. But the process also continues to this day. From cryptographers and developers contributing time and energy, to companies and investors building infrastructure, and to users just wanting to find a better way to store value. If the reset button was hit going all the way back to 2008 when the bitcoin white paper was released, and the same initial code was released, placing the same people in the same rooms, bitcoin would very likely not be what it is today. It may be “better” or “worse,” but ultimately it was and continues to be a product of randomness. It is not the product of consciously directed thought, and it expands beyond the resources of individual minds because of that fact. For those that perceive flaws in bitcoin and have (or had) ideas of how to make a better bitcoin, the intelligence of bitcoin’s design is often observed and acknowledged. Design can be copied and individual features can be changed out, but randomness cannot be replicated.



One week after bitcoin was launched, Hal Finney famously tweeted to the world that he was “running bitcoin.” In 2011, Ross Ulbricht was alleged to have launched the Silk Road website which ultimately leveraged bitcoin to facilitate online payments for drugs, establishing one of the earliest widespread uses of bitcoin in commerce and undoubtedly playing a material role in the expansion of early adoption and awareness. In 2014, Mt. Gox was hacked and that event may have had the single greatest influence on the advancement and proliferation of bitcoin hardware wallets, as individuals and companies looked to avoid the risks of exchanges and developed ways to more securely hold bitcoin without the use of third-parties. In 2017, after a bitcoin service provider drew the ire of Nicolas Dorier, he set out to build a product that would obsolete that provider and service, spawning one of the most exciting open source projects within bitcoin, BTC Pay Server. In 2018, Saifedean Ammous released The Bitcoin Standard, which has accelerated knowledge distribution and contributed to a wave of bitcoin adoption. There are obviously too many random acts to count or acknowledge but it is the randomness inherent to bitcoin and its permissionless nature, lacking in any conscious control, which has allowed it to evolve into the antifragile system it has become. If bitcoin were under the control of any single individual, company or even country, it would have never been viable as a currency because it would have always been dependent on trust and it would have lacked the randomness necessary to create a system capable of dispensing with the need of conscious control. Randomness is irreplicable and the foundation of bitcoin was built on it.

Bitcoin is Antifragile

In aggregate, as a currency and economic system, bitcoin benefits from disorder. It is the constant exposure to stressors, volatility and randomness which causes bitcoin to evolve, adapt and ultimately to become stronger in near-uniform fashion and in a way that would not be possible in the absence of disorder. Bitcoin may still be young, but it is not temporary. It was released into the wild, and what has spawned is a system that cannot be controlled or shut down. It's both everywhere and nowhere, all at the same time. It is like an elusive ghost. Its decentralized and permissionless state eliminates single points of failure and drives innovation, ultimately ensuring both its survival and a constant strengthening of its immune system as a function of time, trial and error. Bitcoin is beyond resilient. The resilient resists shocks and stays the same; bitcoin gets better. While it is easy to fall into a trap, believing bitcoin to be untested, unproven and not permanent, it is precisely the opposite. Bitcoin has been constantly tested for going on 12 years, each time proving to be up to the challenge and emerging from each test in a stronger state. At the end of the day, bitcoin is more permanent than it is risky because of antifragility. As a currency system, it manages to extend the utilization of resources beyond the control of deliberately coordinated effort, entirely dispensing with the need of conscious control all together. Bitcoin is the antifragile competitor to the inherently fragile legacy monetary system. On the one hand, a legacy system crippled by moral hazard, dependent on trust and centralized control. One that accumulates imbalance and fragility when exposed to stress and disorder, principally as a function of trillions in bailouts with each passing shock, which only further weakens its immune system. That compared to bitcoin which is a system devoid of moral hazard and which operates flawlessly on a decentralized basis, without trust and without bailouts. It eliminates imbalance and sources of fragility as a constant process, further strengthening the currency system as a whole and as a function of time. What doesn't kill the legacy monetary system only makes it weaker. What doesn't kill bitcoin only makes it stronger.

“Antifragility is beyond resilience or robustness. The resilient resists shocks and stays the same; the antifragile gets better.” – Nassim Taleb, Antifragile

“But those who clamor for “conscious direction”—and who cannot believe that anything which has evolved without design (and even without our understanding it) should solve problems which we should not be able to solve consciously—should remember this: The problem is precisely how to extend the span of our utilization of resources beyond the span of the control of any one mind; and therefore, how to dispense with the need of conscious control, and how to provide inducements which will make the individuals do the desirable things without anyone having to tell them what to do.” – Hayek, The Use of Knowledge in Society.

Views presented are expressly my own and not those of Unchained Capital or my colleagues. Thanks to Will Cole and Phil Geiger for reviewing and for providing valuable feedback.

Bitcoin Needs You As Much as You Need Bitcoin

By Sylvain Saurel on In Bitcoin We Trust

Posted June 13, 2020

This interdependence is essential.

A unique invention in the history of mankind, Bitcoin was offered by Satoshi Nakamoto to all the inhabitants of the Earth. With this incredible gesture, Satoshi Nakamoto sent the signal that Bitcoin would be the people's money.

Bitcoin belongs to all its users. It has no leader who can make arbitrary decisions about its future.

By doing so, Satoshi Nakamoto decided to put the fate of Bitcoin in the hands of its users. **Bitcoin would become what its users would make of it.** To say the least, users seized the unique opportunity offered by Satoshi Nakamoto.

Since its official launch in early 2009, Bitcoin has become stronger and stronger block by block. You don't need to take my word for granted, just take a look at all the key Bitcoin metrics by yourself.

In this, Bitcoin is true to one of its mottos: "Vires in Numeris".

Vires in Numeris: Bitcoin Is Stronger Than Ever

Don't trust, Verify.

medium.com



Without any support from governments or private investment banks, Bitcoin has managed to reach a market capitalization of over \$170 billion.

Better yet, Bitcoin has no dedicated marketing team. Bitcoin is totally different from all the other cryptocurrencies that launch themselves claiming to dethrone the Bitcoin King. **Bitcoin is clearly the king of the industry**, and will undoubtedly remain so in the future.

Bitcoin needs its users to grow

Instead of marketers, Bitcoin has loyal users who can be compared to missionaries. You have recognized here that I am talking about Bitcoiners.

These Bitcoiners contribute to the improvement and democratization of Bitcoin. Some will participate in the development of Bitcoin. Others will develop services around Bitcoin that will improve its use for thousands of users.

Others will promote its democratization by helping as many people as possible to understand **what Bitcoin really represents**.

By writing articles on a daily basis so that more and more people have the chance to discover Bitcoin, I place myself in the latter category.

However, all Bitcoin users have an important role to play.

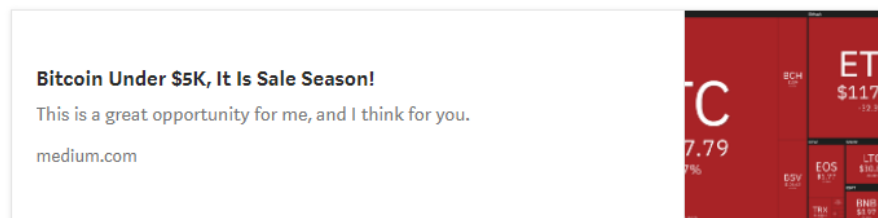
Bitcoin needs its users to live, but also to help new people understand that Bitcoin is an essential weapon to build a better future, especially in terms of money.

The missionaries who participate daily in the democratization of Bitcoin are worth a thousand times more than all the marketing teams on Earth. Indeed, people who act out of conviction rather than mere financial interest are much more patient and resilient.

Nothing can take away a Bitcoiner its confidence in the Bitcoin revolution.

Bitcoin will always be protected by so-called HODLERS of last resort.

I am one of them, and I contributed with others to the strong rebound of Bitcoin during its Black Thursday in March 2020. When its price hit a low of \$3,800, we took advantage of this unique opportunity to accumulate even more Bitcoins.



The monetary and financial system needs you more than you need it

If you have read so far, you will tell me that the fact that Bitcoin needs you is nothing revolutionary compared to the current monetary and financial system.

The current monetary and financial system needs the people. Without you, your government would not be able to borrow hundreds of billions of dollars year-round. If you weren't aware of this, I'm going to tell you a hard truth:

The monetary and financial system needs every citizen to pay their taxes in order to pay back all the money that is printed or borrowed.

If citizens stopped paying their taxes today while taking their money out of the banks, the system would simply implode. So the fiat system needs you to exist.

The comparison between Bitcoin and the fiat system ends there.

If the fiat system needs you, you don't actually need fiat system. It hardly does anything for you. The people have no voice in the current system. You still doubt that? Did the Fed consult the people before arbitrarily deciding to print \$3 trillion in the last three months.

The answer is no.

The Fed is led by a minority of people who are not representative of the people and who make arbitrary decisions with very serious consequences. The consequences of decisions made by the Fed impact a majority of citizens negatively.

The rich people see their wealth increase, while the poor people who need help the most are put in even greater difficulty by this great monetary inflation.

The relationship between you and the fiat system only goes one way.

The fiat system is not a democracy at all. You may have the impression that it is, since you vote to elect your president if you are lucky enough to live in a democratic country. However, do not be fooled.

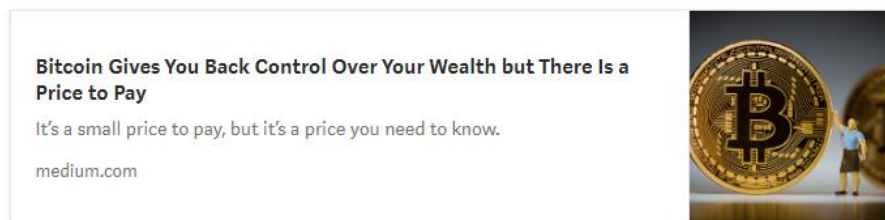
When it comes to the economy, every successive government makes the same bad decisions.

Whether the leaders are on one political side or another, they will always make the people pay for the mistakes of a monetary and financial system that is completely broken.

Bitcoin gives back to its users what they give it

Bitcoin needs its users to continue building its revolution to establish a fairer world for the future. But Bitcoin users need Bitcoin to guard against the current monetary and financial system that does not take them into account.

Bitcoin gives power to its users.

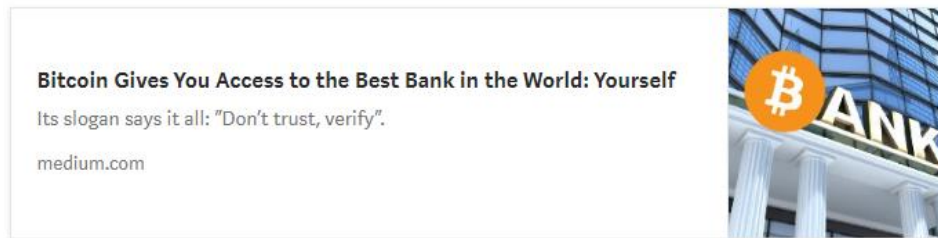


By choosing Bitcoin, you are voting against the current system. You are protesting peacefully. Your voice is taken into account, and you can really make a difference in the future of Bitcoin.

In return for your support of its revolution, Bitcoin allows you to protect what you own from the great monetary inflation. **Bitcoin is proving to be the best store of value, with qualities that are objectively superior to gold.**

One of the big advantages of Bitcoin is that it helps financial inclusion for millions of people around the world.

With a smartphone and an Internet connection, you have access to the best bank in the world thanks to Bitcoin: yourself.



Bitcoin plays a key role in protecting human rights.

Few realize this in Western countries. Those who take the trouble to look at emerging countries understand that Bitcoin is already a plan A for millions of people.

Look at Venezuela, Argentina, Iran, Lebanon, Lebanon, Zimbabwe and Afghanistan. In these countries where citizens are experiencing hyperinflation, Bitcoin is used more than anywhere else in the world.

For the citizens of these countries, Bitcoin is the only weapon to fight against the bad decisions of totally corrupt leaders.

The situation is not as dramatic in the United States, Canada, or Europe at the moment, but we can no longer swear by anything in the world in which we live today.

Who would have thought 6 months ago that a pandemic that had not been seen in decades would hit the world, and that central banks would print \$10,000 billion in 3 months?

No one, of course.

From now on, nothing seems impossible anymore. We live in an uncertain world. As an individual, you will sooner or later find yourself trying to hold on to a minimum of guarantees for your future.

That's where Bitcoin comes in as an extraordinary hedge against uncertainty.

With Bitcoin, you can have guarantees. There will never be more than 21 million BTC in circulation. By buying 1 BTC in 2020, **you have the guarantee that your BTC will still represent 1 BTC out of 21 million in 100 years.**

This historically unprecedented scarcity for a human invention is an integral part of Bitcoin's monetary policy. The automatic and predictable side of this monetary policy is there to protect you. No matter what happens, inflation in the number of new Bitcoins produced each day will halve for every 210,000 blocks mined.

Bitcoin highlights the virtues of quantitative hardening.

Bitcoin Highlights the Virtues of Quantitative Hardening

Bitcoin Quantitative Hardening is to be contrasted with the Quantitative Easing led by the Fed.

medium.com



Bitcoin needs you as much as you need Bitcoin

The more time passes, the more the Bitcoins that are already in circulation will increase in value. **By becoming a Bitcoin HODLER, you not only support Bitcoin by making it even scarcer, but you also protect your future.**

Bitcoin is magical in the sense that it is worth protecting your individual interests while also protecting the interests of the many.

By helping Bitcoin continue to grow stronger, you will enable millions of people around the world to benefit from Bitcoin as well.

The people who support Bitcoin whatever it takes have already understood this interdependent relationship with Bitcoin.

Bitcoin needs you, but you need Bitcoin for your future as well. By supporting Bitcoin, you are working to build a better future for you and the others. This is also one of the reasons why Bitcoiners are often compared to missionaries.

I hope that you will realize this interdependence, and that Bitcoin will change your life just as it has changed mine.

Why Bitcoin is a silent protest against corrupt governments everywhere.

By **Tatiana Koffman**

Posted June 13, 2020

America is undergoing a historic transition. The #BlackLivesMatter movement has prompted protests in 145+ cities around the world. Young and old of all races, genders and nationalities have hit the streets over the last two weeks to raise their voices together against injustice, police brutality and systemic discrimination.

As peaceful protests deteriorated into riots, it became clear that people were not just upset about racism, they were fed up with the abuse of authority that has pervaded modern society. Mandatory lockdowns, lack of adequate or accessible healthcare, a financial system that has shelled out billions of dollars in commercial bailouts, the growing wealth divide — all of these recently prevalent issues were just the tip of the iceberg.



One anti-authoritarian community stood up in solidarity and tweeted: “Bitcoin is a peaceful protest.”

For the newbs: Bitcoin is a non-sovereign, hard cap supply, global, immutable, decentralized and completely digital store of value, held by many as an insurance policy against the irresponsibility of central banks globally. (Credit to Tavis Kling for this concise definition).

Since the creation of Bitcoin 11 years ago, a growing number of people have been choosing to opt-out of the traditional financial system — the central source of power for our governments. They are turning to a new monetary system: one that is not controlled by any single authority, but is rather decentralized and run by a network of computers. As a child born in the Soviet Union, having witnessed the fall of a government, hyperinflation and a run on the banks, all before the age of ten, Bitcoin also piqued my interest.

Bitcoin was born as a movement by the people for the people. And so, I wanted to give the community supporting this movement an opportunity to be heard — sourcing the key ideas in this article through Twitter.

Bitcoin is a protest against corruption.

Naval Ravikant, founder of AngelList once tweeted: “Bitcoin is a tool for freeing humanity from oligarchs and tyrants, dressed up as a get-rich-quick scheme.”

With this perspective in mind, it’s no surprise that Bitcoin has a much higher rate of adoption in countries that have a history of government oppression – Germany, China, Venezuela – and a lower rate of adoption in the U.S. Americans are much more likely to have faith in their U.S. Dollar than a new cryptocurrency.

One story was shared with me anonymously by a Ukrainian software engineer – let’s call him Greg. In 2014, what began as a peaceful protest in Ukraine quickly grew into a civil war, riddling the country with violence and unrest. As expected, due to political instability, the local currency was devalued by 70%. Greg lost his job and was looking for a way to escape the rebellion.

“There was nothing left for me there, I was surrounded by death and destruction. I started plotting an escape.”

Airports and roads were guarded by soldiers to prevent people from fleeing – temporary visits to family, however, were permitted by car. It was well known that many of the officials charged with guarding the borders were corrupt and would confiscate money and valuables at checkpoints. And so Greg, having kept most of his savings in USD, decided to trade it all for Bitcoin. He memorized the 12 words from his seed phrase like “his life depended on it” and ran, with nothing but a small backpack on his person, managing to escape with all of his wealth intact.

[For anyone new to Bitcoin, you can access a Bitcoin wallet from anywhere on the internet as long as you know your seed phrase.]

There are countless stories like Greg’s. Tales of people fleeing persecution in Eastern Europe, South America and Africa, using Bitcoin as a means to carry value with them. For many, Bitcoin is what saved their wealth and, by extension, their life.

Skeptics often use the argument that Bitcoin “isn’t backed by anything.” But this is an inherently privileged North American view. Bitcoin is backed by a demand for financial freedom, for an asset outside the control of governments, and one that cannot be confiscated easily.

America is not immune to a financial revolution.

America is unique in that it has not experienced a major economic upheaval besides the Great Depression and the last financial crisis in 2008, creating a trust in the system. But America’s fiat currency is only about 50 years old, since Nixon abolished the gold standard in 1971, a relatively unproven experiment. Fiat has already failed in other nation states like Venezuela and Zimbabwe.

Bitcoin was born out of protest against the financial system in 2008. Against monetary stimulus in particular. The very first block of Bitcoin famously gives a nod to this anti-authority sentiment by quoting a headline from the UK Times in the code:

“The Times 03/Jan/2009 Chancellor on brink of second bailout for banks.”

History has shown us that a sudden influx of ‘new’ money without any corresponding economic growth leads to inflation: a rise in prices coupled with a fall in the purchasing power of that currency. This is considered a hidden taxation on citizens — prices rise, but wages stay the same.

There is a prevailing sentiment that the elite who control the government, the financial system and the private banks and corporations, engage in the printing of funds in an effort to prop up the inefficient and inherently corrupt business practices of corporate America — all at the expense of ordinary citizens.

Bitcoin is a currency that is, by design, completely independent of any government and its established financial system. Bitcoin strips governments of their power to create more money. It has a hard cap supply of 21 million units, giving it a built in anti-inflationary mechanism and protecting Bitcoin holders from the risks of monetary policies implemented by central banks.

A global world wants a global currency.

Charles de Gaulle, one of France’s former Presidents, addressed the nation in 1965, saying:

“We consider it necessary that international trade be established as it was the case before the great tragedies of the world, on an indisputable monetary base and one that does not bear the mark of any particular country.”

Not too long ago, the vast majority of global trade was tied to gold. Gold has no ideology and has maintained a stable value relative to goods and services for thousands of years.

As the world became more interconnected, governments chose to create their own currencies in order to establish relative power against other nation states in trade negotiations. Today, this is quickly becoming an outdated concept. We are part of a global empire, with a growing disregard for the nationalistic opinions and borders of individual states. It is led by a multi-ethnic elite, held together by a common cosmopolitan culture. Most importantly, the majority of this new generation do not accept the U.S. as its leader or the Dollar as its currency.

Experts have long foreseen the emergence of another revolutionary financial system.

Nobel-prize winning economist Friedrich Hayek was quoted in 1984:

“I don’t believe we shall ever have a good money again before we take the thing out of the hands of government, that is, we can’t take it violently out of the hands of government: all we can do is, by some sly roundabout way, introduce something that they can’t stop.”

Meanwhile, economist Milton Friedman was quoted in an interview in 1999, saying:

“I think that the Internet is going to be one of the major forces for reducing the role of government. The one thing that’s missing, but that will soon be developed, is a reliable e-cash — a method whereby on the Internet you can transfer funds from A to B without A knowing B or B knowing A.”

All of these predictions came true with the creation of Bitcoin.

Bitcoin allows for separation of money and state.

What is the role of government? It is there to enforce a social contract we all inherently enter into just by being born and raised under its jurisdiction. It is there to create order, and to provide basic services such as roads, schools and hospitals. If the government were a corporation we paid to provide these services, there would be no reason for them to also have control over our bank account.

Many argue that money should not be politicized. The wealth you work so hard to create should be intact regardless of the decisions of your government — whether it is to start a war, issue a bailout or make a bad trade agreement. Money backed only by the authority of governments jeopardizes its value. In fact, the entire thesis behind the traditional investment industry is to prevent the erosion of value through inflation.

Bitcoin creates accountability. A money supply tied to Bitcoin would inherently show a transparent account of which funds went to war and police, versus education, healthcare and other necessities for the ordinary citizen.

And so, Bitcoin allows us the opportunity to opt-out of the current system — all without lifting a weapon or raising our voice. A silent, but effective protest.

Think of it like playing monopoly with your friends. Once you realize that the bank is corrupt, all the players could simply agree to create a new form of money. There is no need to burn houses or hotels. We can continue to play the game and remove the power of money from the greedy banker — and thus, we take away the most authoritative weapon they have.

Tweetstorm: Bitcoin Marketing

By **Dan Held**

Posted June 16, 2020

1/ Bitcoin has a decentralized marketing team, which is composed of all Bitcoiners. We are part of a grand A/B testing experiment where we iterate with messaging and propagate different ways to explain Bitcoin to the masses, to teach them how to use Bitcoin, buy Bitcoin.

2/ My personal brand is my iteration on that experiment which I'll cover tomorrow in another thread. Bitcoin comes across as goofy, technical, and boring

3/ I felt that it was important we show Bitcoin as a blend between sci-fi and revolution. A combination of Inception, Blade Runner, and Mr. Robot mixed with educational content. But before we get there tomorrow, a little more on marketing 🖱️

4/ Why does marketing matter? Every product, service, protocol, government, religion, etc. requires its "solution" to be found by its target customer segments.

5/ Bitcoin solves wealth preservation and censorship. Religion solves death, and life operating structure. Apple solves easy to use computers. States solve security. Following me?

6/ Bitcoin needs all of us. If no one ever spoke or promoted it, then none of us would be here. And it's critical that we tap into that mainstream sector through these channels that they frequent.

7/ "We hodler revolutionaries have to care about the direction we move the world; it is our job to trumpet the tool of freedom Bitcoin is to everyone, everywhere, everywhen" @Breedlove22

8/ Marketing is about conveying your solution to the target customer at the right time with the right messaging to convince them to become a customer.

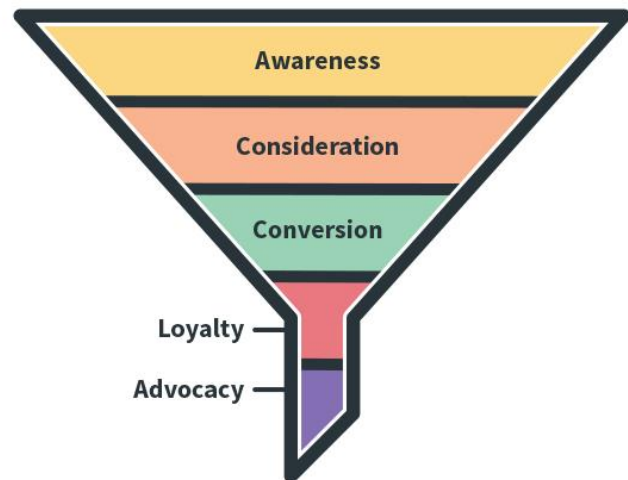


9/ From a clinical perspective, humans take marketing inputs (text, image, video), parse, and then respond via outputs (buying/not buying, subscribing, sharing the content, etc). If you're not marketing something well, then you're simply not providing the right marketing string

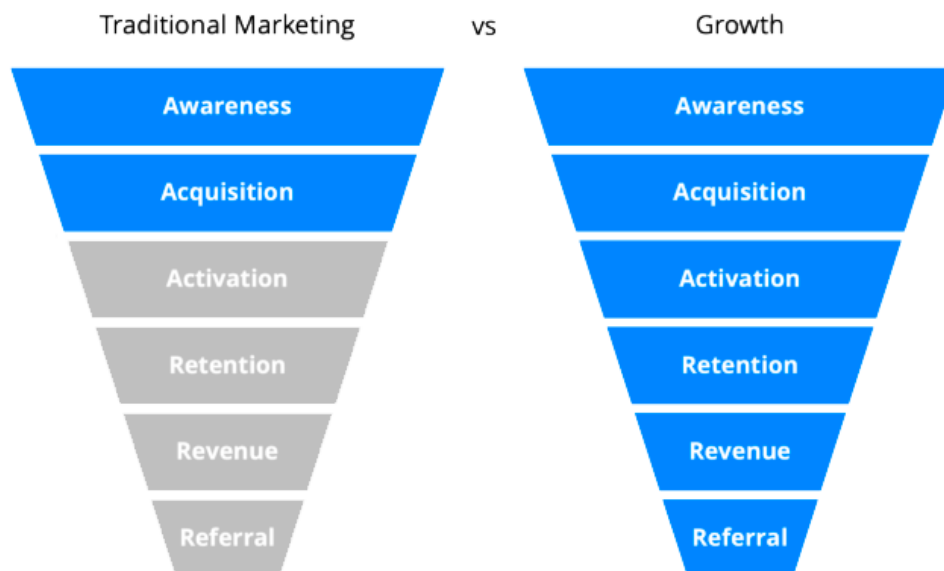
10/ Ok now that we know some of the basics around how messaging changes behavior, let's dive into the concept called "marketing funnel."

11/ A funnel describes the customer journey, for Bitcoin that is:

- Awareness: I've heard about Bitcoin
- Consideration: I think Bitcoin might solve a problem for me
- Conversion: I'm going to buy Bitcoin
- Loyalty: HODL
- Advocacy: Telling friends about Bitcoin



12/ Note there are many marketing funnel designs/definitions, but generally they all convey the same journey. And in tech it is popular to have a growth team which uses a "Growth funnel" to map out that journey, demonstrating a tighter fit between product and marketing.



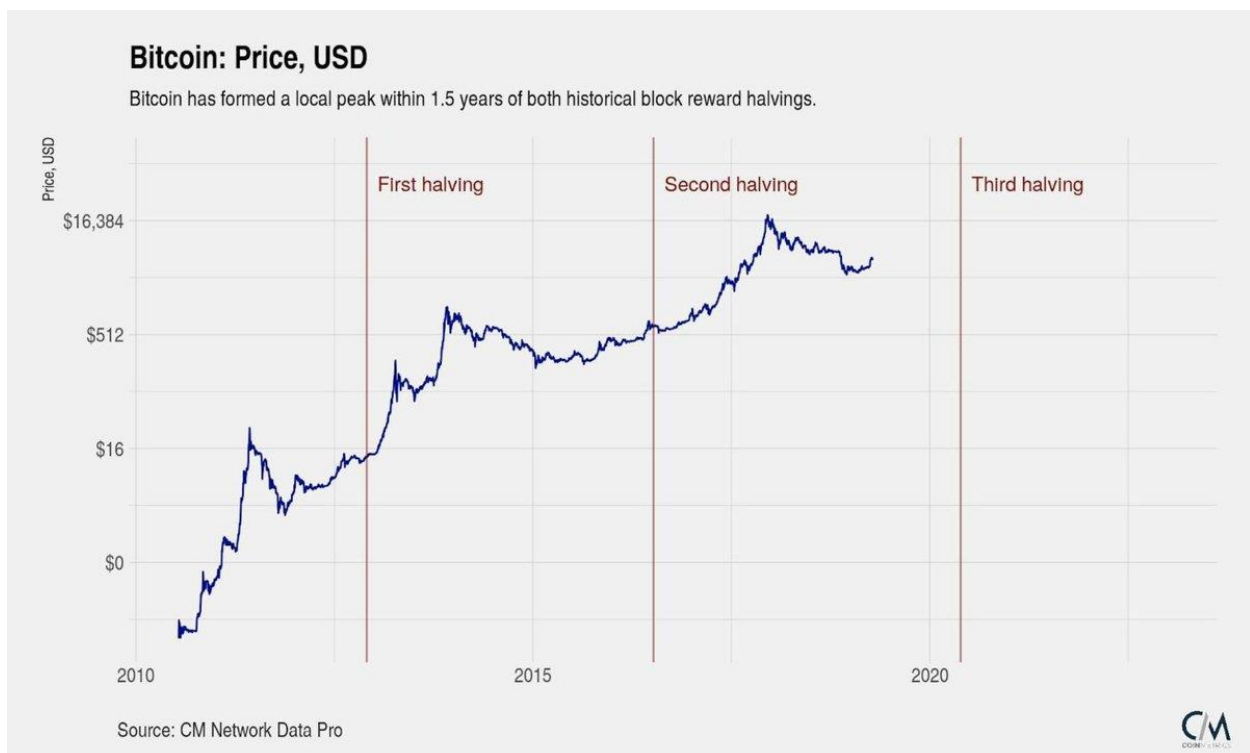
13/ Awareness and consideration: When people become aware of Bitcoin and start to consider it as a new money competitive with their local fiat, it requires a complete restructuring of their trust models.

14/ "You need the simplest version of the idea to grow naturally in the subjects mind...you have to start with the absolute basic" We can't start with Bitcoin, we have to start with people's relationship with their government/money.



Inception - We Need A Forger Eames (Tom Hardy) (3/5) (HD)
 Visit: <http://www.quizandquestions.com> For A Movie Quiz
 Inception Movie Quiz: ...
[youtube.com](https://www.youtube.com)

15/ New user adoption in Bitcoin has been driven by speculation, which Satoshi hypothesized: "As the number of users grows, the value per coin increases. It has the potential for a positive feedback loop; as users increase, the value goes up, which could attract more users"



16/ Some Bitcoiners argue that "Bitcoin will dominate because it is the hardest money ever known. It forces people to understand it better and educate themselves." Bullshit. Most came in for speculation, and the ones who stayed saw/hear CONTENT. You don't automatically "get it"

17/ While we could say that Bitcoin will win solely based on its value props, but people naturally understand a new concept more easily when it's explained simply.

18/ Which also explains why we saw such a rise in objectively poor, but easily explained ideas in 2014-2018 (x/y/z coin is "cheap", ETH is the new App Store, etc)

19/ Price ceilings are set by speculators, and floors by HODLers. If none of the speculators became convicted in Bitcoin, then the price would go to \$0. Our efforts then should be spent on converting a speculator into a believer/HODLer.

20/ Right now people think of Bitcoin as this enormously complex idea. John Oliver adeptly describes it as everything we don't understand about money + everything we don't understand about computers. We must compress the narrative into more digestible content payloads.

21/ Finally, we need to propagate the narrative where normies hang out: Instagram, FB, LinkedIn, YouTube, etc. Most people aren't on Twitter We give ourselves a self congratulatory pat on the back for a good tweet. But dare we wade into the quagmire of other altcoin channels?

22/ What does good marketing look like? Many Bitcoiners feel that good marketers are sleazy salesmen types, especially when they do a "hack" to get engagement. However, they're simply capturing attention, which is increasingly harder to get.

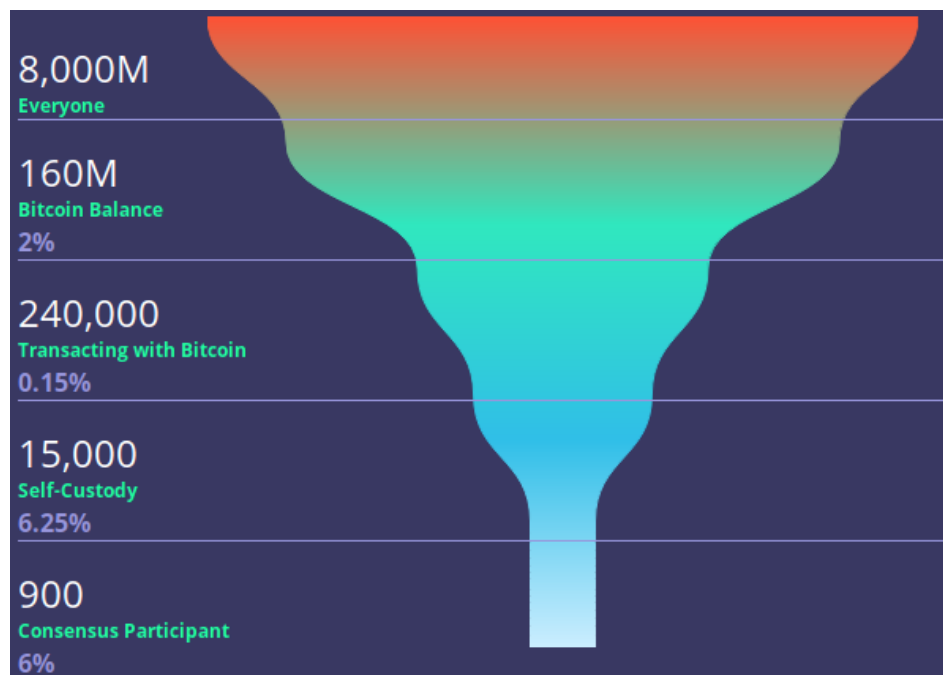
23/ If a certain type of marketing leads to new users (acquisition) that stick around (retention) then it's *inherently* good quality.


24/ These influencers (usually) are trying their best to incept Bitcoin into the mainstream. They won't be able to do that talking about obscure Bitcoin nuance like UTXOs. And the mainstream channels they go on (CNBC/Bloomberg) will only invite them back if engagement is high.

25/ Normies (typically) don't start out on a technical article about Bitcoin's security model.

26/ You can think of [@APompliano](#)/[@PeterMcCormack](#) as top of the funnel.

Whereas [@lopp](#), [@bitmexresearch](#), [@matt_odell](#) are at the bottom. Prospective Bitcoiners will engage with lighter but easier to understand content at the top then eventually travel down the proverbial rabbit hole



27/ Note: chart was not made by me - I'm not necessarily saying the funnel stages are what I would label
Continuing on 

28/ "To think one person or podcast/whatever needs to be called out for marketing themselves or an idea is silly at best." - [@RTHowell](#)

29/ To create great content, [@PeterMcCormack](#) doesn't have to agree 100% with every Bitcoiner: he doesn't have to eat steak everyday, he doesn't need to share the same perspective on intense science/medial conversations, etc. He making Bitcoin appeal to a larger audience.

30/ Peter has a podcast w/ great engagement, that's why he's compensated \$66k/mo. Welcome to capitalism. You might think that he doesn't provide "value" but the market has decided the value of his services. This is in the same vein as: "PoW is wasteful bc I don't like BTC"

31/ Bad marketing can hurt Bitcoin. The "p2p cash" narrative led to a civil war, billions of misallocated capital, hundreds of dead companies (with disenfranchised employees/builders) and created conflicting/damaging expectation that eroded Bitcoin's growth trajectory.

The End Of Gold

By Sven Schnieders

Posted June 17, 2020

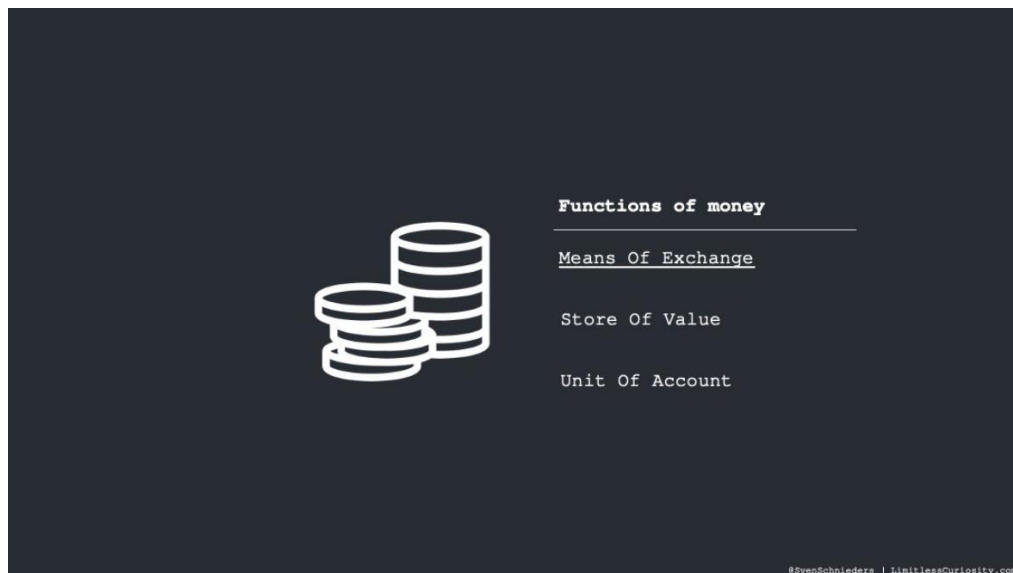
The reason why Bitcoin is much better money



This Essay is based on the talk I gave at the last ValueOfBitcoin conference. It includes a lot of ideas that I have previously outlined in my essays Mass Adoption of Bitcoin's Values and Stop Calling For A Free Market In Money. The argumentation is built from the ground up, which means we will start with the function and properties of money.

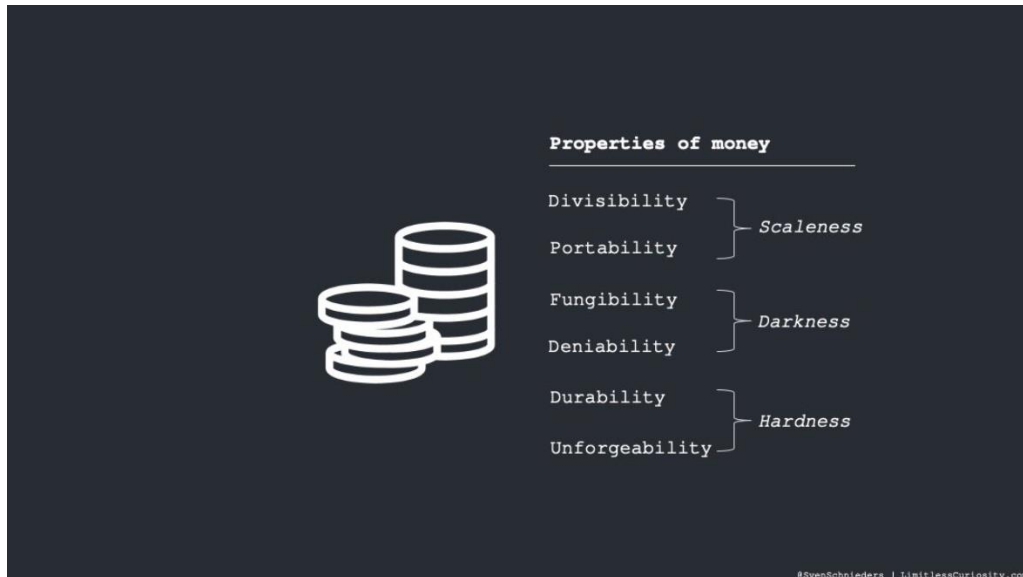
Also, we will only compare Bitcoin and Gold in their function as money. There are many good reasons to invest in gold—and other assets such as real estate—but as I will show, believing it is superior money should not be one of those reasons. Therefore, this essay is not an attack on gold as an investment but only an attack on gold as money.

The Functions of Money



The primary function of money is means of exchange. The other two functions—store of value and unit of account—are sub-functions and can be derived from the means of exchange function. They are only important insofar as they help the means of exchange function. Store of value, for example, is important if you want to exchange your money at a later point in time. It should be obvious then that many things are a great store of value but bad money—e.g., real estate and art. The point of this essay is to show that gold belongs in the same category.

The Properties of Money



These three categories—Scaleness, Darkness, and Hardness—were put forward by Giacomo Zucco, but similar frameworks have been suggested by others and are almost universally accepted. Scaleness expresses the desire for something easily portable across time and space, while it can also be used in small and large quantities. Darkness captures the need for financial privacy. And Hardness refers to the difficulty of creating more supply, which also includes counterfeiting. For a deeper dive into the origins of money and the need for these properties, I recommend reading Nick Szabo’s essay Shelling out, and Giacomo’s series Discovering Bitcoin. We will discuss each of these properties in detail later, but let us first take a brief look at the history of gold.

A Brief History Of Gold

Before the gold standard, people paid with gold and silver coins. Silver was needed for smaller payments because a gold coin is worth too much and not very divisible. This system of physical coins still had two major shortcomings. First, there is no unit of account. Expensive things were priced in gold and cheap things in silver. This is made worse by the fact that the exchange rate—how many grams of silver are needed to buy one gram of gold—fluctuates. The second shortcoming is that settling large transactions (e.g., between banks) is extremely costly and inefficient, which limits the size of the economy.

These two main problems, together with the technological advancement of telegraphs, brought about the change towards the usage of certificates, instead of physical metals. The certificates were backed with a certain amount of gold and could be redeemed immediately. This solved the divisibility problem of gold and made silver useless as money. Gold has a higher stock-to-flow ratio—the new amount of gold that is produced each year compared to existing stock—and is, therefore, better suited for being money (harder). We’ll come back to this aspect of hardness later, but for now, just note that most people prefer to store their wealth in something that inflates little over time.

Despite the advancements in trains and railroads, exchanging physical gold was still expensive. This meant that debt between banks was seldom settled in physical gold; and banks were tempted to issue more certificates than they had gold in their reserves. What followed was a consequence of this fatal flaw outlined beautifully by Saifedean Ammous in *The Bitcoin Standard*:

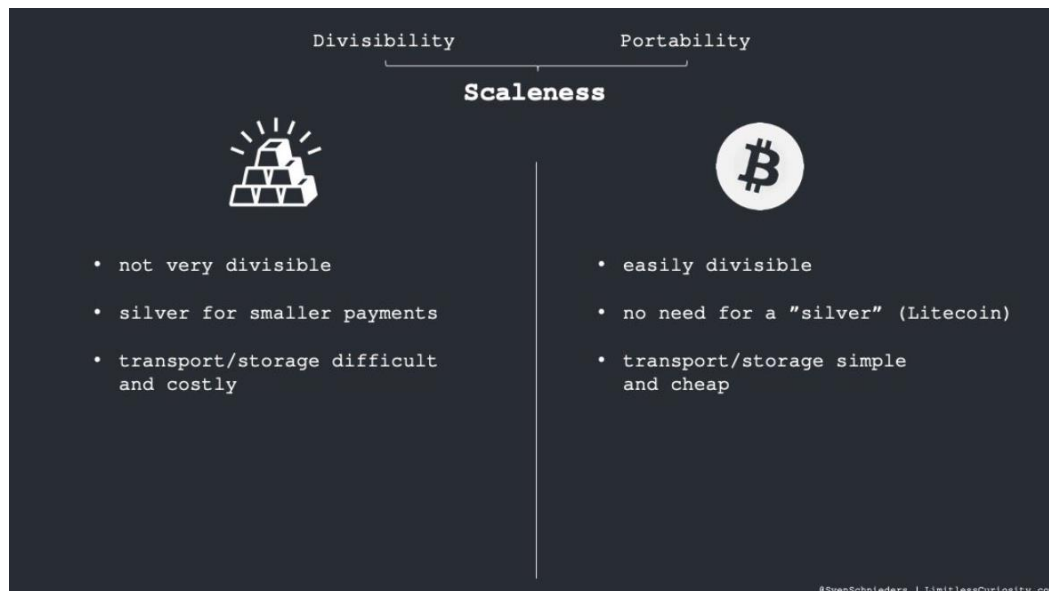


“The fatal flaw of the gold standard at the heart of these two problems was that settlement of physical gold is cumbersome, expensive, and insecure, which meant it had to rely on centralized physical gold reserves in a few locations—banks and central banks—leaving them vulnerable to being taken over by governments.”

This is exactly how the gold standard ended. Governments took control of most of the supply by controlling just a few locations because they needed more money. Then they also outlawed private gold ownership. Since it is difficult to hide large sums of gold and most of the supply was already in the hands of government, no black market developed. This is how the gold standard ended and today’s fiat system began.

Now let’s take a look at the different properties of Gold and Bitcoin and how such an outcome could be prevented in the future.

Scaleness: Divisibility and Portability



As we have already discussed, gold is not very divisible, which is why silver was used for small payments. Portability across time and space—storage and transport—are also very difficult and costly. This fact

makes gold susceptible to centralization because storing large sums of gold, without a third party, is close to impossible in practice.

Bitcoin, on the other hand, is extremely easy to divide (in theory, it is infinitely divisible). It is also simple and cheap to transport and store. Here, the cost of a Bitcoin payment should not be compared to sending money over PayPal, but to a final irreversible settlement like transferring physical gold. This is the only sense in which Bitcoin payments should be considered cheap. Always remember:

Bitcoin doesn't compete with PayPal, but with central banks.

The storage problem is solved by the digital nature of Bitcoin, which allows you to store as much Bitcoin as you want on a short key that you can remember.

Darkness: Fungibility and Deniability



Fungibility refers to the property that all units of our money should be the same as all the other units. This is one of gold's best properties. You can smelt in any gold bar or gold coin and make it look like any other. It is, however, difficult in practice and not possible for an individual because an expensive melting pot is needed (third party).

If you transact gold locally—peer-to-peer—there is no transaction history, and it is possible to deny your connection to any “illegal” business. However, for global or large transactions, this gets very difficult. Nor is it possible to deny the ownership of large sums of gold. You either have to store these large sums by yourself, which is difficult and noticeable, or you have to store your gold in a bank, which means that at least the bank knows how much you own.

Fungibility, and more generally privacy is probably Bitcoin's biggest problem. Since there is a full transaction history—called Blockchain—no Bitcoin is like any other coin. Many people are working on solutions in this space (CoinJoin, PayJoin, Bisq, etc.), and I am confident that we will triumph over ChainAnalysis and KYC. In fact, the solutions available today, if used correctly, are sufficient to acquire

Bitcoin anonymously and break any links. Since storing large sums of Bitcoin is simple, denying that you own large sums is simple as well, provided you know how to use the available privacy tools.

Hardness: Durability and Unforgeability



Gold has great durability and also the highest stock-to-flow ratio of anything on earth (until Bitcoin after the next halving). This is what people refer to when they talk about “sound” or “hard” money. It is an important property that the money supply cannot be inflated at will. It is costly to produce more gold and due to the long history of gold mining, the existing stock is large compared to the amount of new gold that can be mined in a year. This means that even if the demand for gold increases drastically, the supply does not change much. The inflation rate of gold is very low. This is the main property that made gold the best money available until Bitcoin was created.

The problem with gold is that it is relatively easy to counterfeit. People increase the supply by paying with fake gold. This is a big problem because verifying the authenticity of gold is difficult and costly. It also cannot be done by an individual alone because for a 100% verification, a melting pot and a lot of specialized knowledge is needed.

Now, there is a problem: you don’t want to get paid in gold certificates because you can’t be sure that they are fully backed by gold, and you don’t want to entrust your wealth to a third party, but if you are paid in real gold, you also need a third party to verify it for you (and most likely also to store it for you). Bitcoin solves this problem.

The durability of Bitcoin is great because it can be stored decentralized in many different locations. It will soon be the asset with the highest stock-to-flow ratio (the hardest asset) and after all 21 million coins have been mined, it will have a stock-to-flow ratio of infinity. In other words, Bitcoin is the first absolutely scarce good ever. More importantly, however, Bitcoin solves the verifiability problem by having a full transaction history. For a few hundred dollars, anyone can run their own full node and fully verify all Bitcoin they receive. This is the beauty of Bitcoin.

An interesting fact to note is that almost all technological developments favor the attacker over the defender. We have nuclear weapons but no defense because it is almost always easier to use a technology destructively than protectively. The same trend seems to be hurting gold. While fully verifying gold remains difficult, it is becoming easier and easier to manufacture counterfeit gold. This is why forgery scandals like [this one](#), are becoming increasingly common. Cryptography is a rare technology that favors the defender over the attacker by making verification cheap and counterfeiting extremely costly. This is the reason Bitcoin works.

Bitcoin Cannot Be Stopped

Since gold, as we have established, is difficult to store and verify for an individual, it gets naturally centralized in a few locations. These few locations can then be attacked by the state (or anyone else), and this is exactly how the gold standard ended. Due to gold's physical nature, the emergence of a black market is difficult, and the transfer of wealth (or the trade) across borders is almost impossible.

Bitcoin solves these problems. You can store as much Bitcoin as you want in your head by remembering your private key, and you can verify all Bitcoin you receive inexpensively by running a full node. These two key points help keep Bitcoin decentralized. This means that centralized points of attack for the state or anyone else are close to non-existent. Because of its digital nature, sending it across a border is easy, and the emergence of a black market (a parallel economy) is possible. Bitcoin was created to succeed in exactly the adversarial environment where gold has failed.

Gold needs a benevolent state and a huge infrastructure to succeed because you cannot verify and store it by yourself; Bitcoin does not need any of those things.

For these reasons, Bitcoin is the only technology that allows you to claim your monetary sovereignty and liberty—something gold will never be able to do.

The Bitcoin Journey

By Gigi

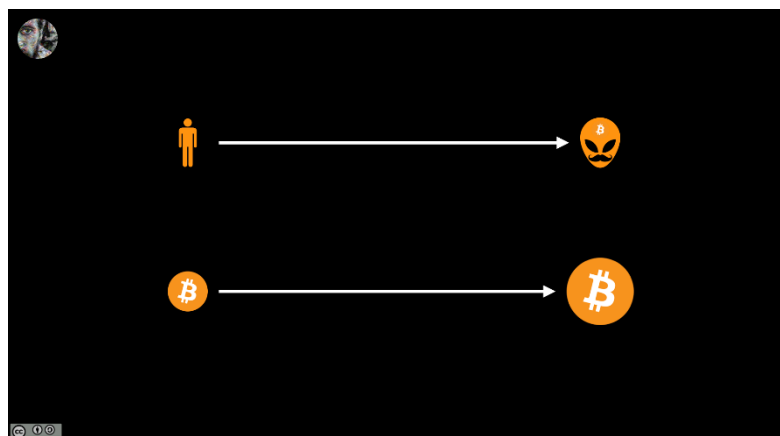
Posted June 15, 2020



A couple of weeks ago I had the immense pleasure of giving the opening talk at the *Value of Bitcoin* conference. I would like to revisit some ideas of this talk and maybe dig deeper into some parts. After all, my keynote *The Bitcoin Journey* was restrained by time: 21 minutes.

Again, I will look at the Bitcoin journey in two parts:





1. The journey of a bitcoiner
2. The journey of Bitcoin



Part 1: The Journey of a Bitcoiner

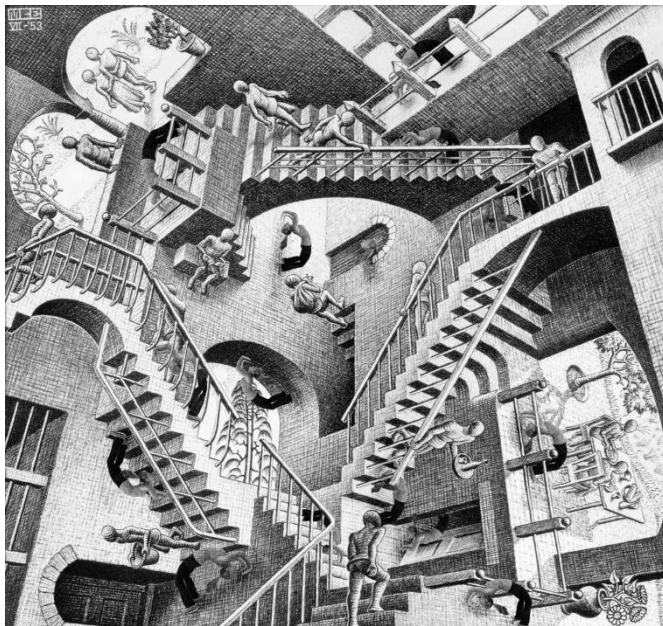
The natural reaction upon encountering Bitcoin for the first time is to dismiss it. Most people reject the idea that Magic Internet Money could work, or could be interesting, or could fix any woes that society might have. Outright dismissal was my first reaction as well: “Oh, this will never really work. It will get hacked one day and all your funny internet money will be gone.” Alas, at least I can find comfort in the fact that I’m not alone with my initial reaction. While some bitcoiners understood the gravity of the situation immediately, most of us mere mortals had to be confronted with Bitcoin multiple times before we took a closer look.

In short, the journey of a bitcoiner usually goes like this:

1. This will never work.
2. Why isn’t it dead yet?
3. Oh, this is interesting ...
4.  
5. 
6. 



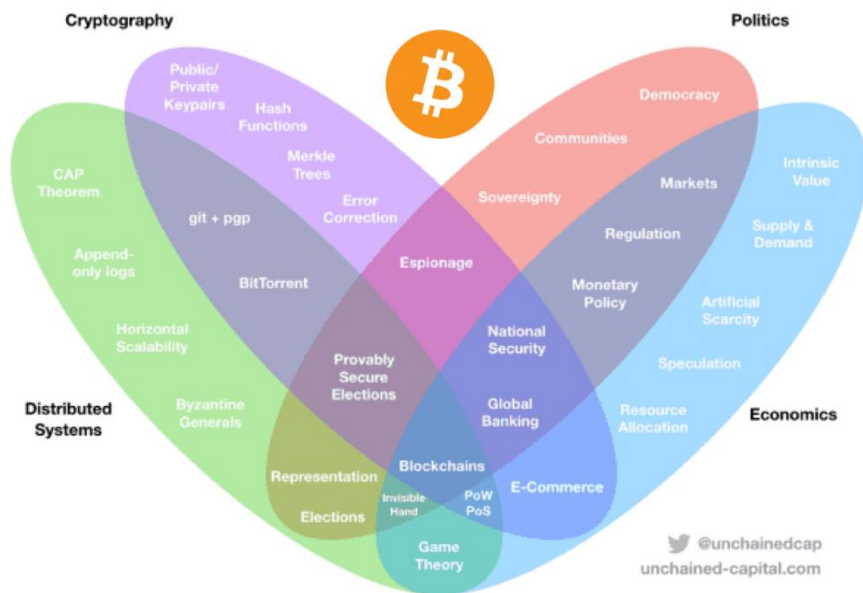
Falling down the Bitcoin rabbit hole can feel a little bit like being stuck in an M.C. Escher painting. Up is down, down is up, a lot of things don’t make sense at first, and the longer you look at it the more confusing it gets. However, there is some order to this chaos. It’s just not apparent at first.



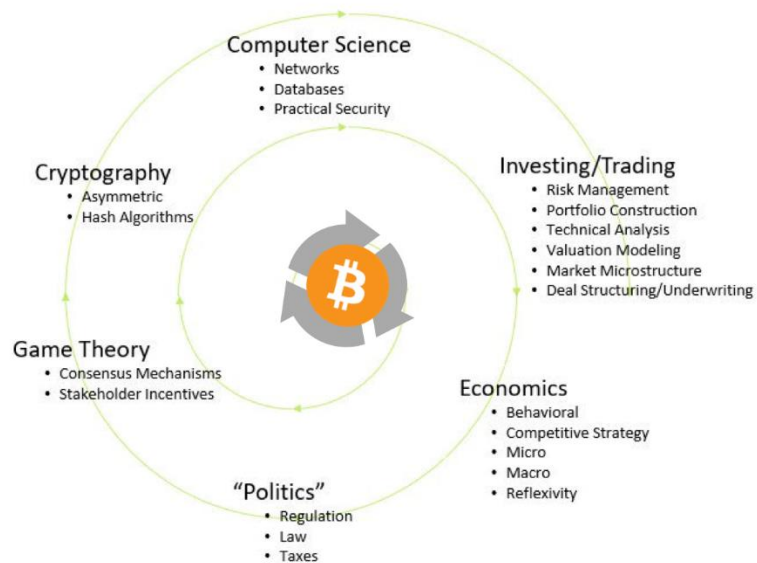
The reason for this initial confusion is, I believe, twofold. First, Bitcoin is extremely interdisciplinary. It spans a lot of topics, even if you just want to get a rudimentary understanding of it. You will probably have to learn some cryptography (at least what the difference between a public key and a private key is), some computer science (how does a decentralized network differ from other computer systems), some trading (where can I buy bitcoin and why does it have the price it currently has), and some game theory (who controls Bitcoin and why is it so hard to change or shut down) just to get started. Curiously, the deeper you dig, the more disciplines will pop up: macroeconomics, scalability, elliptic curve

cryptography, monetary policy, the history of money, the measure and study of scarcity, smart contracts, programming and scripting languages, incentive structures, laws, regulations, privacy, security, psychology, even biology. The list of topics is practically endless.

This idea is quite beautifully illustrated by what I would call The Bitcoin Flower ([Unchained Capital](#), 2017) and The Bitcoin Learning Spiral ([Block Tower](#), Ari Paul, 2018).



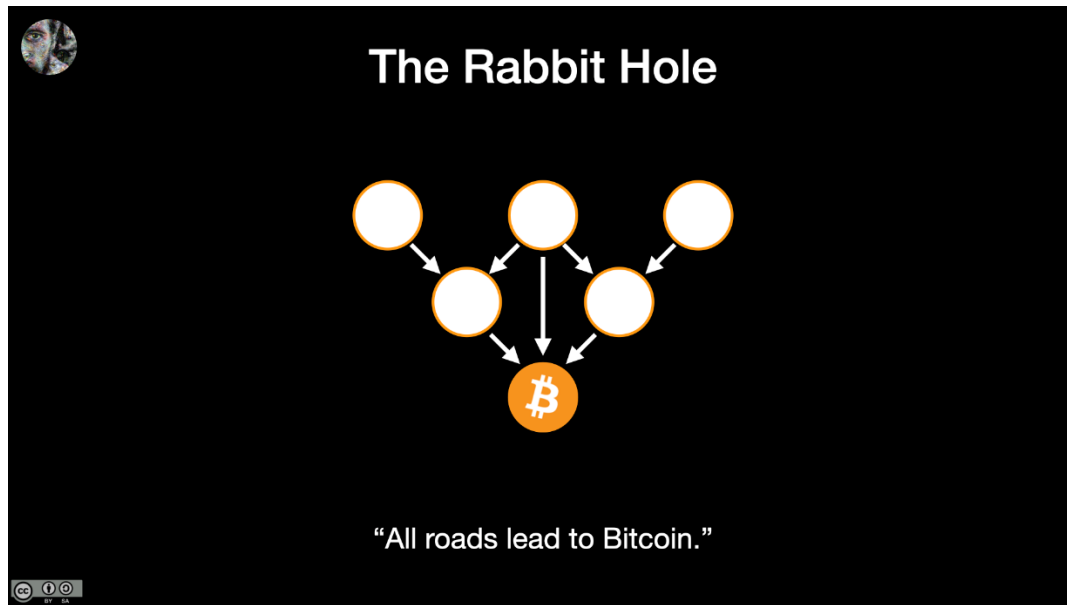
Source: [Unchained Capital](#) (2017)



Source: [BlockTower](#), Ari Paul (May 2018)

The downside of this multidisciplinary nature is that understanding Bitcoin doesn't come easy. The upside is that many roads might lead you to take a closer look at Bitcoin. In other words: many entries lead down this particular rabbit hole. Whether you have a background in computer science, finance, trading, cryptography, physics, economics, are a gold bug, a classical liberal, or have flirted with the idea of cryptoanarchy. All these backgrounds can give you a head-start.

What is interesting, though, is that so many people from so many different backgrounds arrive at the same conclusion: bitcoin is the money of the future. While the rabbit hole has many entries, in the end, all roads lead to Bitcoin.



Part 2: The Journey of Bitcoin

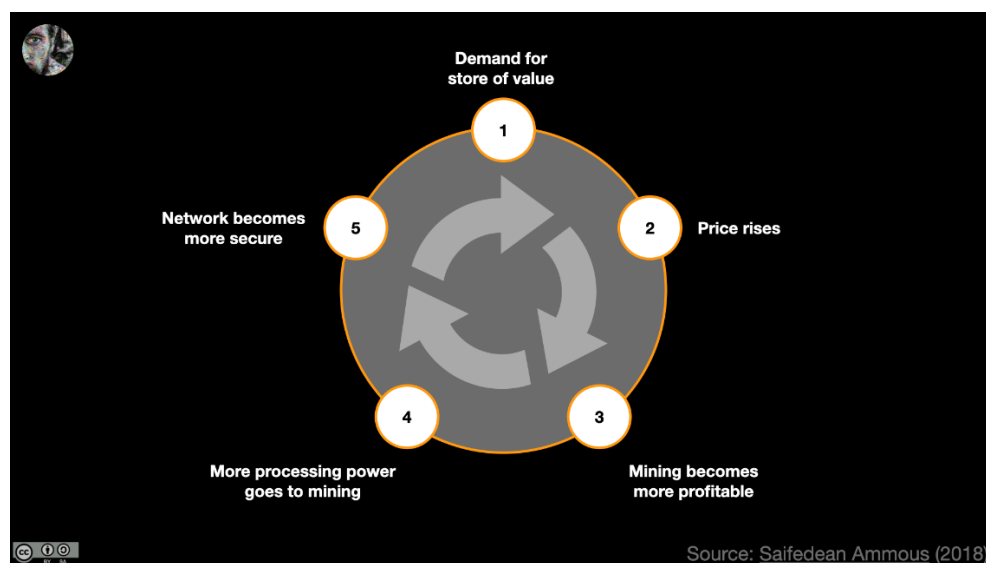
Bitcoin is a zero-to-one invention. Before Satoshi invented Bitcoin, real digital scarcity did not exist; the double-spending problem was unsolved. Today, we live in a world where Bitcoin exists. More importantly, we live in a world where bitcoin has value.

Thus, we can identify three stages:

- Stage 0: Bitcoin does not exist.
- Stage n: Bitcoin exists.
- Stage N: bitcoin has value.



Stage N is important because Bitcoin’s underlying NgU technology requires that bitcoin has some value. Once it acquires value – any value – Bitcoin’s eternal feedback loop kicks in.



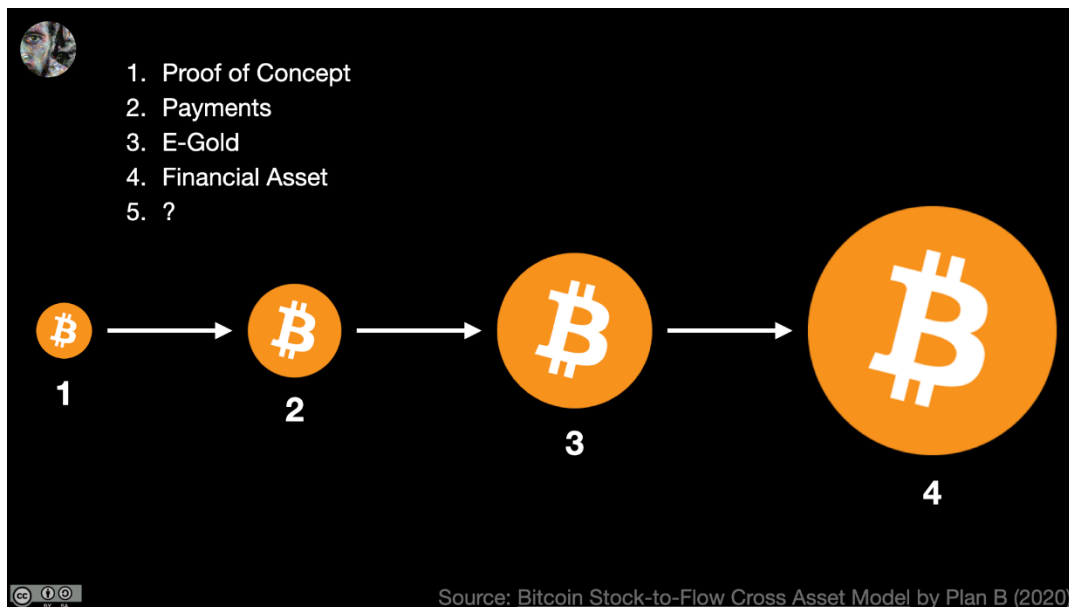
Satoshi alluded to this feedback loop in his writings.

“It might make sense just to get some in case it catches on. If enough people think the same way, that becomes a self fulfilling prophecy.” – Satoshi Nakamoto

Over the last couple of years all kinds of people – artists, researchers, quants, traders, commentators, in short: bitcoiners from all walks of life – noticed that Bitcoin seems to come in waves. In 2018, Hasu and Nic Carter published Visions of Bitcoin, describing the various competing narratives that were used to describe Bitcoin up to this point: e-cash proof of concept, censorship-resistant e-gold, cheap payments network, programmable shared database, anonymous darknet currency, reserve currency for crypto, and finally: an uncorrelated financial asset.

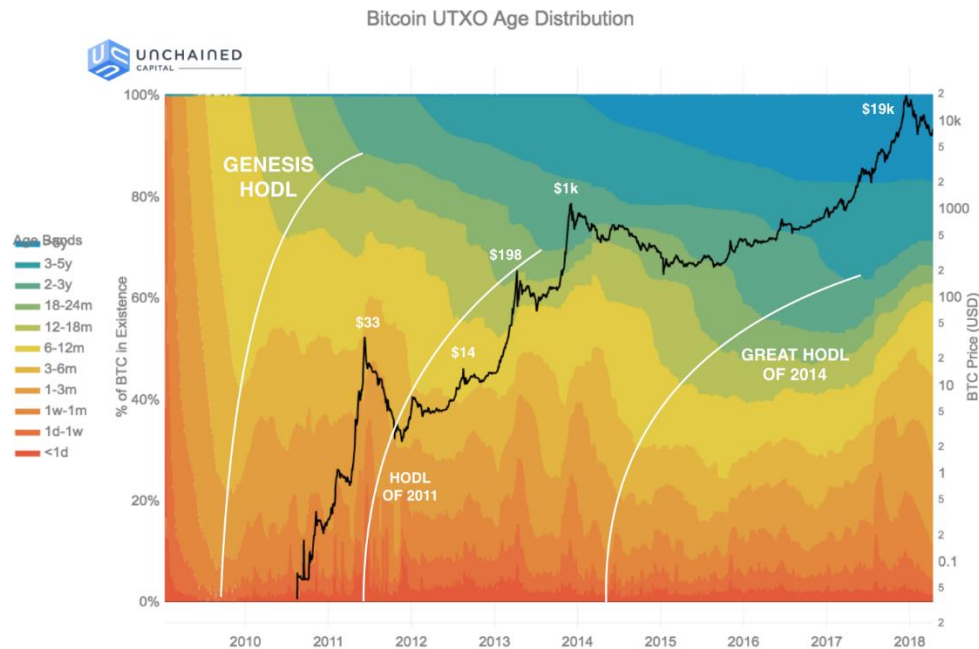
More recently, Plan B published his Stock-to-Flow Cross Asset Model (S2FX) which identifies distinct clusters by looking at the stock-to-flow and market value of bitcoin. He identified four distinct clusters:

1. Proof of Concept
2. Payments
3. E-Gold
4. Financial Asset



If the model holds, we are about to enter Phase 5. How Bitcoin will manifest in this phase will be known only in hindsight.

Another analysis regarding the wavy nature of Bitcoin was done by Unchained Capital, first published in 2018. Their HODL Waves beautifully show the age distribution of the Bitcoin UTXO set. In essence, we can see that a certain percentage of people choose to hold bitcoin for the long term, i.e. for several years. They identified various HODL waves just by looking at the UTXO age: the Genesis HODL, the HODL of 2011, and the HODL of 2014. By looking at the most recent data we can also identify a HODL of 2018.



Source: [HODL Waves](#) by Unchained Capital (2018)

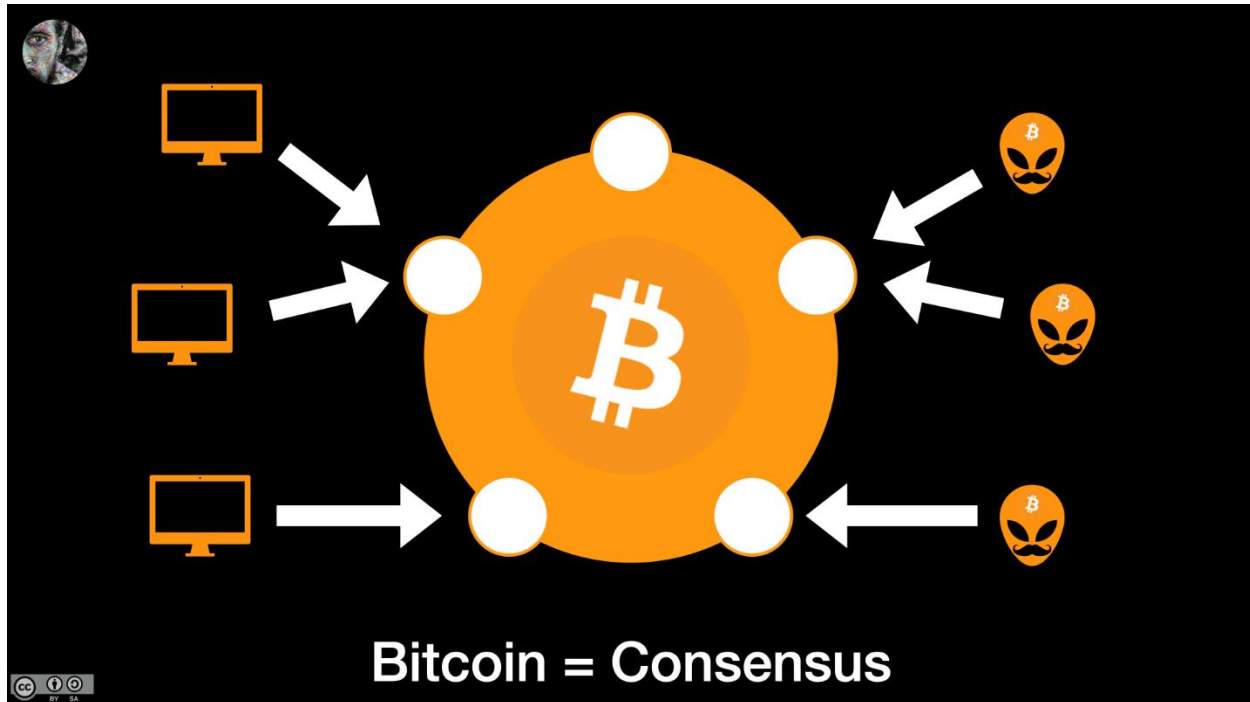
The most entertaining analysis is [this video](#) by Alex Millar, published in 2015. He is looking purely on price, showing how bitcoin tends to accrue value in a massive run-up, only to crash down hard a short time later. However, the price floor after the crash is usually way higher than the previous low, resulting in an upwards trend in the long run.

These various phases and waves show that Bitcoin has a cyclical nature. We already saw how demand, price, and security form an eternal feedback loop. However, many different aspects of Bitcoin are cyclical. Adoption, development, mining, difficulty adjustments, reward eras — all of them are cyclical. Granted, the halvings will stop in about 120 years, but the other cycles will most likely continue.

Part 3: Coming Full Circle

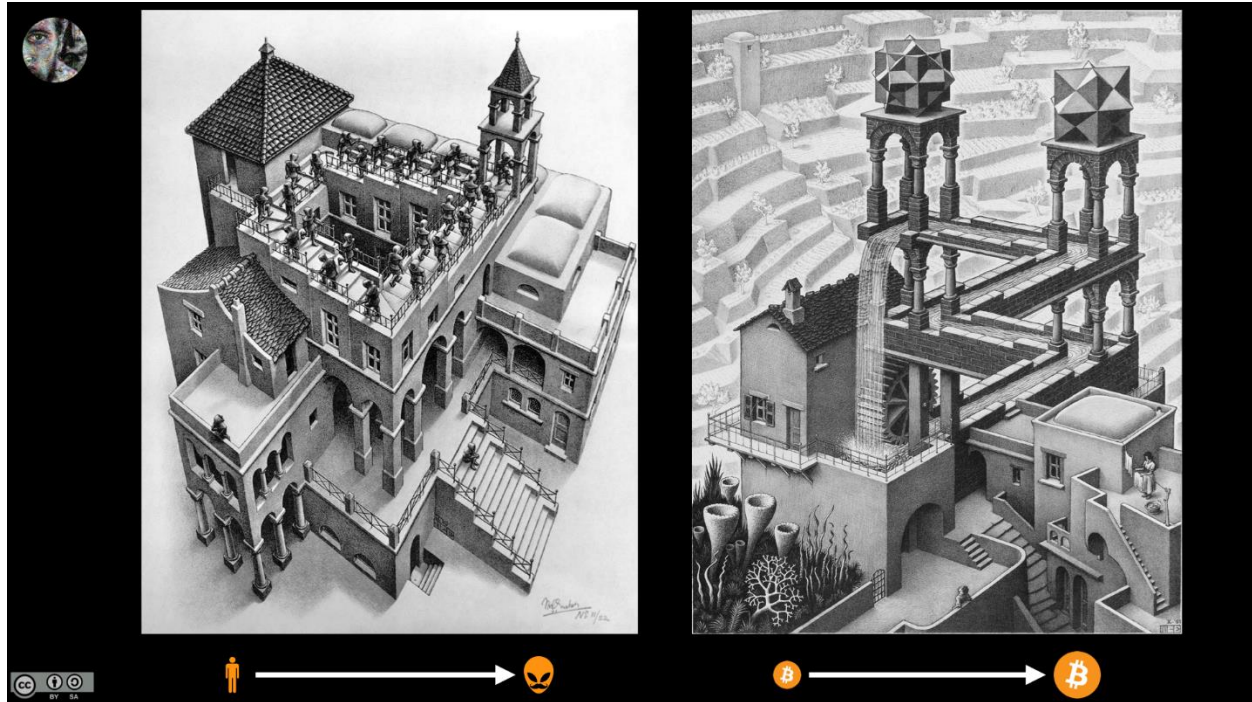
The essence of Bitcoin, the one thing that is truly unchanging, is the output of the system: the UTXO set. Nodes work together to constantly append it, verifying blocks and transactions, adding what is valid and discarding what is invalid. The chain tip is the shared understanding of all nodes: the version of the ledger which is most accurate and up-to-date.

Similarly, people are building a shared corpus of knowledge and mental models trying to figure out what Bitcoin is. Bitcoiners work together to constantly add to the knowledge, incorporating what is valid and meaningful, discarding what is invalid or doesn't make sense. Our shared understanding of Bitcoin can be seen as a Schelling Point: the conclusion that most people arrived at after intense study, often without indoctrination or communication with others.



A Bitcoin node doesn't trust what others are saying: it verifies all data as best as it can. Similarly, most bitcoiners don't trust what others are saying: they verify narratives and mental models as best as they can.

Just like Bitcoin is a game without an end, falling down the Bitcoin rabbit hole is a journey without an end. Bitcoin is an ever-changing, organic system. It will evolve, as will our individual and collective understanding of it. In other words: I believe that the reason why no-one has found the bottom of the rabbit hole yet is that there is no bottom. The rabbit hole is circular. In the coming years and decades, many people will try to fully understand what Bitcoin is and what it might become. But try as we might, I'm afraid a complete understanding will never be gained. We will all have to find our peace with this alien technology, or we are bound to walk in paradoxical circles around it in our quest to full comprehension.



In the end, if Bitcoin continues to be successful, it is bound to disappear. Just like the internet and electricity before it, it will move to the background, like running water in your home or the air you breathe. Everyone will take Bitcoin for granted. Consequently, bitcoiners will disappear. Just like today, you don't have to identify as an "internet person" anymore, in the future, you won't have to identify as a bitcoiner anymore. When this day comes, we will have entered the final stage.

Stage O: Bitcoin is Omnipresent.

Translations

- [German translation](#) by [Ge3onim0](#) & [Fab](#)

Further Resources

- [Recording of the talk](#) on YouTube
- [Slides](#) on SpeakerDeck
- [21 Lessons](#) aka my journey down the rabbit hole

Bitcoin's Town Square

By **Zane Pocock** on **Mempool Review**

Posted June 18, 2020

Why mempools are the network's most brutal information space

To the average Bitcoin participant, mempools are simply a list of pending transactions to check in on when they have a transaction to broadcast. But they are so much more.

Mempools are a bustling, brutal marketplace of pure data. They reflect all the knowledge of the pressures, needs, time preference and means of every single participant demanding transaction settlement on the Bitcoin network. And they distill all this knowledge into a real-time price signal anyone can interpret and interact with.

Mempools are the centerpiece of the entire Bitcoin economy. And they are totally underrated.

Note: mempools are tightly integrated with other components of the Bitcoin network, particularly mining and transaction verification, that are out of scope for this article to explore. We will uncover what we need to make everything clear, but this article is more focused on a mental model for understanding mempools than technical exactitude.

Thousands of Mempools

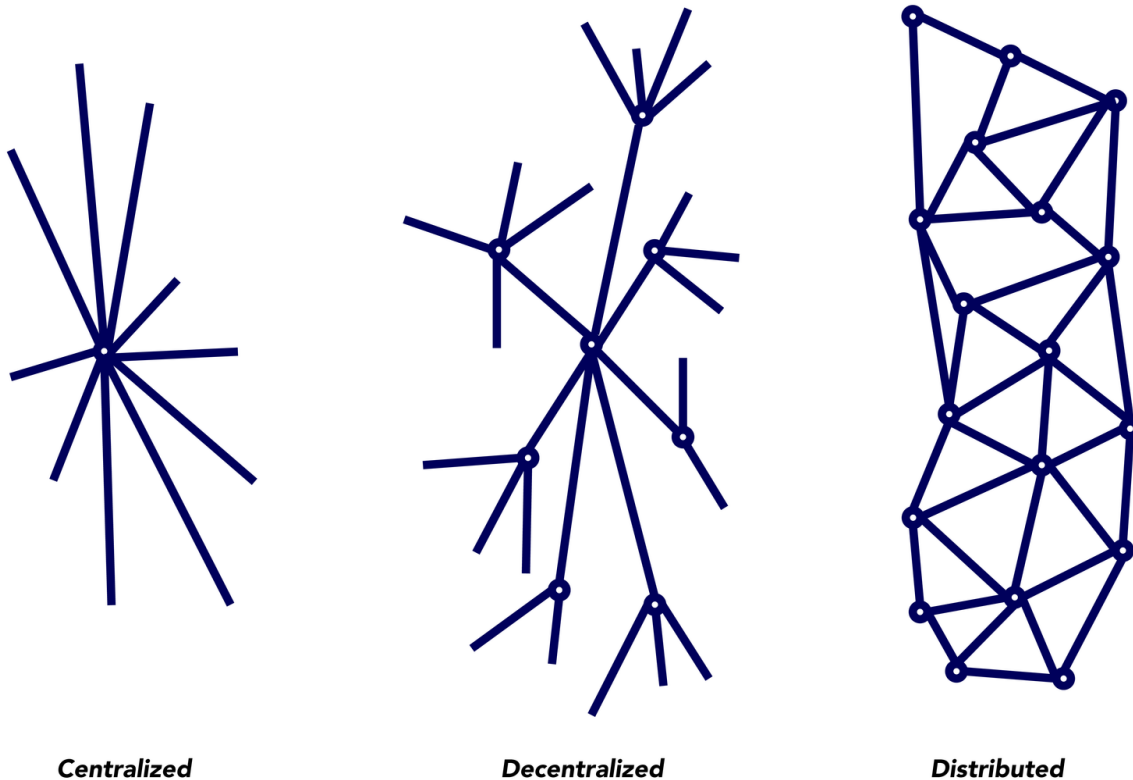
At its simplest abstraction, “the mempool”, short for Memory Pool, can be thought of as a database of pending Bitcoin transactions. These are transactions that have been broadcast by users but haven't yet been included in a block. Because they have not been mined into a block, such transactions are considered “unconfirmed”.

We refer to “the mempool” here in quotes because this term is a colloquialism that neglects the true nature of how the Bitcoin network functions, and it's worth correcting. While “the mempool” would imply that there is a single master list of unconfirmed transactions, there is no such certainty. Rather, every participant running a full node will have a slightly different version.



When we talk about “the mempool” we thus aren’t strictly talking about a ubiquitous information space. We’re talking hypothetically about all the transactions spread across all the mempools. Most mempools might have most of the transactions but the idea of “the mempool” is a shortcut that helps us make generalizations and perform economic calculations.

Why is this? The Bitcoin protocol functions such that each node represents an intersection on a distributed network, each with a unique set of connections to other nodes.



When a participant broadcasts a transaction to the network through a node (hopefully their own), that node will pass the transaction data on to the other nodes that it has direct connections with. These nodes will first verify that the transaction is legitimate, and if so, they will update their list of unconfirmed transactions to include it and pass the data on to the other nodes that they, in turn, are connected to. Those nodes will repeat the process until the percentage of nodes with a copy of this transaction approaches 100%. This is called a transaction relay.



So, what happens when those transactions are mined into a block? While humans think of miners as huge industrial enterprises hashing transaction data at great cost, nodes on the Bitcoin network simply interact with miners as they do with any other node. These nodes, which seen through a human lens happen to “mine”, keep their own version of the mempool from which they select transactions to include in a block when they successfully meet the current network criteria, roughly every ten minutes. Those blocks then

propagate back through the network in much the same way as transactions, with each node verifying that they meet certain criteria, updating their copy of the settlement ledger (“the blockchain”), and passing the message on to others. Each individual node first tries to validate these blocks with the transactions they already have in their mempool and request any missing transactions from peers, after which they flush these transactions from their mempool as they are no longer “unconfirmed”. For a high-level understanding of some more nuanced parts of this process, Marty Bent published a wonderful graphic explanation by Bitcoin Core contributor Amiti Uttarwar.

This is why it’s important to understand “the mempool” as a collection of independent mempools: it’s easy to accidentally equate the idea of a shared mempool with the certainty of the blockchain and its settlement assurances. While every participant eventually stores an identical record of final settlement (the blockchain), there is no such record of truth for those transactions awaiting settlement. For our purposes, understanding “the mempool” as a marketplace, this is important: calculations we might like to make will always be probabilistic.

While the Bitcoin network is best seen simply as a communication protocol dealing in scarce information space, mempools are a clearing house for the allocation of that information space. Users of the Bitcoin protocol can roughly keep track of their unconfirmed transactions through metrics gathered from their own mempool. If you have initiated your own transaction before, you might have noticed that wallets such as Electrum will tell you its “position in mempool” expressed as, say, “13 MB from tip.” As far as a miner is concerned, the two most important data points about a transaction is its size (in terms of data requirements, not value) and the feerate it’s willing to pay. If you imagine your mempool as a list of transactions ordered by the feerate each is paying, this is *very roughly* telling the participant that their transaction is estimated to be about 13 MB worth of >1 MB blocks away from being included because that is how high it is bidding, so say 11 blocks or 110 minutes assuming ten-minute block times (to more technically proficient readers, please bear with me here—I recognize this is quite a simplification).

Current Bitcoin Mempool

Where is my transaction in the mempool?

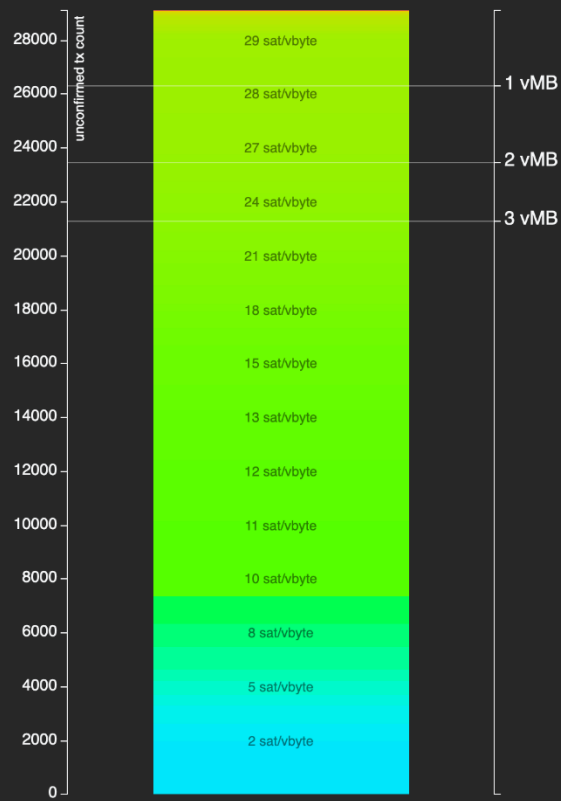
The chart shows a mempool snapshot from my node. The mempool contains unconfirmed transactions waiting to be included in a block. Each transaction pays a fee and has a size. Transactions paying a higher fee per size (feerate) are usually included earlier than low feerate transactions.

The stacked bars in the chart represent grouped and sorted transactions by their feerate. The bar height of each feerate group corresponds to the amount of transactions in that group. The highest feerate groups appear at the top of the chart descending to lower feerates. Each horizontal line shows one megabyte of transactions. The bars are colorcoded according to their feerate.

29095 unconfirmed Transactions (15.52 MB)

Enter or try a random transaction id to see where it is in the mempool:

4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc7



<https://mempool.observer/>

The Use of Knowledge in Bitcoin Society

Austrian economist F. A. Hayek would have loved mempools. In his 1945 essay *The Use of Knowledge in Society*, he illustrates the profound importance of price signals by making the case that every economic actor has some of the information all of the time, but all of the information none of the time. At its most simplified, his argument is a knock-out refutation of the idea of a planned economy: how could a central planning board possibly keep up with the dynamism of each individual component of the economy? Price signals and their fluctuations are immensely powerful as they tend towards carrying all of this information, despite no single individual needing to know exactly why certain prices have moved in certain directions. Hayek's insight was to understand that in all cases, what is known by a single agent is only a small fraction of the sum total of knowledge held by all members of society. A decentralized economy thus complements the dispersed nature of information spread throughout society. Much like transactions propagating through mempools, specific and granular market dynamics can efficiently propagate through an entire economy via price signals.

“The marvel is that in a case like that of a scarcity of one raw material, without an order being issued, without more than perhaps a handful of people knowing the cause, tens of thousands of people whose

identity could not be ascertained by months of investigation, are made to use the material or its products more sparingly; that is, they move in the right direction.” —F. A. Hayek

It's no surprise that in our present Information Age, Hayek's essay is gaining prominence anew. For example, *The Use of Knowledge in Society* is central to Jimmy Wales' philosophy for how to manage the Wikipedia project. At the outset he would “imagine a world in which every single person on the planet is given free access to the sum of all human knowledge.” Extending Hayek's thesis beyond the purely economic realm and into all knowledge, what is more likely to be successful? The centrally-planned mission of Google to “organize the world's information”, or the organic, open Wikipedia built on the foundational Hayekian idea that “when information is dispersed (as it always is), decisions are best left to those with the most local knowledge?”

Applying these ideas back to the economic information spaces of Bitcoin, the impactful nature of mempools becomes apparent. When a participant is attempting to broadcast a transaction to the Bitcoin network, it matters not why their mempool is giving them certain indicators. But those indicators carry enough real-time knowledge from the activity of the **entire global Bitcoin economy** to make the best economic decision for those UTXOs they control at that point in time.

If, for example, a network participant's mempool is starting to fill up, one might say the network is getting “busy.” This might be because more people were buying and withdrawing Bitcoin from exchanges in anticipation of some bullish event. It might be because participants are nervous about the solvency of a particular exchange and they're running for the exits via base-layer final settlement. It might be because a large actor is consolidating UTXOs ... And so on and so forth, and in all sorts of combinations. But the basic principle of interacting with mempools is this: when a block is mined, transactions are removed from mempools. Others continue to fill it up. And sometimes there's a traffic jam if new transactions arrive at a higher rate than they are cleared.

Many of these hypotheses can, of course, be tested with further research, but what's important for the average actor is simple and doesn't require any further knowledge: for whatever reason, more transactions are awaiting settlement. As a result, your mempool is telling you that you'll have to pay up for your place in the limited information space of a newly minted block.

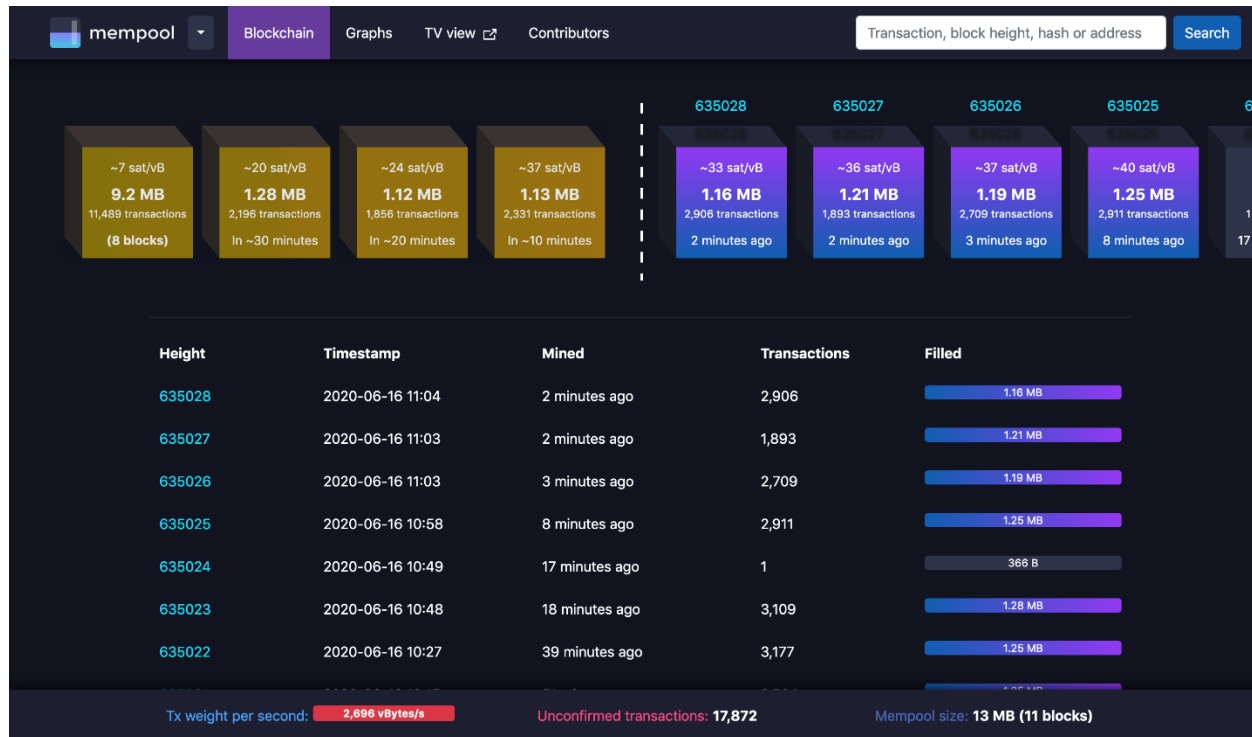
This principle can be illustrated with tools such as the beautiful <https://mempool.space/>. On the live graph view below, stratified by feerate, it can be observed that mempools have been getting slightly busier over the course of the past two hours. With 13MB of unconfirmed transactions outstanding, the tool estimates the network will require the next 11 blocks to clear if no new transactions are added. We don't need to know *why*. It is helpful enough that we can observe the entire global demand for blockspace (i.e. demand for inclusion in a future mined block) in this concentrated, open knowledge. The white dotted line on the graph shows us which bids are most likely to be included in the next block. Though this is no guarantee, it's a calculation we can make based on what we know to be one of the primary miner incentives: earning as much from fees as possible.



<https://mempool.space/graphs>

From the knowledge of global blockspace demand illustrated in the mempool visualization above, we can go on to calculate estimates for Bitcoin's native price signal—feerates—and other knowledge such as estimated time to settlement. In the "Blockchain" tab below, the tool takes knowledge such as the current state of the mempool, the protocol's allowable block size, and the protocol's target block time of ten minutes to estimate the price a transaction must bid to be included in n number of blocks, or $n * 10$ minutes as measured in human time.

Based on the needs and knowledge exclusive to each individual participant looking to use the protocol at any given moment in time, they make their own calculations for the fee they can afford to pay and the urgency with which they need their transactions reflected in the global ledger of final settlement. And they perform this calculation against the entire sum knowledge of every single other participant using the network across the entire globe, all concentrated into these few signals.



<https://mempool.space/>

Bitcoin's Native Market

There is something underappreciated about the nature of mempools. Taken together as the abstract idea of “the mempool”, they represent a bustling global marketplace of pure distilled information, interpreted in line with other knowledge to give an idea of the global demand and availability to settle transactions, with no group of people responsible for anything—just individuals doing what’s required to meet their needs with whatever means they have available to them.

From the Heyekian perspective, specific knowledge of the external factors influencing the price signal for settlement are irrelevant to the individual participant—what your mempool tells you is all you need to know. It’s a pure, network-native marketplace that can be efficiently interacted with in the complete absence of any external inputs. You’re using information space (scarcity encumbered by UTXOs, measured in units of “bitcoin”) to buy a position for settlement in another form of information space (block space) based on summarized global knowledge you can glean from yet another, more ephemeral, information space (mempools).

The mempool is Bitcoin’s town square. It’s a brutal, unrelenting marketplace—the exchange at the center of the entire Bitcoin network’s economic activity. Everyone is bidding their worth to anyone who will listen. Sometimes they won’t be heard and they’ll miss a good opportunity. Sometimes they’ll bid low and get lucky. This is a marketplace that exists purely in Bitcoin’s information spaces. No restricted access via on or off ramps. No one pleading their case for a charitable interpretation of their needs. Just a ruthless, global settlement market native to the Bitcoin network. If Bitcoin does indeed become the center of global commerce in the years to come, the mempool will be the single most important component to watch for many of those using it.

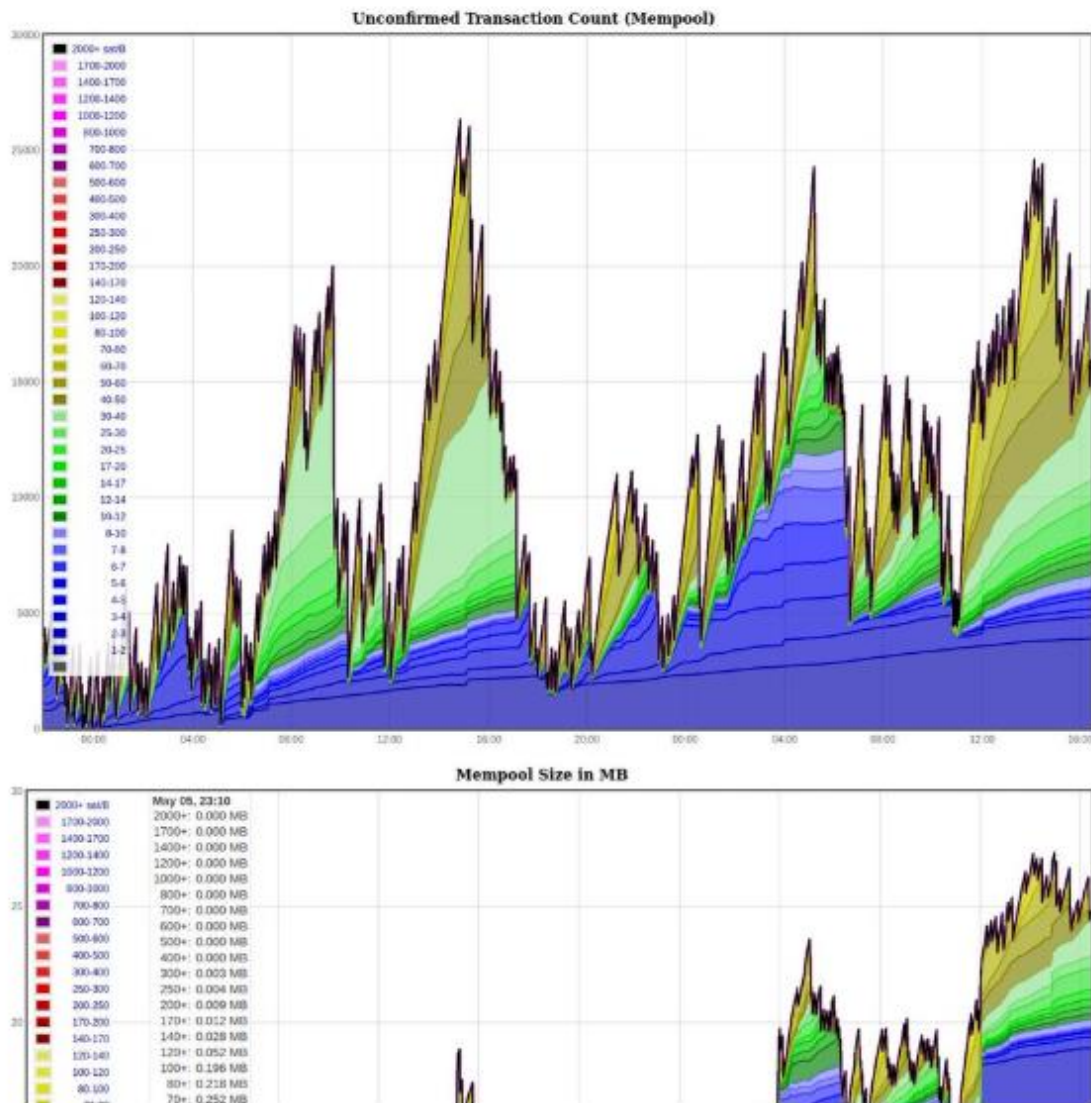
In this pure anarchic (meaning an absence of authority, not chaos) global market, daily news updates will attempt to interpret contributing factors to make predictions for concerned participants. High profile participants will pontificate on what certain events “mean.” Gossip will spread about large participants wasting their precious, scarce UTXO information space overpaying on fees. So too will companies be frowned upon and called out for such inefficient use of blockspace that they affect the entire network, such as the case of the daily BitMEX broadcast at 13:08 UTC, which regularly changes the shape of the mempool and forces other participants to adjust their bids or expectations as a result. The author of that piece, B10C, is an early example of what might be considered a mempool researcher. Prolific Bitcoin StackExchange contributor Murch might similarly be considered thus.



Murch 🍌
@murchandamus



In before some chimera muses about transaction spam again:
Someone appears to be queuing low-time-preference transactions to benefit from periods with low blockspace demand. Given the low count (see top) and large size (see bottom), these appear to be consolidation transactions.



♥ 20 7:49 PM - May 7, 2020



👤 See Murch 🍌's other Tweets



For similar graphs: <http://bitcoin-mempool.info/#0,24h>

When people talk about the Jevons paradox as it relates to predictions about Bitcoin's future, this network-native marketplace for transaction settlement will be the centerpiece of such a dynamic. Jevons paradox is the observation that increasing efficiency from technological progress does not alleviate pressures on the underlying commodity's use, but instead tends to increase the rate of consumption from rising demand. Thus, as efficiencies are found for Bitcoin's blockspace—pooling transactions to share costs, second layer solutions clearing in isolation and only settling intermittently, etc.—the opportunities they bring for more participants and more use cases will be profound.

And without talking to another soul or learning any of the specifics, all of this will be reflected in the simple knowledge we can glean from our mempools.

How I checked over 1 trillion mnemonics in 30 hours to win a bitcoin

By John Cantrell

Posted June 18, 2020

TLDR;

* Alistair Milne tweeted that he planned to giveaway 1 Bitcoin in a wallet generated using a 12-word mnemonic.

- With 8 known words there are 2^{40} (~1.1 trillion) possible mnemonics.
- To test a single mnemonic we have to generate a seed from the mnemonic, master private key from the seed, and an address from the master private key.
- I wrote a CPU version in Rust to benchmark performance of a CPU solver. My Macbook was only able to check ~1,250 mnemonics per second which means it would have taken about **25 years** to check all 2^{40} possible mnemonics.
- I ported all necessary code for generating and checking a mnemonic (SHA-256, SHA-512, RIPEMD-160, EC Addition, EC Multiplication) to OpenCL C which is a programming language to run code on a GPU.
- The GPU version was able to check ~143,000 mnemonics per second which means it would take ~83 days to check all 2^{40} possible mnemonics.
- I wrote a server application that would orchestrate the distribution of work into batches of ~16 million mnemonics to a pool of GPU workers. Each GPU worker would ask the server for the next batch of work to do, perform the work, and log the result back to the server.
- I spent ~\$350 renting GPUs from vast.ai (plus ~\$75 for free from Azure).
- I was worried about other people doing the same and is why I included a .01 BTC miner fee. I didn't think even this would be enough and thought there could be a 'race to zero' where people continually increased the fee trying to get the miners to include their transaction in the next block.
- I have open sourced all the code used to do this. Please see the bottom of the article for the links to the various projects.
- Creating a contest that isn't won by software is difficult. I'd like to pay-it-forward and try crafting one myself. Follow me on Twitter @johncantrell97 for details.

Full Story

Alistair Milne tweeted that he planned to giveaway 1 Bitcoin in a wallet generated using a 12-word mnemonic.

This most likely meant it was generated using a BIP-39 mnemonic and was later confirmed when he provided the first few seed words and eventually the entire BIP-39 word list in a tweet.

A BIP-39 mnemonic is generated using words from a fixed list of 2048 potential words. Each word is represented by an integer from 0 to 2047 corresponding to its position in the list. In binary you need 11 bits to represent a number up to 2047. Therefore to represent a 12-word mnemonic you would need 12×11 or 132 bits. It turns out BIP-39 uses 128 bits of randomness and then uses SHA-256 to generate a 4-bit checksum that is appended to the end of the original 128-bits to get you the required 132 bits for 12 words.

This means if we wanted to iterate all possible 12-word mnemonics we need to count from 0 to $2^{128}-1$, where each number can be interpreted as a single mnemonic, converted to an address, and then checked against the address that holds the 1 BTC. Seems pretty easy at first glance but we quickly learn that this number is way too large to iterate in a timely manner.

Luckily, we do not need to actually check all 2^{128} possibilities because Alistair was going to release 1 seed word every couple of days. Each seed word we collect reduces the possibilities we need to check by a factor of 2^{11} or 2048.

He also mentioned he was going to release the last 3 or 4 words all at once to prevent brute forcing (or so he thought) so this meant I would need to be able to brute force at least the last 4 words in at most a couple of days for this to work in enough time to claim the prize.

With 8 words that means we know 8×11 or 88 bits of the 128 bits we are trying to figure out. It means there are 'only' $2^{(128-88)}$ or 2^{40} possible mnemonics we would have to check. This is 1,099,511,627,776 or roughly 1.1 trillion possible mnemonics.

I wasn't sure how long it would take to try 1 trillion possibilities so I wrote a quick program to get a baseline benchmark, so I could have some sense of exactly what I was dealing with, and if I thought it would even be possible to do.

The strategy I was going to use was to calculate a start and end number that I needed to iterate between based on a set of known input words. For each number I would calculate the address corresponding to that number and then check if the address was the one that held the 1 BTC. If it was the address I would then create and sign a transaction to sweep the funds into a wallet I control.

The first version I wrote in Rust using existing libraries (rust-bitcoin, rust-wallet, and ring) to handle all the hashes and elliptic curve math. Doing some quick benchmarking proved that using a CPU for this was not going to be feasible.

My laptop (2.5 GHz Dual-Core Intel Core i7) was only able to perform ~1,250 mnemonic to address checks per second or about 108,000,000 per day. This means it would take my CPU about **25 years** to generate and check the 1 trillion possibilities needed to brute force the mnemonic while only knowing 8 of the words.

In order to achieve this in 1 day I would need to be able to improve the performance by about 9,000x its current speed.

My next attempt was to rent a more powerful machine to see how fast the same CPU-only version could potentially run. I rented a 32-core CPU-optimized machine from Digital Ocean and was able to record a benchmark of ~8,000 per second which was only ~6 times improvement over my laptop.

I would still need about a 1,000 times increase in performance from here in order to do this. I didn't think I was going to get anywhere close to that by trying to optimize the CPU code as it was likely already pretty well optimized in the existing libraries I was using.

Enter the GPU

Over the last decade there has been a rise in utilizing GPU's to perform general purpose programming. In Bitcoin we saw this relatively early on when people started using GPU's to perform the operations required to mine.

So how exactly does a GPU help us solve this problem faster? It turns out that a single GPU core is actually slower than its CPU counterpart when used for general purpose programming. The performance gains are typically seen when you are able to efficiently parallelize a program. This is because a single GPU device typically has thousands of cores you can utilize for your computation.

Luckily for us, our problem parallelizes extremely well. Each of the 2^{40} numbers we want to check runs the exact same computation (number -> mnemonic -> seed -> master private key -> address). This means we could give each GPU core 1 number to try and could run thousands of attempts in parallel.

I quickly learned about OpenCL which is a standard open source programming language for writing software that will run on almost any GPU device. OpenCL C is very similar to the C programming language with a few differences. One of those differences is how memory works. In a GPU you have four main types of memory available to you (Global, Constant, Local, and Private). Global memory is shared across all GPU cores and is very slow to access, you want to minimize its use as much as possible. Constant and Private memory are extremely fast but limited in space. I believe most devices only support 64kB of constant memory. Local memory is shared by a "group" of workers and its speed is somewhere between Global and Constant.

My goal was to fit everything I needed into the 64kB of constant memory and never need to read from global or local memory to maximize the speed of the program. This proved to be a bit tricky because the standard precomputed secp256k1 multiplication table took up exactly 64kB by itself. Luckily, I was able to precompute a smaller table that used only 32kB but ran ~75% slower than the full table. The BIP-39 word list took up another ~20kB and the SHA2 hashes took up another ~6kB so I was already using ~58kB of the 64kB available to me right from the start. This left me with about ~6kB of wiggle room to work with.

Ideally I would be able to do all of the computation on the GPU. This meant number -> mnemonic -> seed -> master private key -> address all calculated by the GPU and written in OpenCL.

What exactly needs to be implemented to handle each of those steps? Let's dive into each step we need to take to go all the way from a number to the bitcoin address. If you don't care about these details then just skip ahead in the article to the **Implementing in OpenCL** section.

Convert a Number into a 12-Word BIP-39 Mnemonic

Let's look at an example of how you can convert a number into a 12-word seed.

First let's start with a really big number:

34,267,283,446,455,273,173,114,040,093,663,453,845

From here we need to convert this number into a 128-bit number in binary.

```
0001100111000111101000111000001111010011000101110001100100100010
0111110101001000101010000011111100000111001010100110001010010101
```

We can get the last 4 bits (the checksum) by calculating the SHA-256 hash of this value and taking the first 4 bits of the result. In this case we get a checksum of 0101.

Now we append the checksum to the end and split our 132 bits into groups of 11 bits:

```
|00011001110|00111101000|11100000111|10100110001|01110001100|100
10001001|11110101001|00010101000|00111111000|00111001010|1001100
0101|00101010101|
```

We then convert each group of 11 bits into a number representing the index:

```
|206|488|1799|1329|908|1161|1961|168|504|458|1221|341|
```

Finally we use these as indices into the [BIP-39 english wordlist](#) to find each corresponding word:

border dial thought plastic immense muffin vivid bench disease deer obvious click

This is how we can map any number to a 12-word mnemonic. This step only costs us 1 SHA-256 calculation.

Mnemonic to Seed

The next step is to take this 132-bit mnemonic string and use it to generate a 64 byte binary seed. How do you extend a 132 bit string into 64 bytes? BIP-39 does this using a [Password-Based Key Derivation Function](#) with [HMAC-SHA512](#) as the hash function, the string "mnemonic" as the salt, and the 12-word mnemonic as the password. It also uses 2048 iterations and each iteration requires two SHA512 calculations. This means this step will cost in total ~4096 SHA-512 calculations.

This is similar to how a lot of websites store hashed passwords in their database. The main idea is to make it slow to guess lots of passwords when trying to brute force the hash of someone's password. You can control how long it takes to check a single password by increasing the number of iterations or using a slower hash function like scrypt or bcrypt.

Seed to BIP-32 Master Private Key

Once we have a seed we need to convert it into a BIP-32 (HD) Wallet. You can read the [full BIP for all the details](#) but at a high level BIP-32 defines a way to generate a master private key from a seed and then use that master key-pair to generate up to 2^{512} child key-pairs.

It's a great solution for building wallet software as it makes it easy for a user to backup a single secret (their mnemonic) but to be able to generate nearly endless addresses (for all practical purposes). It has other nice benefits where you can generate child public keys without needing the private keys to be present (great for businesses that need to generate receive addresses without needing to have private keys on their server).

To convert our seed into a master private key according to BIP-32 we need to calculate HMAC-SHA512("Bitcoin seed", mnemonic_seed). HMAC-SHA512 produces a 64 byte output. We take the first 32 bytes as the master private key and the other 32 bytes are used later as the 'chaincode' to 'extend' the key when generating children key-pairs.

To calculate [HMAC-SHA512](#) of a 132 byte input will take only two SHA-512 calculations.

Master Private Key to Address

This step involves taking our BIP-32 master private key and deriving child key-pairs based on the derivation path required to get to the address that holds the Bitcoin. If we look at the [address in an explorer](#) we can see that it was generated using [BIP-49 P2WPKH-nested-in-P2SH](#).

This means the derivation path is in the format `m / 49' / coin_type' / account' / change / address_index`.

Figuring out the derivation path was a huge risk for this project. I assumed that Alistair simply generated a new wallet and the only transaction made was to deposit the 1 BTC. With that assumption it means the derivation path for the first address would be `m/49'/0'/0'/0/0`.

This means we need to take the Master Private Key and generate three hardened private keys and then two normal private keys.

Each hardened private key requires a HMAC-SHA-512 calculation (2 SHA-512 hashes) and one secp256k1 scalar addition.

Each normal private key has the same requirements as a hardened key plus the need to calculate the associated public key from the private key. To calculate the public key we need to perform an elliptic curve multiplication of the scalar represented by the private key by the secp256k1 group generator point G.

The last step is to take the calculated public key and convert it into P2SHWPKH address. This involves building the correct [script](#) and then using hash160 (RIPEMD-160 followed by SHA-256) to get the address and then SHA256 (twice) to calculate a 4-byte checksum.

In total this step costs us 10 SHA-512's, 3 SHA-256, and 1 RIPEMD-160 hashes. It also costs us 5 EC scalar additions and 3 EC multiplications.

Total Cost

We have to do all of these steps for EACH mnemonic we want to try:

Number to Mnemonic – 1 SHA-256

Mnemonic to Seed – 4096 SHA-512

Seed to Private Key – 2 SHA-512

Private Key to Address – 10 SHA-512, 3 SHA-256, 1 RIPEMD-160, 5 EC Additions, 3 EC Multiplications

At a glance it looks like the seed generation step will be the slowest though it's hard to know how to compare SHA-512 hash to EC operations in terms of cost without some benchmarks. It will turn out that they both are relatively slow compared to the other steps but the seed generation is at least an order of magnitude more costly than the others.

Implementing in OpenCL

So in order to implement this entire flow in OpenCL I would need a way to perform SHA-256, SHA-512, RIPEMD-160, EC Addition, and EC Multiplication. I would also need to orchestrate it all together in a way to solve my problem.

My strategy was to find open source C implementations of all of the algorithms and port them to OpenCL C. I started with SHA-256 and SHA-512 because these alone would allow me to calculate number -> mnemonic -> seed and I knew that generating the seed was the slowest part by far.

Eventually I got seed generation working in OpenCL and my first benchmark using a nVidia 2080Ti showed me that I could generate 142,857 seeds per second. Wow! Now we were getting somewhere.

This meant a single nVidia 2080Ti could generate ~12 billion seeds per day. This still meant it would take **83 days** to generate all trillion seeds. That was a lot better than the 25 years my CPU was going to take. However, this was still only generating the seeds and a seed wasn't enough to know if the mnemonic was correct or not. I would still need to complete the process of converting the seed all the way to an address to be able to verify if it was the correct mnemonic.

I then went back and benchmarked my CPU version of the seed to address generation to see how long that would take. The 32-core Digital Ocean machine was able to process about 52,000 seeds per second. This was pretty decent but after the OpenCL seed generation improvements it was now the bottleneck and would still take over 221 days to complete. Additionally, I would need to coordinate moving the seeds generated from GPU back to the CPU to finish their processing. This coordination would take time and be a more complicated program to write.

My goal was to move the entire calculation into the GPU.

This meant I needed to be able to perform EC math (addition and multiplication) in OpenCL. I took the [open source libsecp256k1 implementation](#) that Bitcoin uses and ported it to OpenCL C. It required me

to first understand how the libsecp256k1 library was structured and what exactly I needed to port in order to generate an address from a master private key.

It turned out to be about 2,000 lines of code that I needed to port. Luckily, OpenCL C and standard C are similar enough that there wasn't a lot of changes required. The changes involved me implementing some memory management functions like memcpy, memset, and memzero that OpenCL does not support. It also involved me removing the blinding that is done when performing EC Multiplication and precomputing a 32kB table instead of the default 64kB one.

After all is said and done I ran some sanity tests and was surprised to discover that my OpenCL implementation was actually working correctly.

I then re-ran my benchmarks using the 2080Ti and saw that the time added to calculate the address from the seed using the GPU was negligible. It only added a few hundred milliseconds per 1 million seeds.

I was now able to run the entire process 100% on a GPU but it was still going to take ~80 days to enumerate the 1 trillion possible mnemonics using a 2080Ti.

I then tried running it on a bunch of different video cards (1080, 1080Ti, 2070, 2070Ti, Tesla K80, Tesla P100, and Tesla V100). To my surprise the performance didn't change that much across GPUs. Even the top of the line Tesla V100 was only about 15% faster but cost almost 4x as much to rent.

On the lower end the 1080/1070s were roughly 3 to 4 times slower than the 2080Ti but were only about half the cost. The 2080Ti seemed to be the most cost efficient card to use for this problem. How many could I get and how would I orchestrate all of this?

If I was to solve this in 24 hours I would need the power of about 80 2080Ti's.

Orchestrating a GPU Pool

If I wanted to distribute this problem across multiple GPUs the simple answer is to just break down the 2^{40} numbers we need to iterate into 80 equal parts and run each part on a single GPU. Unfortunately, it would not be this simple.

I first needed to figure out how I was going to get access to all of these machines. My first thought was to use the major cloud providers (AWS, Google Cloud, and Microsoft Azure). I quickly learned that these companies have strict quotas on the number of GPUs you can provision (some of them ZERO!) with a new account.

Luckily, I came across a [GPU marketplace](https://vast.ai) (Vast.ai) that let people who had unused GPUs rent them out to anyone who wanted access to GPUs. They had large inventory of 1080's and 1080Ti's but not as many 2080Ti's as I needed. The inventory fluctuated all the time depending on how many people were renting them, how much they were willing to pay, and how many providers were online at the time.

This meant I wasn't going to easily be able to allocate exactly 80 2080Ti's and evenly distribute my workload across them all.

I ended up building a simple centralized server that would act as the distributor of work. It is pretty similar to how a mining pool works. Each GPU worker would make a request to the centralized server for a batch of work to perform, perform the work, and then log the work (and a solution if it found one) back to the server. Each worker would continue to do this in a loop until there was no more work to do.

This meant I could easily spin up as many cards as I wanted as fast as I wanted and the central server would be able to keep track of what the next batch of work was when one was requested. Each worker instance didn't need to know anything about what part of the work it needed to perform, it could just blindly ask the server for the next batch to work on.

This solution does add more time in terms of network latency. I needed to make the batch size large enough so that the added network latency was a small percentage of the total time. I ended up using a batch size of 16,777,216 which means there would be 65,536 batches of work to compute all 2^{40} possible mnemonics.

A 16,777,216 batch took the 2080Ti slightly less than 2 minutes to compute. This means the less than 1 second network latency was adding less than 1% additional computation time.

Testing the System

This ended up being a more complicated system than I originally envisioned and I was worried there would be a bug or that it wouldn't work as expected when the time came. I ended up going through a full end to end test to make sure everything was actually working.

I created a wallet with a new BIP-39 mnemonic and transferred 0.0001 BTC into it. I then initiated my system with 9 known seed words (so it wouldn't take as long or cost me as much). I rented a couple 2080Ti's on vast and let it rip. Within 20 minutes it had found the solution and swept the 0.0001 BTC to a Trezor wallet I controlled. I felt like I was ready even though I was unsure I'd actually be able to get enough compute power in time to perform the task when it was needed.

I felt like there was still a way to optimize the SHA-512 code I was using by trying to port the version of SHA-512 that hashcat was using as they have an extremely optimized version. Since SHA-512 was the most used method and the current bottleneck any improvements made here could drastically reduce the number of GPUs needed. I was about halfway through this implementation when Alistair released the 8th word.

The Big Day

I immediately threw away the optimized SHA-512 I was working on and went back to the version I knew was working from earlier. I started renting as many 2080Ti, 2080, 2070, 2070Ti, 1080Ti's as I could from vast.ai. In the meantime I had been able to get my gpu quota increased on Azure (+a \$200 free credit for new accounts) to rent up to 40 GPUs over there. Unfortunately, the machines I had access to over there were only roughly ~50% as powerful as a 2080Ti. However, this meant I was able to get roughly 20 2080Ti's for free from Azure alone.

At the peak I was testing about 40 billion mnemonics per hour. This means it should have taken around 25 hours to test the 1 trillion mnemonics. I knew that on average it should only take 50% of the time (depending on what the 9th word actually was). If the word started with A then it would finish in 1 hour and if it started with a Z then it would take the full 25 hours. Of course my testing rate was not steady at 40 billion per hour as machines on vast.ai come and go as people outbid me or go offline. I had to continually scan the list of available machines and rent more as they became available.

As the day went on without finding the solution I became worried it wouldn't work because there were a lot of ways that my approach could fail:

- I assumed the words he was releasing were in the correct order. If they were not in order there would have been 8! (factorial) more possibilities (making 8 words basically impossible to brute force) and my code wasn't trying the different permutations anyway.
- I assumed I had all 8 words correct. While most were obvious there were a couple where I felt like there could be other options. I was not trying any of those other options, only the 8 I thought were correct.
- I assumed he was using the first address of the first account of the HD wallet derived at m/49'/0'/0'/0/0. If he used any other derivation path (second or later address) I would not have found it. I was *REALLY* nervous about this one because there was no way I could know for sure what derivation path he had used. Luckily, he used a brand new wallet without generating extra addresses before depositing the 1 BTC.

After a full day of running my work server status showed that it was about 85% of the way done with testing all possibilities and I had largely given up hope that it would work. I literally almost turned it off at this point to implement a version that tested more than just the first address because I was convinced that assumption was wrong.

I couldn't get myself to actually stop it at that point as I had come so far so I just let it continue. To my surprise a little while later that evening (at 91%) and after almost 30 hours and exactly 1 trillion checks (1,000,710,602,752) it had found a solution!

I couldn't believe it had worked. I nervously plugged in my Trezor to check the balance to make sure I hadn't screwed up the code that generated and signed the transaction to sweep the BTC. To my relief the 0.99 BTC was there!

I then nervously waited for a confirmation to arrive. I was worried that another person (or eve Alistair) would try to steal back the Bitcoin by continually increasing the miner fee so that a miner would include their transaction over mine. This is one of the reasons I started with a relatively high fee (0.01 BTC). I didn't have time to implement a tool that watched the mempool for competing transactions and automatically bumped my fee but I thought it would be a good idea.

However, after a few minutes my transaction was included in a block. Wow, it really had worked.

Final Thoughts

I had a lot of fun and learned a lot working on this problem. I have been thinking of ways to run a similar type of giveaway while avoiding the possibility of someone writing software to win. It's not so easy actually.

Even if he had decided to release the last 5 words all at once to prevent brute forcing I could still have software running that was waiting for me to enter each word as I figured them out, assuming it was some kind of puzzle and automatically sweep the coins faster than any human could.

I was thinking he could have used a deeper derivation path and while my initial version of software would have missed this it would be trivial and not that much slower to check lots of derivation paths for the used address. I think the issue here is even for humans, the wallet software that handles the recovery process only scans for a small number of unused addresses before stopping so he couldn't have put it too deep if he wanted users to be able to use a normal wallet to recover it.

Another idea is to give the words out of order which would have made it impossible to brute force early but still doesn't stop me from using software to enumerate all possible orderings and sweep the btc faster than a human could ever hope to do it once enough words were released.

At the end of the day software will always be faster than humans at this kind of task. I think the only real way is to make the discovery of the actual words the difficult part. Some kind of puzzle where solving it provides you with all of the words at once so the race is more about solving the puzzle than it is about how fast you can enter the words.

The Software

I have made all of the projects I used to solve this problem open source for anyone interested in learning exactly how it was done. Hopefully it will be useful for someone learning about GPU programming or to help someone recover some lost BTC.

BIP39-Solver-CPU: This is the CPU benchmark tool I wrote in Rust to get an idea of how long it will take to solve on a CPU for certain number of unknown words

BIP39-Solver-GPU: This is the actual GPU version I ran on each worker GPU to solve this problem.

BIP39-Solver-Server: This is the actual server I ran that handled distributing the work to all the workers.

Bitcoin and the Trust Problem: Is Bitcoin adoption accelerated by the abuse of trust?

By Karo Zagorus

Posted June 4, 2020

Download the *Bitcoin and the Trust Problem*
original thesis PDF.

**Examining how our trust is being breached
and abused, how we are used for rent-
seeking, how governments impoverish us
through the use of Monetary Nationalism
and examining whether Bitcoin is the
solution to restore individual freedom and
limit the reach of government.**

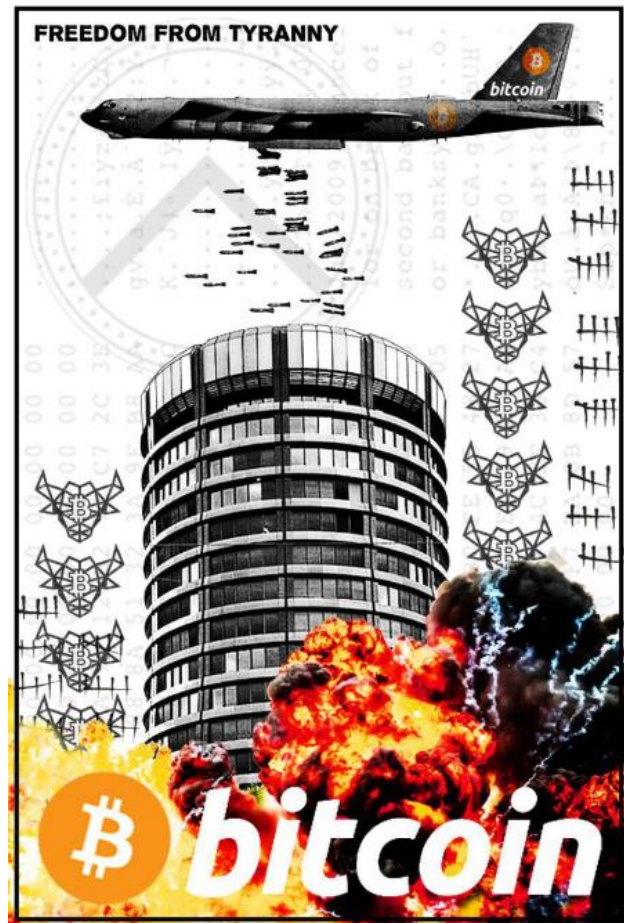
Art by Made X Forever

Disclaimer

This Thesis here, **is not**, in any sense, shape or form a **financial advice**. Information found in this Thesis are the findings of the author and his own personal views and does not constitute an advice in any form. Investing in Bitcoin, other Cryptocurrencies, Blockchain Technology or Companies that use Blockchain Technology comes with an **extreme risk**. Cryptocurrencies are **extremely volatile** and often traded on **illiquid markets**. Investing in cryptocurrencies can incur **complete loss of investment**. Consult a *professional* before investing. The author of this Thesis or his Consultants **are not liable** for **any damages** deriving from reckless **investments that resulted** from uneducated decisions that originate or manifest from information within this Thesis or based on the content of this Thesis. Loss incurring from reckless investment based on the findings in this Thesis **is not in any way the responsibility of the Author** of this Thesis.

*This is a scientific academic research; **it is not a financial advice.***

Public and private keys and addresses displayed within this Thesis are only for technical demonstration only._



BY PROCEEDING TO READ THIS THESIS YOU AGREE TO NOT HOLD LIABLE THE AUTHOR AND HIS CONSULTANT(S) FOR ANY LOSS OR DAMAGES RESULTING FROM INVESTMENT DECISIONS THAT WERE BASED ON THE CONTENT OF THIS THESIS. YOU FORFEIT ALL RIGHTS AND ABILITIES TO ABITRATION AND CLAIMS OF DAMAGES PAST, PRESENT OR FUTURE BY PROCEEDING WITH THE READING OF THIS THESIS. Released under CC BY 4.0 license.

Letter of Acknowledgement

I want to thank first my Family, my Mother, Father, my Grandmother and Grandfather for the past 10 years of my continued presence at home and giving me the opportunity to finish my studies in higher education.

The second person I want to thank is Satoshi Nakamoto for creating Bitcoin and showing millions of people around the globe that there can be alternatives and we can achieve those if we work hard enough to create them.

The third person I want to thank is Professor Miklos N. for taking the red pill and following me down the rabbit hole with this thesis as I went onto explore Bitcoin further to uncover its underlying past and its secrets. I thank you for your continued support and time listening to my crazy ideas and being open about them.

The fourth person I want to thank is Martin Habovštiak who introduced me to Paralelná Polis. Thank you for coordinating my stay in Bratislava and giving me this unforgettable experience of how freedom and liberty looks like. Also, I thank those who accompanied me and shared their views and experiences with me during my weeklong stay at Paralelná Polis. Further thank you for Modus Operandi, Giacomo, BitcoinOldGuy, Andrej, Erik, Simon, Richard, Palo, Dusky, Juraj and his mother Zuzka.

The fifth person I want to thank is Samourai Wallet for making it possible for me to attend the 6th Annual Hacker's Congress Paralelní Polis 2019 in Prague. You were right, it has changed my perspective and opened new doors of possibilities and opportunities for me. I want to also thank the organizers of HCPP19 and every other new and old bitcoiner friend I met at the conference.

I also want to thank Balint Harmat and David Molnar and the rest of the guys at Wasabi Wallet for participating in my research and allowing me to visit their office in Budapest.

Not last, I also want to thank Erik Jacobi and his wife Frankie for inviting me over to Hamburg for a weekend, for showing me around the beautiful City of Hamburg, showing me the problems modern society faces and giving me feedback on the progression of my thesis.

Also, I want to thank CandleLover for spending a day with me in Berlin and talking about all things that is Bitcoin. Also, a mention for his friends who I met with in Berlin.

I also want to thank the guys over at Paralelná Polis Kosice for showing me around the center of Kosice, sharing their cryptoanarchist experiences and initial experiences of how difficult it can be to start a Parallel Polis.

Another big thank you for jimbo for providing late stage feedback and showing me that my undertaking was not for nothing.

Also, a thank you for Kalle Rosenbaum for giving feedback on the Bitcoin section of this thesis.

I also want to thank my friend Silent Lamb who made it possible for me to attend Guns n' Bitcoin 2020 Switzerland in January this year. We survived the shootout at Lungern Bruning Indoor, the Luzern Coop Scare and beat Wuhan to it before it got there.

Before last, I want to thank my friends, Duck and Leffe for being there and accompanying me along the way as I worked on my thesis during my university studies.

And for last, I want to thank every Bitcoin Pleb friend of mine, O.G. Bitcoiner and Bitcoin Maximalist who I got to talk with and those who managed to share their experiences with me, both online and in the real world. So thank you guys, especially, Hodlonaut, 2357_is_prime, Psychedelic El Barto, Catoshi Meowmoto, FF2K, rusticbison, Fabio Krauss, Vlad Costesa, BTChap, MrHodl, Max Hillerband, CryptoScamHub, Shinobi, andhans, Dvor Ka, Dave Bradley, Francis Poulliot, Made X Forever, Steph B., Bitko Yinowsky, Martin Fischer, TDevD, American Hodl, Sebastian Geisler, Rory, CanEx, Martin Tan, Awyee, Chaz, Saint Bitcoin, Coinicarus, Tanuki, Nunya Bidness, BTCPat, Mr.Hash, StopAndDecrypt, CryptoNT, Stephan Livera, Grubles, 6102bitcoin, DK, Jingles, bavarianledger, Melik Manukyan, goodc0re, ovib0s, Travin Keith, Dr. Maxim Orlovsky, Olga Ukolova, Dafar, Bitcoin Only, paintedfrog, Ti Kawamoto, Bas Peters, WhiteRabbit, CryptoHangover, bitcoinpasada and everyone else I have managed to leave out by accident.

Thank you for being there every day and staying awesome, making every day unique and eventful with your presence and contribution to the community.

Foreword

Bitcoin. Often when we utter this one word, even as part of a question, we can never know what response we will get from those who we say it to. If we are lucky, majority of those who we will interact with have little knowledge of what Bitcoin is. Even less had the chance to hear about it, a fraction of that knows what it is used for, how it works, how it is created or what is the basic underlying principle of the entire system that is called as Bitcoin. (Taiberg; Bogart; Capital Creators)

There might be some cases when we manage to come across someone who have heard about it and understands the basic speculative spectrum of it, who will then immediately dismiss it as a vaporware tulip mania that is destined to crash to zero. (Cheng; De) Often these answers come from well-educated and knowledge individuals who have some or vast experience in the field of speculation and trading. (De; Monaghan; Golumbia) Since Bitcoin is not backed by any government or any scarce natural resource, they immediately arrive to the point of dismissal because they do not understand how it works or they cannot comprehend how “magical internet money” can have any value proposition at all. (Ossinger; English)

But, if we dig deeper and are extremely lucky, we might reach one of those select few out there, out of the more than 30 million early adopters (Szmigiera), who partially or actively, interact with Bitcoin as of

today. These individuals are the biggest question mark in Human History. We must ask the question, why these individuals went as far as to personally elect to use Bitcoin. Some of them mention a multitude of reasons, some among along the lines to invest into it, to speculate on the price of it, store value, protect personal assets from hyperinflation and to escape the reach of authoritative governments. (Bogart; Bohr and Bashir) Some might dismiss it, but it is apparent that Bitcoin is spreading, rapidly, according to a research done by Blockchain Capital, among members of the public, and as of today, we have still failed to find reasons why this is happening and what is causing it. (Bogart)

In today's world, (Hughes; Servon) there is an underlying problem related to the generalization of distrust towards aspects of modern-day institutions such as banks, money, and politics within not just Western Democracies, but in various parts all around the world. (Edelman) The order of trust, or similar forms of it that we perceive it, as of today, is being constantly challenged by outside factors in our relative space that we live in that seem to force members of our society to start exploring alternative solutions for their daily problems. (Fukuyama; Servon) Since Bitcoin, the mother of the Blockchain technology, seems to promise a future that brings us further liberty and financial freedom in a world that is riddled with exploitation and injustice. But this comes at a cost of a potential complete reformation every aspect of civilized life. (Swan)

Since as of right now, it is a matter of urgency that we research this extremely disruptive technology that forces a potential civilizational evolutionary transition on us, we must begin researching it immediately. But as an unfortunate fact, very few academics are actively considering the sociological and anthropological consequences that could result out of the few of available research focusing on Bitcoin. (Bohr and Bashir; Bashir, Strickland and Bohr) Considering the fact how fast the Internet became wide spread in the world, and now how much depends on its actual operation, we can see that there are clear parallels among the line between it and technology that are built right onto of the internet. For example, Social Media needed over 10 years to reach its current active userbase, and even in some countries, platforms like Facebook are the actual internet for those with access to it on their mobile devices. (Mozur; BBC Trending)

If we introduce in a new technology like Bitcoin, running on the internet and fulfilling all monetary aspects of currency, while society maintains its value through social consensus, hyperbitcoinization, (a hyperinflationary demonetization event in which fiat currencies exit usage by the decision of the free market (D. Krawisz)), might not be decades but just a couple years' time away. (Ammous; Bogart) Since Bitcoin is an antifragile system, that creates negative black swan events for its competitors, the deriding effects resulting from its adoption must be further subject of studies. (Taleb, Antifragile; Taleb, The Black Swan) We will now venture into this hidden world that so few can call themselves a part of.

We will discover the reasons why it exists and the mechanisms that keep it alive and make it revolutionary.

I. Introduction to the Dissolution of Trust

Ever since the beginning of time, trust was and is still a necessary element for human progress. In a world of survival and beyond it was the essential tool to provide humans with friendships and alliances. Without

trust, many elements of our modern-day society would not function, services provided to us would cease to work and to exist. Kings would have not ruled over lands and anarchy would have gone rampant in the whole world where everyone, is to themselves and nobody else can be trusted. Without this being possible, we would have not seen such human development across the two millennia. (Fukuyama)

Group formation's essential element is trust, this is how people with common interest were able to group together to survive, to build families and empires. For one man to go beyond the creed of the family and form relationships, trust was imperative to establish these connections. (Fukuyama)

Our ability to form trust is an essential human trait that enables us to establish relationships with entities and other human beings. Often this is difficult because trust is not a very morphable human trait, but something that is built or earned over time; although we can trust also blindly if situation is given. This inherent ability to trust, has cultural, religious, and political roots. Depending on the individual, where one is born, decides what will be the inherent cultural programming of the characteristics of this ability to trust. (Fukuyama)

In today's world, trust governs many layers of society, (Fukuyama) for example when we chose political parties, we can either vote under personal principles or by beliefs, onto candidates who, we trust or trust to a certain degree that they will be more effective at governing a country, and will not impede on our trust and support by embezzling funds, impede our rights and freedoms and turn a democracy into an oligarchy. When we call the Ambulance, Police or the Fire Service we believe and trust that they will respond and provide help in the time of need because they serve society independently that of its affiliation and citizenship, humans in need will be provided help in a functional country with a functional public emergency services system. We believe that the medics in the ambulance will be well trained, that the police will be impartial and not ask for bribes, and that the fire fighters will risk their lives to save those who are in imminent danger. We trust that agents of security services of our nation work tirelessly to avert dangers, prevent terrorism, and disrupt most forms of espionage without impeding on the rights, liberties, and privacy of its citizens.

When we put money into a bank, we trust the institution, that it will be responsibly managing our money and not spend it, not lend it out recklessly, not charge us exorbitant fees and embezzle our money through questionable investments and loans. We expect contracts to function as is written, that attempts to bridge trust especially in low-trust cultures, like when we sign up for a Mobile Service, Health Insurance or Car Insurance, we expect and trust that the service provider will not breach that contract and charge us extortionate charges or fail to pay us if we file for an insurance claim. We also trust that a central bank will maintain a healthy monetary policy. That it will not go rampant with its ability to print out countless amounts of fiat money, with that over inflate the currency that we use, that it will keep our economic interests at the forefront to keep the country competitive and that the money it creates wield value and others will accept that form of value as a monetary unit of account. We can also trust blindly others, like neighbors, that they are not going to attempt to breach into our house and/or threaten our lives.

We expect that our legal system will work and function as normal, under the guides of the constitution and present laws, protecting society from harms, mediating conflicts, and enforcing contracts. When we go into a supermarket, we expect that the food products sold there are safe and won't damage our health or

worse, and that other products are safe, we trust that the consumer safety governmental organizations will provide necessary guidelines to create this safety net that we can rely on, that will prevent others from selling poisonous food or electronical equipment's that are defective, that can fire hazard or cause cancer.

Trust is also necessary for economic progress and for the creation of prosperity. (Fukuyama) Functional economies in the modern world require the formation of businesses and their expansion to create progress and this can only be accomplished with the accumulation of wealth. (Fukuyama) The money everyone makes and earns today is also based on trust; its subjective value is based on nation states that give fiat currencies value through exercised enforcement of value through the means of National Monetarism. (Ammous) Often people don't consider money such an important matter, but as it is, it seems we are undervaluing its importance to society, (Ammous) because without any form of currency or unit of account we would have not had a formation of any country, (at least initially). (Ammous) soldiers would not serve their kings if they did not receive a form of reward that was of value. These in the early days were usually in the forms of dowry or a valuable animal that they could use for husbandry and later as transition happened towards gold and other units of account made it possible to better store value over time, this created prosperity and allowed empires to rise or fall. (Ammous; Fukuyama)

Small family businesses are also trust based, the father, mother or son also works at the company, but as the company keeps prospering and producing goods, making more money it becomes necessary for it to keep expanding to maintain its own competitiveness which essentially requires members of the family to start devolving this trust and decentralizing it. (Fukuyama) The ability to incorporate was a turning point that allowed families to turn from sole owners into shareholders. When small family businesses turn into megacorporation, they essentially become extremely hard to manage alone and this is where it becomes difficult in certain cultures to trust others with the leadership of a company that they created and lead for years. Therefore, trained management became necessity to consider and hire. (Fukuyama)

Large companies like Apple, Mitsubishi, Samsung, Sony have all went through these phases and still exist as of today because their transformation into international organizations was made possible by the decentralization of trust while still making it possible for shareholders to maintain oversight over the operation of the companies. If competitiveness would have not prompted the families (those who operated small and medium sized businesses) to incorporate their business, there would be no possibility for the creation of prosperity. If Steve Jobs would have not partner with others when it became necessary to come out of the garage, we would not have fancy electronics such as like the Apple iMac Computers and iOS Phones and Tablets. If Bill Gates would have not formed Microsoft back in the day, we would probably use something different than Windows. If Larry Page and Sergey Brin would have not trusted each other, we would not have Google the Search Engine, nor any Android smart phones. (Fukuyama)

In a normally functioning society, we expect these to function properly, which serve as the basis of our lives, our country, and its economy and that of the world's.

When we start facing problems regarding our trust in others, when others step past our trust's boundaries, when they impede on that or abuse it, then we start facing problems and begin to distrust others. Distrust makes it much harder to establish trust in others. (Edelman; Fukuyama) If our trust is abused, chances that it will get permanently damaged and distrust will inhibit the formation of trust. It will make it difficult

for example to trust politicians if they often become corrupt, it will be difficult to choose new candidates and chances that people will not go to vote any longer due to their distrust of the system. (Edelman) We will distrust the police more if they are abusing their authority.

We will distrust banks if they are misusing our deposits or fail to be held accountable. (Fukuyama) Central Banks can also betray our trust by overinflating our currencies to create more immediate value for themselves and steal from its citizens throughout inflation. Similarly like in the case of Venezuela, where the value of the Venezuelan Bolivar has gone through a hyperinflation and because of that Venezuelans must barter every day or use US Dollar notes to buy goods and to access services. (Ammous) This ability of central banks to inflate the monetary supply has made it possible to wage unlimited warfare and also apparently served as the cause of both World Wars. (Ammous) After World War I, Austria faced a hyperinflation because it has begun printing out more money than the gold reserves that were available to backing its currency and therefore the Austrian Crowns have lost a tremendous amount of value because of the reckless printing of money. (Ammous) Germany after World War I also have attempted to pay back its reparations using inflation, they printed out unlimited amounts of Deutschmarks to finance their debt but instead it has led to the collapse of their economy during the Great Depression. (Ammous) Previously, wars before Monetary Nationalism required rulers to tax subjects to fund wars, and these were limited in scale and size. (Ammous)

As of today, it is apparent that we are living through the crisis of trust. Until recently there been no ways to eliminate the abuse of trust. This abuse of trust seems to endanger the networking of human beings, which is required to promote progress which in turn allows the creation of shared prosperity in society. (Fukuyama; Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System) And this long standing vacancy for alternatives made it possible for others to abuse this trust, repeatedly, especially within the United States' banking industry. (Servon)

The 2008 Global Financial Crisis has also accelerated this problem. Today we are facing an increasing trust problem, the erosion of trust or possibly the establishment of distrust, as shown in the Edelman Trust Barometer. It shows that trust is on the decline globally, at unprecedented scale as never seen before. (Edelman)

In this Thesis, I am set out on the journey of examining this problem that we are facing today, by looking at core institutions of our society and examining them and seeking out why they are not working as how we are expecting them to work.

We are going to explore pressing matters that affect our daily lives and continue to challenge our world views. Events that have played a pivotal role in creating the hypothetical destruction of trust within society. (Edelman) We will look at certain possible causes of this dissolution, we will examine and contrast American events to Hungarian and other ones and attempt to correlate them to the given problem.

The research methodology will consist of examining empirical evidence of the mentioned effects and processes. Later with this we will weight their importance and see how they are contributing as a main driving force towards the adoption of the potential solution. (Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System) By examining historical events and currently ongoing issues, we will see how

trust is put to a test in today's world. Only by this we will be able to figure out what is truly going on (Andersch; Pritzker; Prentice and Clown; Huebner; Ammous; Adler) and it will allow us to better understand why people do what they actually do to bridge or solve this problem permanently.

A.The Unbanking of Trust

Ever since the start of the 2008 Financial Crisis, the factor of trust been an ever-increasing problem. (Edelman) Trust since 2008 has been on the gradual decline. (Edelman) This is a big problem, because many of our systems demand some amount of trust to function properly. We often must trust politicians who also interact with our financial system and legislate laws that make changes to monetary policy. We also must trust other third-party banks or money processing third parties like PayPal, Venmo or CashApp to handle our transactions. (Servon) Banks and other payment processing third parties (E.g.: MasterCard) are essential for us to make daily transactions; to buy food in shops (physically or on the Internet) with debit or credit cards and are often required by employers (for example mostly in Europe) to receive their monthly wages. When financial institutions begin limiting access to their services apparent problems started to happen and it becomes much harder for those who seek lines of credit to get by. In the US there has been a transition from using lines of credit for the wants to the needs and essentials which dramatically increased their usage and their demand. (Servon)

Banks, up until 2008, have thought of themselves as invincible institutions who were protected from the dangers of financial collapse, where central banks would attempt to bail them out with fresh government money to provide liquidity for their services. But this have changed in 2008 when the Federal Reserve of the United States has refused to bail out Lehman Brothers. (Servon) This has caused a massive cascade of bank failures in the United States and abroad, and intensified the global financial collapse. (Servon)

Banks, during the 2008 Financial Crisis in the United States, have resorted to restructure debt and close off credit lines to debtors who suddenly found themselves in hot water. According to Lisa Servon, there been many issues preceding this problem starting from the 1980's merging of Residential and Investment Banking Sectors (Federal Reserve Bank of St. Louis), the racial bias in credit worthiness reports and the under rating of client's credit rating from Prime to Sub-Prime which came with higher interest rates. Ever since the 1980's Banks transitioned from serving the people towards serving their own interests (Servon) by eliminating the access of middle- and lower-class citizens, who are financially struggling⁶, to have an active and affordable bank account and imposing trickery through contracts that increased the fee profits of banks. This sudden change of focus for banks towards a fee based profit structure driven people away from them, forcing those with less income to choose alternative financial institutions such as Check Cashers like RiteCheck in the State of New York and Pay Day Lenders in other parts of the country where it is legal. (Servon)

Those who were luckier not to have their credit line taken away permanently had seen their yearly interest rates go up dramatically due to being put also into Sub-Prime credit category automatically when automated systems de-risked outstanding banking debts. This have directly led to the question whether Banks have lost any sense of social responsibility they have once had towards society. (Servon) As it

appears, in the past this was not the case, when Residential branches were still separate from Investment Banks. A transition of change has gone through where banks have completely lost touch with their clients and were no longer worthy of any meaningful consideration due to complex state and federal regulations and requirements. Contracts began to ever increasingly dictate how far this relationship can go and it have physically alienated clients from these institutions to limit down the legal liability of banks. As bank contracts were to become ever increasingly complex and more difficult to navigate the more responsibility have fallen onto the client (Servon) to understand the terms of service, the free structure and other conditions, some of these conditions banks did not have to communicate towards the client and enabled some banks to restructure debits from accounts in a way that incurred an extortionate imposing of overdraft charges onto account balances. (Servon)

In Hungary, Erste Bank was the prime example of how Banks have lost contact with reality (Anon1) and no longer consider the human factor of reality in comparison to example cases in the United States. (Servon) When the crisis has hit in, Erste Bank has decided to immediately shut down or limit down the credit card line of account holders who had alterations in their employment. (Anon1) Those debtors who taken up Euro based loans were also hit with increased overall monthly installments that were difficult for them to finance. (Emese) This resulted in their accounts immediately being closed, later the bank has neglected to accept repayments of all outstanding loans from debtors who were attempting to keep repaying their debts. Instead they were continuously misled by Erste Bank representatives. It was revealed that they were only repaying their own credit card debts and no other loans, and late fees and interest piled up on their original outstanding Euro based debts. (Anon1) Later Erste Bank sold the outstanding loans of debtors while refusing to negotiate, restructure debts or consider other factors from debtors. (kasnykm) Instead it has decided to shut down repayment and sell the outstanding debts to debt collecting agencies like Intrum Justitia for a fraction of the total loan cost², (Portfolio.hu) who then proceeded to use questionable ethical and moral standards to pursue debtors. (kasnykm) Instead of offering option to have a reasonable timeframe and restructure debts. Erste Bank debtors in Hungary suddenly found that they are now forced to repay their original loan's double amount back to the new creditor, (Anon1) because a loan collector has imposed additional fines up to the original amount of outstanding total debt. This resulted in making the debt look like it is the original amount being repaid all over again. (Anon1; kasnykm) This for many has proven extremely difficult in Hungary and a wave of foreclosures has started threatening the lives of many families in the country. (Emese) While the Hungarian Government at that time attempted to give help for families, these protective nets were slowly removed and clients were forced out of their homes either way. (MTI; Márk)

This amount of low diligence exercise by banks to look out for the financial safety of clients seems to show that there is indeed no longer any informal moral relationship existing between client and bank. (Servon) This seems to correlate with the European examples also (Anon1; Servon). The problem had unwarranted consequences. Banks often abuse for their own gains by liberally using banking contracts to impose fines and other financial penalties onto consumers who have an exceedingly tough time paying, especially in the US. (Servon) Therefore, it is apparent that clients for banks no longer have any value as in sense of being a person, and instead what dictates decision makings are government by the hard-coded rules of the contracts that can make or break a relationship. This is one reason Bankers cannot fully communicate or

befriend clients, banking contracts must protect a bank from all forms of liabilities while attempting to conform with state regulations. (Servon)

The differences between European banks and US based banks are quite stark, there are more Europeans with bank accounts with access to services on the internet and mobile banking than Americans. (Servon) Un- or underbanked Americans do not have the luxury to purchase goods or access subscriptions on the internet. Therefore, other third-party service providers come in as a solution provider (like RiteCheck) to make it possible for those without a bank account or one with limited usability to be able to access services. (Servon)

As it is observed and concluded by Lisa Servon, banks do not respect us anymore and do not consider us as customers. (Servon) Instead, this have evolved into a relationship where a one bank competes with other banks to attract more customers and by that drive up their profit margin by misusing customers as just a number in the quarterly profit report. (Servon) More and more are looking for other alternatives that give them a much cheaper or even freer access to financial services, alternative financial institutions or so called Fintech companies are already attempting to provide solutions. (Servon) While banks are actively taking part in risky financial activities and these can't be audited by anyone. The results of the 2008 crisis have caused mass foreclosures and indebtedness, personal bankruptcy cases have also increased.^[3] (Servon) The main culprits of the Financial Collapse have not been charged and nobody was legally charged for their questionable financial activities. This raises the question that nobody has been sentenced, whether this has been made justified because many people have fallen victims of this crisis and since only at least one person was sentenced and fined in such manner. Certainly this decision is not going to deter others from doing such activities in the future. (Cohan; Deener) Since nobody was charged, there was no crime committed in essence, giving space again for financial irresponsibility in a world where banking secrets keep up a fragile system that Central Banks control. (Ammous)

Since Banking institutions cannot be audited by individuals, we cannot assure their safe operation and that the bank complies with US Federal Financial Regulations. Therefore, we are fully at their own discretion of how they are operating. (Ammous; Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System)

i. The Unbanking of America

Lisa Servon's *The Unbanking of America: How the New Middle Class Survives* has in essence failed to discover the root cause of the problem and only examined issues facing the American population from a problem-solving angle. On layman's terms it is more logical but nowhere near enough to solve the issues that the people of the United States face every day. Lisa Servon has failed to step outside of the box and examine truly alternative financial solutions that could potentially inhibit the negative effects caused by the legacy banking system. (Servon)

This is although not a failure of her research, it can only be attributed to the research methodology and Servon's approach to the problem that she was examining. When Servon selectively went to fintech organizations she has failed to realize that one of the companies were already using a type of blockchain

technology that was developed in house. Even with best of attempt to reach her for a comment via email there been no response, therefore it is not possible to know why she has not examined the predecessor technology as a potential solution. (Servon)

This unfortunately resulted in an incomplete conclusion in her book. The financial system's original problem rather denotes that she was skeptical of any separate solution because of its possible outlandish nature, non-state operated digital currencies in this to separate state and currency from each other and give back the power into the hands of the people via established social consensus throughout the free market. Her inability seeing this, is a very important factor that can be directly derived from the conclusion. (Servon)

But other than that, Servon have managed to shed light on the important daily issues Americans face every day. She has shown that banks now seem to be passively isolating and alienating customers from the banking system. She showed us how slow the system is to clear checks; how alternative financial companies are trying to speed up check clearances and how Rotating Credit and Savings Associations were giving lifelines for individuals and small family companies. She did so while exploring their inner workings and complex trust based structures. (Servon) When Servon examined how contracts at banks work, her discovery confirmed the hypothesis that these types of strict contracts make it impossible to build a relationship with low- and middle-income customers, since banks have to consider mitigating risks that their services bring. (Servon) She also found that the regular change of ownership of small branches further divide communities. When a bank changes hand it often changes its overall brand and makes its overall perception to others alien. If we have trusted a bank like Bank of America a few weeks ago, we might have a difficult time if Wells Fargo takes over our local branch's operation and completely replaces the staff working within that bank. (Servon)

Her work has proven that Check Cashing organizations are more human oriented and give much direct feedback to customers than Banks do. Check Cashers with their straightforward fee structures are much more understandable than complex banking contracts and fee structures that are often designed to force consumers to fall into fee traps. While these organizations might be called predatory, (due to their higher than average prices per transaction), similarly like as Payday Lenders in the US, it often the only available option that can provide lifeline for American consumers who have no other option left in a system that seems so much set against providing easy access to banking services. (Servon)

The finding in the book seem to suggest, that distrust towards banks has not increased, and shows that instead of generating distrust towards banks, consumers instead opt to change banks or go unbanked to avoid coming across the same problem again. (Servon) Consumers in this respect have one key mitigating tool in their arsenal, called choice. (Servon)

B. The Era of Post-Truth

Ever since the beginning of early days of modern journalism, the press was a prestigious institution, which had the most vital role in modern day democracies. The free press's role is to oversee our free

democracies and hold those in power to account for their actions. Without the free press, we would not be able to hold politicians accountable for the embezzlement of funds, or for their misuse of power.

As of today, the role of the free press is damaged, and people trust it less. (Edelman) With the advent of the social media, the speed of news accelerated, and it is now not just journalists who can break the news, but the ordinary people too. Let it be a protest against a corrupt government, disaster happening or police abusing their power, news now propagate much faster thanks to these new mass communication solutions.

Unfortunately, it is not just news that people share, but falsified stories that do not have any gram of truth behind them. Since the 2016 US Presidential Elections, we are living the era of the post-truth where information we consume is not pure, but instead it is actively manipulated by third parties that have different political ideologies at play and wish to influence our decision-making abilities, with that making their own choice of political candidates elected and their own discourse continued. This apparent interference with the quality and impartiality of the news seems to have damaged American's view of both the media and that of politics, since many now cannot get access to the information they require to make informed decisions. The information they now receive is now biased.

Donald J. Trump the 45th President of the United States now often calls out media outlets who he views as biased as Fake News, these outlets are often then have their operations restricted, their press passes removed and sanctioned, blocking their abilities to do their jobs. But although we must view these from the opposite side, because these news outlets are often biased towards President Donald Trump. The coverage of the Russia Probe has gained more a traction on left-leaning news outlets than those of right-leaning, while liberal news outlets mostly focused on critical views of Donald Trump have often subsided positive developments of the Presidency. Such as protection of autoworker and coal miner jobs, which was more favored by the President during his campaign, but liberals consider these less pressing than the protection of civil rights, minorities, free access to abortions and protection of different sexual orientations.

The news landscape in the United States is now very different than pre-2010, according to the Economist, there is now a greater ideological gap between Americans regarding their political views, about whether or not media outlets as biased, and what kind of actions they would take against outlets that are biased in their perspective. Left-leaning voters often favor not touching outlets but while Conservative leaning considers sanctioning or closing down outlets that are not impartial in content. (The Economist) Noam Chomsky argues that this is because of the ever-degrading quality of the news provided for Americans while other more controversial media outlets often provide views that Americans do not often have access to. Some of these outlets Chomsky have claimed were for example RT and SputnikNews, while he has distanced himself from outlets like CNN or the BBC. (Chomsky)

Similar events have developed in Hungary when Viktor Orban's childhood friend, Lorinc Meszaros, who was originally a plumber by profession, has begun purchasing media outlets in Hungary. When the State Media was transformed in Hungary, the new official guidance for the company was to be a political propaganda outlet that parroted the Hungarian Government's views and that of the FIDESZ-KDNP party. (SIXX)

In 2016, the Hungarian government used a shady Austrian company called as Vienna Capital Partners, who was the majority owner of Mediaworks, to shut down a left-leaning newspaper called Nepszabadsag, with this essentially beginning the war on the free press in the country. Nepszabadsag was a major newspaper that enjoyed favourable views of the Hungarian middle and lower classes. By having the company eliminated through this trickery, the Hungarian government has essentially cut the news source of hundreds of thousands of Hungarians. Overnight the media landscape of the country was changed, and the discourse has begun tilting towards that of the Hungarian Government's. (Sarkadi)

Hungary although is a different case because the country only had brief periods of time when it had its media free of political interference. Before the change of system in Hungary in 1989, the media was heavily censored by the ruling socialists who were abiding by the ideological standards of the USSR. The news back in those days were basically political propaganda, which attempted to portray the west as an evil to socialism. (Cull, Gatov and Pomerantsev)

This inherent culturally encoded inability of some Hungarians resulted in the careless consumption of news, especially among those who are uneducated and the elderly. The state media M1 TV offers hourly news and reports from Hungary on all kinds of issues, this repetition of information often feeds altered perceptions and views for Hungarians, especially during election times, that over time attempts to alter the perception of viewers of certain political messages and objectives that are important for the government. This repetition often reinforces the information over time and forms misconceptions in the minds of the viewers who will be more susceptible later to believe that the European Union is impeding on their country's democracy or that there are still migrants coming to Hungary who attempt to steal their jobs and bring crime with themselves. These concepts often create an artificial fear in people, especially the elderly, who will be terrorized by the prospects of migrants² invading their home country or their homes. (Halasz and Boros)

The effect of this news alienation has on educated viewers are even more stark. Educated consumers of news are able to filter out fake news and establish a reality check for news that do not conform to their reality. Often these people end up having to expose themselves to more news media outlets, especially on the internet, in order to make a better educated attempt of establishing the truth for themselves by comparing and contrasting headlines and content of information across news sites. This although does not make it easier to establish facts from multiple sources and instead re-confirms bias and makes the consumption of information much harder that further erodes people's trust in the news media. (Langlois)

Through the actual brainwashing of the people, governments can control them through carefully constructed messages that over time makes their views conform to that of the ruling party's (Magyar, Gulyas and Kovacs), just as similarly as how George Orwell's Nineteen Eighty-Four portrays a world where a totalitarian regime has taken over and are now actively manipulating the discourse and instilling fears into the minds of the people to force them to keep believing what they are saying, while all of that information is not true but that of a fabrication. The similarities between Hungary's example and that of Orwell's book is quite striking (Magyar, Gulyas and Kovacs), it is arguable that Hungary's totalitarian control of the news media was directly copied over from that of Russia's example. But so far, the

Hungarian example has avoided every type of bodily harm in contrast to that of the model set by Russia. (Magyari)

When teenagers from the Macedonian village of Veles started creating fake news sites, their main goal was to have a stream of income generated by advertising. These sites managed to gain attraction because they propagated partisan false news that conformed to the bias of the readers who were not just conservative leaning. Catchy, sensationalist headlines often served as a very good starting point for convincing consumers that the news have some value of truth while it only attempted to fool the readers. (Subramanian)

The sheer amount of fake news people consumed during the US Presidential Elections was staggering, and it has prompted Google and Facebook to actively curate news and ban sites from their search engines and to cut ad revenue for them. (Subramanian)

Troll Farms⁸ operated in Russia by the Russian Government also attempted to interfere in the electoral discourse. Their operation on Facebook attempted to create social conflict between both sides of the political spectrum just to intensify differences and enable the spread of false news to be more effective. Voters who saw messages that do not confirm to their political views were more than likely to be later susceptible to other fake news that have targeted their political views with over exaggerated messages with false content. Often this content was very politically biased or contained over exaggerated statements. (Lee)

Our demand for access to unbiased news is constantly eroding our trust in the news media. Whether we are conservative or liberal, the evil cycle of trust erosion in the institutions of the media is never ending. Attacks targeting journalists, as like how Viktor Orban or other members of the FIDESZ-KDNP party attack journalists by labelling them as organizations funded by George Soros or Lajos Simicska², they directly attack their image and portray these news outlets impartiality questionable for others, hinting that the news they are covering is funded by Soros and should not be trusted by anyone. (Beauchamp)

The problem this poses for us is quite immense, because without a properly functioning free press that is able to provide us with unbiased news, we cannot establish the factuality of the information provided and we cannot exercise our rights as citizens to oversee the correct operation of our democracies. Because of this in countries like Russia, people like Russian President Vladimir Putin can freely do whatever he wants without anyone in Russia rising an issue about his executive actions as President of the Federation. If it is even somehow reaching the public, the information can be put to rest by the careful control of the discourse that attempts to silence those who wish to raise a word about the possible corruption ongoing. If journalists in Russia keep attempting to investigate scandals, they can easily find themselves in hot water, have their news outlet bought up by a Russian Oligarch and later shut down, have the authorities make their lives impossible or have Strong-Man's paid to resort to physical harassments, attacks and even murder to silence their opponents. (Denber)

C. The Great Chasm of Political Polarization

Since the rise of illiberalism and populism across the western world we can see that we have already lost trust in our system. People are rebelling against present forms of politics and choosing candidates and solutions that seem to do more harm than good for them. But, if we look more closer at the problem, we will see these choices are logical and their choices are just as justified as anyone else's when they exercise their civil rights during elections.

According to Andreas M. Antonopoulos, (London Real) the wellbeing of a nation cannot be measured correctly with just one national index where we can claim that an economy is properly functioning and that its positive effects are benefiting the entire country. (London Real) In some countries, for example the United Kingdom or in Greece, there can be majority of people who are feeling discontent with their situation and that seems to counter certain national economic well-being statistics. (London Real) This is worthy of consideration because in this section we are going to look more closely at what has happened in the United States, Britain and in Hungary. We will then see how it reflects to the issues mentioned by Antonopoulos. If we consider that over 50% of Americans voted as a majority for an opposing candidate, can that election victory be then called satisfactory? (Abramson)

As America becomes ever increasingly divided among political ideological lines, it becomes more and more apparent that it can cause problems for members of the public, therefore we must investigate this, because there is too much dependent upon politicians' decisions that can affect our lives. (Pew Research Center)

i. The Legacy of Brexit

The 2016 Brexit Referendum have shown us that there is a clear disconnection between people and politics, the 51.89% of eligible British Voters have chosen to leave the European Union.

Rural British voters, the elderly and those who receive less support from the British Government, or the European Union were in overwhelmingly in favor of leaving the European Union. People who felt absolutely no effects of the EU's positive impacts saw absolutely no reason to remain member of it. Even business owners who were exporting into the EU had chosen to leave, not considering the possible downsides for their own business interest, but instead have placed their own self and their country's interest beforehand. (Oliver)

The fact that a generation gap began tearing the country apart is apparent because younger voters were overwhelmingly in favor of having the UK remain member of the EU. Younger people often can see the freedom within the European Union because of their interconnectivity and ability to communicate with others cross borders. Their perception of the EU was more in some sense influenced by these freedoms, the freedoms they wanted to keep with their choice to remain. (Shuster)

The Brexit Referendum's result can be attributed to the failure of the UK Government and that of the European Union that they were unable to improve the lives of ordinary British people in any meaningful way. The ever-increasing cost of living put further strain on people and the overwhelmed National Health Service made it difficult to have timely access to healthcare services. (Barr; Yeginsu) A mass influx of foreigners into the country also has accelerated resentment towards the European project. Some have

perceived that the EU Parliament is directly interfering in their sovereign country's internal processes by legislating laws that they have not agreed to beforehand, claiming that these laws are made by Bureaucrats in Brussels who they did not elect. In a sense this is a possible reason because the remoteness and quasi isolated feel of the workings of the European Parliament make it not so obvious that although they have actually elected members who the British people have chosen, those people are able to veto or reject legislation passed by the EU Parliament. (Nardelli; Arnott)

Since there is obviously just a marginal support for Brexit as of right now with a total of 3.78% margin, we cannot call the outcome of this vote a decisive decision. Instead what it has done is split communities, alienate family members and cause more than 3 years of bickering over how the United Kingdom will leave the European Union. (Dimpleby and Mooney) Prime Minister Theresa May in June has declared that she is resigning because she has essentially failed to bring about the decision of the British people who voted for Brexit. Multiple of her attempts were rejected by the members of the British parliament. Her Chequers Plan did not pass and caused a longer stalemate that required the extension of Brexit until the end of October 2019. (Stewart)

This has caused many Brexit supporters and conservative voters to criticize her inability, these people now feel betrayed like their 2016 Brexit vote was meaningless. (Jones)

Although the vote was non-binding, the Government could always decide to back out of leaving the EU, but with that they risk further alienating more people from politics and could for ever leave a dent on the public's perception of the British democratic process. As of right now, it seems that the UK is on a path towards a catastrophic no deal Brexit that will cause mass disruptions across the UK. There is a potential for food shortages, loss of jobs, higher prices for goods and a shortage of medicine. (Oliver) Such problems in a high advanced western democracy are shocking and has never seen and arguably appear like it was a decision of self-harm. (Hutton) The next Prime Minister Boris Johnson have staunchly stood next to his support of a hard line exit out of the European Union which caused further conflict within halls of Parliament. (Mason and Walker)

The legitimacy of the decision was also called into question because of how Vote Leave has breached UK Campaign Finance laws by overspending on their campaign through other unaffiliated leave leaning campaign groups. Their connection to a political consulting firm called Cambridge Analytica was also called into question due to their shady tactics of how they data mined user's data for behavioral analysis of their potential voting choice. Vote Leave also have overexaggerated claims related to the financing of the NHS claiming that they will be able to contribute 350 million pounds a week to it, but later Nigel Farage in an interview have called the claims unfounded and impossible to meet, essentially saying that they have lied to the British people. (McCann and Morgan)

If the United Kingdom manages to crash out without a deal from the European Union, the consequences of that will be far reaching and its damage potentially impossible to repair. The possibility of withdrawing of Article 50 and nullification of the Brexit vote can also come with such an effect. Both choices will alienate people to a great extent, but the greater damaging possibility can solely be found in a No Deal Brexit scenario. There is a great potential for both sides drifting apart further ideologically, creating fringes in both groups. The disillusionment of the unmet promises and the hardships that will follow

hides a very dangerous development. Remain voters will not be able to trust the government and will further drift towards the left potentially and reject all forms of cooperation with conservatives in the future. While leave voters would be disappointed with the outcome, they would also not feel comfortable with the shortages and the way Brexit was handled, essentially damaging the Conservative Party further. With this potentially giving space for far right leaning political parties to enter the British Parliament that would even further erode trust in British society and create social conflict across ideologies. We can see that then it would be impossible to reach consensus unless both political parties are eliminated from the parliament and new ones are given the chance to attempt something new.

This is an evil cycle that is unending until the results of the Brexit Referendum are enforced.

ii. Fallout of the 2016 US Presidential Elections

The Revelations of the 2016 US Presidential Elections can be also felt globally, the shock election of Donald J. Trump as the 45th President of the United States has caused political disillusion across the globe. People who thought that a candidate such as Donald Trump would stand absolutely no chance in winning the race were spectacularly disproven when he defeated the contender Hillary Clinton. Donald Trump has won the election with the race with just over 62 million votes of Americans, it was 46.1% of total votes, while Hillary Clinton has won the popular vote with 48.2%, a 2.1% difference, but because of how the Electoral College works in the United States, more areas have voted for Donald Trump. Often Americans cite an electoral college map of the United States as a proof that Donald Trump's support was more widespread, but less people decided about the vote, it was the minority's choice that he was elected.

Some would argue this is a catastrophe that should have never happen, but this is not problem, because it has shown that there are many Americans who are disconnected from the policies of the previous president Barack Obama. This election basically proven that Barack Obama did little to appease republican leaning voters during his presidency, and in most cases has caused problems for them with the accelerated closure of coal factories. (Achenbach and Clement)

Alienated republicans who lost faith in the system resisted other republicans who were more mainstream and instead elected to have Donald Trump due to his completely clean and inexperienced history. He run on a platform to make America great again for the average Americans who are struggling, championing himself as the President of the People.

This although came at a cost and was not fully accepted by democrat voters. Speculations have begun spreading that President Donald Trump or his campaign staff could have possibly colluded with foreign actors. Accusations of vote rigging have become the norm after the election and months later, after the firing of James Comey the head of the FBI, an investigation was started to investigate the possible obstruction of justice and connection between the Trump Campaign staff members and potential Russian foreign agents. (Yglesias)

News outlets daily were repeating bombshell reports that they claimed have proven that Donald Trump was installed by the Russian government or Vladimir Putin, but so far this has not been proven without a reasonable doubt. (McKay) The outside interference of foreign actors was also possible during the election.

Foreign actors from places like Macedonia were running fake news sites that were relying on advertising revenue collected when people visited these websites. (Subramanian) These sites often contained news that had sensationalist headlines that smeared the democratic contender Hillary Clinton with misleading information that targeted Republican voters. A possibility of a Russian Troll Farm operated by the Russian Government was also scrutinized since their operation on Facebook showed that they were targeting Americans with biased news that attempted to influence their vote's outcome. (Myers and Evstatieva) Facebook cited that over 100 million Americans saw the advertisements on their personal timeline on Facebook and it could have had a detrimental effect on the election's outcome, although Facebook's Founder and CEO Mark Zuckerberg have denied the possibility of such. (Weise)

Also, possible connections were found between members of the Trump Campaign and the British political consultancy firm called Cambridge Analytica. (Wagner) Cambridge Analytica have exploited Facebook by running surveys that had pervasive access to user's data, which was far reaching, allowing them to see into the political leaning of hundreds of millions of Americans, with that essentially having the ability to build a complex political ideology map with which they could have targeted voters much more easily. (Chang) Later the company had whistleblowers claiming that they are doing very pervasive policy influencing abroad. An Australian news channel went undercover posing as an African Country's representative that wanted to influence its voter's thinking and alter the results of an election. (Prokop) The company was closed down and the investigation into it is still ongoing by the Metropolitan Police in the United Kingdom. (The Guardian)

We can clearly see how such a controversy can affect people in the United States. According to *Pew Research Center*, in 2014 we have reached the largest gap of political ideology between the Liberals and Conservatives among politically engaged, before 2008, this gap was non-existent, and policy often overlap with the interest of both Conservatives and Liberals. Today, this gap has seemingly increased, and polarization is much more apparent. (Pew Research Center; Edelman)

The progressive policies of Barack Obama have failed to improve the lives of rural Americans while it did improve the state of civil rights and liberties they were enjoying, especially in relation to LGBTQ+ rights¹⁰. Americans are still largely divided on critical policies such as Gun Rights, Environmental Protection and Abortions. (Bialik)

The divide between Americans across the two spectrums seem to be just growing unending, reaching common ground between Democrats and Republican so far seems to be very difficult and often cause stalemates in the halls of Congress. (Caldwell)

This kind of disillusion with the system and government is slowly turning Americans towards more radical ideologies, such as the Alt-Right, and the Anti-Fascist movements that seem to polarize America today. Both sides seem extremely intolerant and unable to agree on anything. (Saphiro)

Ever since 2010 there has been a dramatic rise in numbers of Libertarian Voters, as social policy ever increasingly started to go towards liberalization of rights and freedoms for individuals. Their solutions seem ever increasingly more reachable and their views more favorable than the currently mainstream parties in Congress. Other than the American Green Party, the Libertarian agenda seems to be able to

provide actual solutions for problems that Americans face today. Ranging from streamlining the complex bureaucracy and limiting the reach of government while giving back the freedoms to all Americans that the Founding Fathers meant to give to them with the given protections grounded in the Bill of Rights and in the 1st and 2nd Amendments. (Rosenberg)

Democrats on the other end do not feel content with the policies enacted by the Trump Administration. They perceive their approach to policy as conducive towards their freedoms. Especially towards Abortions, with the installment of the new Supreme Court Judge Brett Kavanaugh who could change the tide on a possible re-examination of the 1973 Roe vs Wade decision that granted the option for woman for abortions. The overturning of this decision could mean a much more restricted access for woman to seek reproductive healthcare and access to abortions in the United States. Most democrats do not want such a thing to happen and vehemently oppose such changes that impede on the rights of woman.

Barack Obama multiple times attempted to introduce legislation to control the sales of weapons in the US to little success. The Second Amendment of the United States clearly states that the rights of American Citizens should not be infringed upon and access to weaponry should be a right granted by Citizenship. Since as it is declared in the Second Amendment, the presence of a well-trained irregular militia is required to protect the freedoms of Americans even if that comes at great price. Most democrats on the other hand would gladly restrict the sales of guns and introduce in legislation requiring mandatory background checks and registration of gun ownership. This is entirely unacceptable for most Republican and Libertarian voters and also seem to be splitting some democrat leaning voters. (McCammond)

Democratic presidential candidate Beto O'Rourke has suggested that he would go as far as using lethal force to take away AR-15s and AK-47s from law abiding Americans. On Twitter, his message has been immediately denounced as an actual threat to kill people who refuses to surrender their weapons. (Stockler) A US State Representative Briscoe Cain tweeted a play of words where he has said that his weapon is ready for O'Rourke which was immediately perceived by O'Rourke as a direct threat against his life. (CNN Politics) Although, gun control is not solely a subject targeted by democrats, often republicans also alter laws that introduce in new regulations that make it more difficult to access weapons, for example the banning of bump stocks were signed into law by President Donald Trump himself which was initiated by him after a mass shooting at a concert in Las Vegas. Gun Hobbyists supporters of the Second Amendment were quick to also denounce Beto's threats and called for the increased use of 3D Printed weapons to prevent the Federal Government or the Police from confiscating weapons.

Gun hobbyists argue that new 3D printed weapons can counter the government overreach of power and protect them from illegal interferences targeting their Second Amendment rights. (Li and Lifthrasir, 2: Behind Enemy Lines - A.G. Leaks; Li and Lifthrasir, 5: Come and Print It - Ivan The Troll)

It appears to be that the spread of 3D printed weapons is a direct effect of politicians impediment upon the Second Amendment rights of US Citizens. (Li and Lifthrasir, 5: Come and Print It - Ivan The Troll) The spread of 3D Printing technology and its easy access have prompted some to invent new forms of weapons and improve upon older types, with extremely overwhelming results. Ranging from the original plastic Liberator to 3D Printed Glock lower-receivers (Biggs), partially plastic submachine guns like the FGC9 (FuggGunControl, Fuck Gun Control 9 Carbine; Deterrence Dispensed), the Plastikov type AK-47 receiver

(FuggGunControl, Plastikov 3D Printed AK Receiver) and sci-fi-like shotguns with rotating loading mechanisms that function similarly to Revolvers called as the Liberator12k ZZ6-12. (BigTanGringo)

The spread of 3D printed weapons seems right now inevitable that seek to restore individual freedom and one's ability to protect themselves and their property. These are easily accessible files that can be downloaded from the internet from censorship resistant applications like Keybase, which is a PGP key storage service with encrypted chat functionalities is built in. Services like Keybase make it extremely difficult for governments to censor these activities of private citizens who seek weapon schematics and files to print weapons in the privacy of their home. (Li and Lifthrasir, 7: BitcoinGun Lawyer Part I; Li and Lifthrasir, 2: Behind Enemy Lines - A.G. Leaks)

At this point we must ask the question, how long is it possible to play a cat and mouse game where political parties replace one another repeatedly, where they impede upon the rights of others, and seek to restrict our freedom? How long is it possible to continue this cycle without having political parties losing their legitimacy completely?

We cannot eliminate the possibility that this problem can cause a cyclical loss of trust and increase of distrust. Which in fact would make it harder to make proper decisions. People will become reluctant if their options are limited. Therefore, chances that, they will even avoid taking part in the voting process all together by abstaining on all candidates.

iii. Hungary's Illiberalism

Ever since the 2010 Hungarian Parliamentary Elections, Prime Minister Viktor Orban lead FIDESZ-KDNP coalition has uninterruptedly served as Hungary's Government. When millions of Hungarians voted for the coalition party, they were mostly driven by resentment and distrust towards the Hungarian Socialist Party MSZP and were also desperate for a change after the 2008 Global Financial Crisis as Hungary's total national debt kept growing.

At this time, the FIDESZ party, in coalition with the Christian Democratic People's Party, was more centrist in political orientation and appealed to many young voters and old alike. Only after the beginning of the European Migration Crisis could we clearly see the direct effects of how the governing party was slowly transitioning towards the far right. Voters who were staunch supporters of the government suddenly found themselves alienated from their party because of their new, more nationalist agenda that did not suit their ideology.

During the Migration Crisis, the Government of Hungary resorted to mass media campaigns and advertisements targeting Hungarians with messages drumming up fears of incoming Migrants who were on their way to Hungary. Displaying large white texts on blue background saying: "If you come to Hungary, you cannot take the Hungarian's jobs!" or "If you come to Hungary, you must respect our Culture."

The question was quickly raised why these messages were in Hungarian. For it clearly did not target mostly Arabic speaking migrants arriving into Hungary. These messages were the beginning of a targeted

and systematic advertisement campaign that attempted to drive the public discourse and instill fear into the minds of the Hungarian people.

Years later, these campaigns kept going on and broadening their assault with the establishment of the State Media outlet as the loudspeaker of the government that parroted its political ideology to viewers. George Soros, the billionaire speculator was also chosen as a scapegoat to blame him for the influx of migrants, as the person of interest who wants to dilute Europe with the hordes of Muslims. A similar demagoguery can be found in Turkey also with connection to Fethullah Gulen who is a Turkish Islamic Scholar currently in exile in the United States, he is also used similarly as a scapegoat by Turkish President Recep Tayyip Erdogan.

The closure of Nepszabadsag has also eroded press freedom in Hungary and limited down opposition voices so much in Hungary that the US Department of Foreign Affairs introduced a grant for any company in Hungary that was willing to create a news outlet that ran independent news outlets not connected with the Government or its views.

Since most of the Hungarian news outlets are now owned by Hungarian oligarchs it is very difficult for independent outlets to properly operate. The recent acquisition of HirTV by Lorinc Meszaros affiliated news channel Echo TV further limited people's options to consume unbiased news.

The oligarchy system which Viktor Orban has built out in Hungary clearly shows that they are actively attempting to manage the discourse of Hungarians with actively managed propaganda and coordinated news releases through outlets owned by allies of the governing party. Friends of Viktor Orban own many hotels, bars, nightclubs and other businesses around tourist destinations and around Lake Balaton that keep generating them immense profits.

The misuse of EU funding is also a huge issue, the recent ELIOS Scandal in Hungary shed light onto how family members of Viktor Orban was able to embezzle EU funds while providing inferior public lighting option for cities. The EU watchdog for fund embezzlement OLAF has already made its recommendation for legal pursuit against the possible fraud committed by them, but nobody so far has been fined or imprisoned for their illegal activities.

Hungary's fixation on improving the national sports facilities, like Stadiums, has also drawn the ire of Hungarians because of how much the Hungarian Health Service is neglected. Hospitals cannot afford soap in restrooms, neither the ability to maintain proper hygiene in them, which resulted in the rise of dangerous anti-biotic resistant MRSA cases. These rising MRSA cases are often denied outright by the government in order to prevent a potential panic from occurring within hospitals. Doctors in Hungary don't receive proper wages and many of them leave Hungary to work abroad for a much higher wage. (Lenard)

The Education system in Hungary is also crumbling, teachers are not provided the necessary wages and schools and kindergartens are severely underfunded. This underfunding although made some places in Hungary offer almost German or Dutch minimal wage level offerings for certain kindergarten teachers, desperations often leads them to offer even those applicants who lack training just to immediately fill these vacant positions.

The neglect that the Hungarian government shows towards these areas are astonishing and is actively upsetting Hungarians.

The recent 2018 Hungarian Parliamentary Election shows that Hungary's opposition was successfully fragmented by the governing party. The way Hungary's electorate is set up made it impossible for smaller parties to gain seats in the Parliament and their fragmentation made it possible for a minority choice to take seats. Although the opposition has a higher number of supporters combined, their inability shows that they are unable to cooperate, even on the removal of the currently ruling government.

More people have voted for the opposition parties than for the currently ruling FIDESZ-KDNP party, but they still have managed to achieve more than two third majority in Parliament because of how the Hungarian Election System is designed.

This shows us that Viktor Orban's plan to fragment the opposition has so far been successful. His targeted attacks alienated voters from smaller parties while labelling their leaders as agents of George Soros or supporters of illegal migration.

Hungary is in essence polarized, but the recent 2019 European Parliamentary Election seems to hint that there are now new parties emerging that could have a fighting chance at replacing the currently ruling government.

Hungarians have a really hard time trusting political parties, since right now the last two governments that were serving both were corrupt and this does not increase the confidence of the public easily in other political parties. As the Hungarian public's trust is now ever increasingly looking fragmented, a possible consensus seems difficult to achieve. Smaller parties like the Momentum Party will have a very difficult time convincing voters that their political agenda can be trusted. Essentially this shows that the Government's goal has succeeded and managed to permanently divide Hungary into small fragmented politically incompatible ideologies that cannot agree with each other in any way. Exceptions do apply in the case of the new Major of Hodmezovasarhely, Peter Marky-Zay, where the opposition was able to work together before the parliamentary elections. However, it did not translate into a global movement for the parties to unite together during the general election.

Research done by the Hungarian Scientific Academy seems to show that members of the ruling government began using Newspeak. (Magyar, Gulyas and Kovacs) The use of Newspeak by members of the Hungarian Government shows very high possibility for preparatory attempts for a potential change of support towards the European Union after the EU funding for projects in Hungary cease to happen. This could potentially mean that words used by members of the government could correlate with targeted ideological influencing attempts that try to prepare Hungarians for a potential exit from the European Union if it does not serve the interest of Viktor Orban or the FIDESZ-KDNP government. (Magyar, Gulyas and Kovacs)

If Hungarians fail to act in the upcoming years, it is apparent that there will be challenging times ahead that could be detrimental for their economic and political wellbeing for the foreseeable future.

As we have finished up this section, we now can see that there are complex issues present within society, ranging from the unbanking of individuals to the political polarization we experience today. These are just the symptoms of a disease that took hold over us for just over 100 years. Now, in the next chapter we will get to understand the virus that causes this severe disease, which in return, creates these problems we that we just discussed.

D. Monetary Nationalism

Ever since the start of the 20th century, some researchers have been arguing that there is a currently ongoing slowdown of technological development. (Huebner; Adler) Since the end of the 19th century, speed at what technological innovation was evolving began to decline dramatically. (Huebner) According to Jonathan Huebner, new innovations right now only focus on improving already existing technologies and do not seek to introduce in new ones. (Huebner)

This declining trend seems to show that there is a global decline towards true innovation and a move towards profit maximalization have occurred. (Huebner) The world as of today faces a global anti-biotics crisis with the spread of anti-biotics resistant bacteria. (U.S. Food and Drug Administration) Large pharmaceutical companies now only focus on other medicines that give them a constant stream of income. Medications that many people take are often prescribed on a regular basis for longer periods of time, this way generating income for pharmaceutical companies. (Pollack) But on the contrary, their problem with anti-biotics is that these medications are only used once for a limited time and does not provide a profitable venture for them. Thus, research and development towards these important medications are exceptionally low and we see very few new anti-biotics that can fight resistant bacteria that evolved and mutated throughout the decades. (European Center for Disease Prevention and Control)

The declining innovation trend seems to point at the fact that humans right now prefer instant gratification and profit seeking to drive innovation. It is no longer in the pursuit of new technologies or things that make life better, but instead just new improved inventions of older technologies. (Huebner) The microchip manufacturing also relies on these factors. The two competing microchip makers, Intel and AMD, are in essence creating improved technologies that improve upon their already existing architectures, this is purely is based on the demand of the computer industry. Long gone the times when new, innovative technologies were created for non-existent markets that do not utilize such technologies. (Huebner)

If Huebner's research and modelling is correct, something has happened during and after the turn of the century, which we must look more closely at to better understand the potential innovation halt that the future holds for us. (Huebner; Adler)

Huebner's findings can also be correlated to another surprising factor, starting from the early 90s, namely the declining rates of births in developed nations, especially in Japan, Hungary and other European countries. (Kyodo)

The economical standards and theories of John Maynard Keynes seem to be one of the key players in this problem for us. (Ammous) As argued by the followers of the Austrian School of Economics, and its notable

followers like Ludwig von Mises, Friedrich A. Hayek, Murray Rothbard, the effects of Monetary Nationalism can be solely blamed. (Ammous)

The effect that can be mostly linked to our problem is the debasement of currency, as part of monetary nationalism¹¹. (Ammous) This is not a new phenomenon. Throughout the millennia there were multiple cases of such debasements (E.g.: The debasement of the Roman Denarius), that resulted in the destabilization of civilized society. (Ammous)

As it has become necessary for society to transact with currency throughout history, new forms of money appeared that people used to transact or keep records of their property. From the early Yap stones to beads, people encountered multiple challenges by others who wanted to gain financial superiority over one another to expand their own interests across lands and civilization. Yap Lands saw a sudden change in their society thanks to the newly mined Yap Stones that quickly devalued their stone currency, and African societies fell under the dominance of Europeans who had easy access to the creation of glass beads with which they purchased land and property from them. (Ammous; Szabo, Shelling Out - The Origins of Money)

Similarly, the Roman Empire also attempted to exert control of their empire through the debasement of the Denarius. It saw its value crash over three consecutive leadership changes that had different monetary policies which favored the minting of more coins through the decreasing of silver present in the coins and introduction of other metals to dilute it. (Ammous) While there were scarcity in terms of coins and had a high silver content, it had relatively high value. At that time prosperity was observed in the Roman Empire. But when the currency was debased and it lost its value, the collapse was inevitable and those who were enjoying a lifestyle in the cities were no longer able to sustain themselves. (Ammous)

Later with the spread of gold coins, empires and trade have flourished. (Ammous) Doing trade with gold coins were easy because the coins usually had different amount of gold present in them and that served as the basis of an exchange rate for traders. (Ammous) In China though, with the introduction of paper money, this was not so easy because at those times western traders were unable to exchange Chinese paper money back at home to gold because nobody was using them, and these paper notes had no value back in Europe. (Ammous) The over printing of paper fiat currency has already been noted by researchers and its consequences are well documented. (Glahn) As other countries started pursuing the printing of paper money, which at that time were backed by gold, the exchange of foreign currency was similarly easy. (Ammous)

During World War I, the Christmas Truce of 1914 showed that wars, with the debasement of currency and without politically charged ideology, appear to make no sense for soldiers. It has miraculously resulted in a truce where soldiers from both warring sides came together to celebrate Christmas for a few days. (Ammous) This has shown that the only fuel behind this war was funding of it by opposing sides. After the First World War, the Austro-Hungarian Empire's gold backed currency has collapsed due to the limitless printing of money that was required to fund the war. This resulted in the total loss of value of the currency used by the Austro-Hungarian Empire. (Ammous) The Weimar Republic after the war has also resorted to the debasement of the Mark, its currency, in order to repay the mounting reparation debt, it had to pay for allied nations as a punishment. Since the Mark was no longer covered by a gold standard, a

hyperinflationary effect has resulted due to the mass printing of fiat currency. Later, with the crash of the Dow Jones Industrial Average the great depression has created further dissent which directly allowed the rise of Adolf Hitler into power. (Ammous) Those who were seeking a way out of the hyperinflationary crisis and the great depression have resorted to nationalistic views quickly and this made it possible to make the views of Adolf Hitler more accessible to the masses by putting blame onto others for the problems that were experienced by Germans during these crises. (Ammous)

Similar effects can be observed in today's modern times, in relation to the Greek Debt Crisis which resulted in far-right elements becoming mainstream like the Golden Dawn movement that seeks to solve the problem through a more nationalist political agenda. (Strickland)

When Franklin D. Roosevelt signed Executive Order 6102, he directly attempted to impede upon the monetary wealth of Americans by attempting to control the flow of money and giving access for the US for more gold to hold on reserves. (Ammous) Gold was confiscated from private individuals through the use of force. That year June, the United States has went off the Gold Standard and the US Dollar was no longer backed by Gold. (Ammous) Other countries like Hungary has also followed suit and has left the Gold Standard due to the hyperinflation of the Hungarian Pengo, which was the largest ever hyperinflation that happened in human history. (Bomberger and Makinen) In 1944, the United States used the Breton Woods Conference after World War II to bring about a control of gold reserves around the world, by creating a gold reserve agreement that allowed signatory countries to exchange the US dollar notes they held in reserves into actual gold. (Ammous) In 1971, President Nixon noted that he could exert more power into the hands of the US if he removed the gold exchange program completely. On the 15th of August 1971, President Nixon, has officially ended the exchange program and forced countries to use the US dollar instead as a reserve currency without the ability to exchange them to gold. In 1976, the dollar's description was officially changed and the words claiming it to being backed by gold were removed and were turned into notes of the US Federal Reserve Bank, creating a pure fiat currency out of the US Dollar. (Ammous)

Examining the effects that the debasement of the US dollar has created, we can observe that from 1921, till today 2019, the US dollar has lost more than 90% of its given face value, essentially losing most of its value that it had in the past. The sharp contrast between how much 1 dollar was able to get for one person back in 1921, and its value today, makes the loss of value of the dollar very apparent. (Prentice and Clown) When a currency loses 90% of its total value over a period of almost 100 years, we can clearly see that it could pose potential harm to its users, and also to those who actively hold dollars in reserves. (Ammous)

The global abandonment of the gold standard also led to the proliferation of national currency exchange rates that fluctuate every day based on the traded and speculated value of a currency. This makes it much harder for businesses to do trade abroad where the exchange of currency often serves as a barrier of trade and commerce. (Ammous)

When such systematic debasement of currency happens, we must ask the question whether this is intentional. Most users of national currencies do not seem to understand what is the basis of money that they hold and mostly rely on their own interpretation of what is the value of the money that they use. Also, in academic circles it is difficult to find people who understand how fiat currencies function,

because of the well spread ideologies of Keynesian Economics. (Ammous) Keynes's focus on aggregate spending and avoidance of savings seem to have caused a long-term effect on society, which made it possible that individuals can no longer clearly understand the meaning of money that governments today print out in abundance at little to no added cost. (Ammous)

John Maynard Keynes multiple times stated that savings are dangerous (Ammous) and often cause economic instabilities, and that increasing spending creates future prosperity. (Ammous) To some it might seem like normality, since universities around the world religiously teach these views as part of the curriculum (Ammous) and rely on them as the basis of economics. (Ammous) But if we take a closer look, we can find evidence that Keynes had very little economics knowledge and experience before he began spreading his views on economics (Ammous). Saifedean Ammous states that, Keynes had inadequate understanding of how market economies work. (Ammous)

If we look at the claims present in the book by Saifedean Ammous, *The Bitcoin Standard*, we can see that there are obvious correlations between the behavior of John Maynard Keynes and his spending habits. (Ammous) For example, it is due to his way of acquiring wealth by the means of inheritance that he has begun spending. For a person so short sighted like Keynes (Ammous) it might look that he is creating a prosperous future for himself by spending his wealth right now, but it is on the contrary. His view that current spending accelerates market development seemed to have a rather negative effect on himself. It has gone beyond that because it has effectively created a spending drive that requires central banks to continue spending and creating money to keep the GDP high and climbing, while indebting themselves relentlessly. (Ammous)

Keynes's example clearly shows a generational divide as it is described by Francis Fukuyama. Since Keynes was not the person who earned his own wealth, he felt entitled to spend it, not understanding that there were others before him in the family who had to work hard to make that wealth happen and remain stable down for multiple generations. Just as Chinese families today struggle with this problem, generations later when family members lose interest in their parent's businesses and begin searching for alternative opportunities. (Fukuyama)

Keynes on multiple occasions cited the book which he essentially popularized in mainstream economics, written by John M. Robertson, titled *Fallacy of Savings*. Robertson clearly claimed that total savings in population would lead to declining trends of demand and output and much lower savings. But this is illogical in market economies because the lack of savings and increased debt based aggregate spending seem to lead to economic bubbles that rob wealth away from the individuals. (Ammous; Prentice and Clown)

The effect of Keynesian economics and Monetary Nationalism is a very deep issue. (Ammous; Davidson and Rees-Mogg; Hayek, *The Road to Serfdom*; Rothbard) The first effect we can see from the debasement of currency is that fiat money loses value over time and makes savings impossible due to inflation created by central banks that effectively steal value away and hand it over to the government or to the first spender of the currency. When gold is mined out, it is not the person speculating on the value of gold who gains value, but the entity that mines out the gold and sells it first hand to a buyer. Afterwards the buyer won't be able to sell it again for the same price but much less, effectively making gold work like a pyramid

scheme. The more we are selling from the asset in a given market the less value it will hold for others after our sale fulfilled. Similar effect plays off when Central Banks print out fiat money, with little added cost. (Ammous)

This type of devaluation of currency makes it difficult for people to hold and save money over time because it enforces a mental requirement to spend the fiat money in order to gain instant gratification. (Ammous) If an individual for example in the United States decided to save money from 1930 until 2015, the value of the savings would have decreased if no additional amount was added to the savings. This proves that fiat currencies are terrible store of value. (Prentice and Clown; Ammous) The aggregated spending theory also enforces spending, similarly, by making governments borrow money from central banks and spending that money. Funding public services, education, healthcare, infrastructure projects and militaries. Governments literally print out free money and hand it out as if it has any form of value, while enforcing that currency's purchasing power using military might and violence. (Ammous)

Essentially, the fiat currencies governments print out today are not backed by anything. Individuals are often ignorant about such facts and claim that paper money is backed by monetary metals which is not true but instead just Central Banks hold monetary metals as reserves and that paper money essentially wields no value due to that. (Ammous) Value is only later added when value producing humans attribute the fiat currency with value through their own work. This association process is enforced by government's action because a government uses its military might and violence to enforce the usage of a currency, and because of that when humans work for wages, they associated the created value with the paper notes, attributing value to the piece of paper that is not backed by anything but its usage enforced by the state through violence. This is what gives paper money value, and that is what governments impede upon by printing more to dilute the monetary base. The value someone produces today by working is essentially robbed away through theft committed by central banks and governments throughout the manipulation of the monetary supply. (Ammous)

This type of theft through inflation allowed the Astro-Hungarian and the German Empire to wage limitless war during World War I. Before the debasement of currency was an actively practiced solution for Kings and later for Governments, Kings had set out taxes to fund wars or other projects and the main solution was not often that they would just debase their currency to gain more money. Other governments also resorted to the use of inflation to finance their war efforts during World War I and World War II and beyond. The debasement of currency became the de-facto standard of war where printed out money served as the fuel of senseless wars waged by political opponents and authoritative imperialists. (Ammous)

i. The Disruption of the Global Time Preference

As the debasement of currency has begun, a complex sociological change has gone down within society. This effect was the permanent change in time preference¹², independent of the cultural code. (Ammous) Due to the fact that money today, for a large majority of humans on Earth is an indispensable part of daily

life. Only few isolated ethnic communities exist today that do not rely on money and still barter daily. (Ammous)

When time preference rises, the need for immediate gratification increases. This effect comes hand in hand with fiat currencies inflationary property, which in fact created by central banking monetary policy. (Ammous)

When there is a lack of savings within a population (World Bank), we can see that there are declining rates of marriages and births. (Kyodo) The lack of savings makes it difficult to foresee the future and commit one's self towards a marriage and if the situation is not acceptable neither will it be possible for someone to raise a child. (Ammous) This today seems to become a standard behavior within society among those who cannot sustain themselves properly and will not take risks in life like going into a marriage or having a child. (Ammous) Of course, this can be different based on a person's actual financial situation, because high time preference effects might not be so visible with individuals who live well above the average. If someone can afford to sustain themselves, then there are higher chances that the available wealth will allow that individual to form a family and raise a child. If there is a sound basis for prosperity that one has created for themselves, then these will not be often visible in this sense. While others who do not have access to banking systems and live well under the average, will often resort to loans and overspending. (Ammous)

When individuals resort to loans, they are not spending their money but rather spending money from their own future self to fulfill an immediate demand for a service or product that require immediate expenditure. (Ammous) When individuals attempted to overspend before the 2008 Financial Crisis, they quickly found that upon the effects of the crisis their personal finances were easily compromised by a change in work status, a demotion, or a loss of employment. (Anon1; Servon; Ammous)

Banks have quickly reacted to this situation by downgrading credit status, restructuring debts, and re-classifying them as defaulted because of change in the individuals' financial circumstance. This alone has led Erste Bank Zrt. to cancel the loans of thousands of people in Hungary, by that jeopardizing their economic and emotional/mental wellbeing. The effect although is more shocking if we manage to understand why it has happened in the first place, since it could have been avoidable on the side of the bank, but they still have decided to go with another solution, which resulted in the default of thousands of debtors. (Anon1)

Banks as of today do not consider human beings based on their personal situation, especially in the United States, but instead solely rely on numbers calculated by computers. These algorithms then decide whether an individual is eligible for a loan or other type of financial instrument. (Servon)

This fact does not directly mean that Banks are evil, or that the bank teller we meet sometimes is trying to exploit our financial situation. (Servon) Rather, the operation of a bank, as a company, was changed on the basis of human time preference enforced by those who invest into the financial institution. (Ammous) If we are investing into stocks, for example, we do so because we expect the stocks to gain value over time based on the performance of the company. Shareholders then expect banks to release quarterly, monthly, or even yearly reports of their financial situation and development. If we are holding stocks that allow us

to exercise a vote, and one that even pays us dividends, then we are inclined towards enforcing a for-profit attitude onto the company. This can be done by changing the executive officer of a company through voting, for example.

When a company's wellbeing is measured just in numbers and economic output, there tends to be a trend of profit maximization. (Ammous; Servon) After the banking regulations in the United States were changed, Investment and Residential Banking institution were able to merge. (Servon) It has caused the lowering of total interest rates on deposits and the start of riskier banking behavior that directly resulted in the 2008 Global Financial Crisis. (Servon)

The fact that profits are so important for these institutions is inherent, because of capitalism, which is not necessarily negative effect. However, it can turn into a problem when there is an exploitative attitude exercised by institutions to increase their profit margins at the direct expense of its clients. (Servon)

Individuals who hold shares and wish to gain profits have directly led to the increase in time preference of such institutions. And it is not isolated to banking, this also apparent in the Insurance sphere where obscured contracts are sometimes used to make it impossible to fulfill claims, based on the wording of the contract that was signed between the institution and the client. (Servon)

This type of time preference change is the main factor why there is lack of accessible lifesaving medications which are often outrageously priced, (Pollack) often citing research and development costs that companies must seek to even out with the sale of the medications. (Pollack) When immediate profits cannot be fulfilled, their research and development will not receive sufficient funding for its realization. Instead, other medications will be prioritized that give a company a steady stream of income, just as it was explained previously in main section of this chapter. Often such research now requires the involvement of governments and research universities because there is a lack of willingness from Pharmaceutical companies to participate actively in their research. (CDC)

Comparable situation can be observed with the development of electronic vehicles. Up until Tesla Motors has created a viable demand for electronic vehicles, auto manufacturers kept putting their focus onto fossil fuel based vehicles, and just a couple years now that some companies, like General Motors, declared that they would be going fully electric by 2023. (Davies) The lack of demand for electric vehicles kept driving the profit maximization of the fossil fuel based vehicles. It is well notable that Tesla was running deeply in negative operational costs before it began selling its latest models. This also indicates a much more lower time preference on the side of Tesla Motors than the other companies which did not wish to participate fully in such research or development. (O'Kane)

Research and development right now are not focusing on long term sustainability and modern inventions, but rather the exploitation of a given market segment that drives sales of certain products. In turn, drives up profits and increases the price of shares due to increased profits generated by the company. (Ammous)

When we examine the funding of healthcare and education in Hungary, we can see certain similarities that are present in Keynesian economics, namely, the sole reliance on numbers. (Ammous) Governments today are not considering inner factors in their decisions but rather base their decisions on statistics that

lack meaningful feedback of a given economics or social situation, eliminating the option of considering all factors that could improve a given problem. (Ammous) Therefore, healthcare and education in Hungary don't receive adequate funding. The Hungarian Government rather focuses on different ventures that appear more lucrative for itself. (Goldblatt and Nolan)

Members of governments do not go to these places to individually examine their circumstances and to make individual case by case decisions based on their given situation. (Ammous)

It is clearly apparent that Keynesian Economics and Monetary Nationalism have directly led to the global increase in time preference within society (Ammous), that ultimately began to damage it with a long lasting effect that is impossible to repair. (Ammous; Steil)

High time preference has resulted in the debasement of currency and the ending of the gold standard (Ammous), which have also accelerated the increase of time preference and made it more appealing for companies and institutions to abuse the individual's trust for their own financial gains. (Ammous)

This effect of monetary nationalism seems to indicate that the abuse of human trust is not a direct goal of the system. (Ammous) Although, some might argue that this is the abuse of trust, which is in turn not completely false. (Ammous) The problem we are facing is a self-reinforcing situation where the lack of choice alters behavior and changes the time preference of humans. (Servon) Those controlling companies have also have their time preference changed and according to that the operation of a company is executed based on the expectation of high time preference shareholders. (Ammous) In the end, it results in a situation where the system seeks to exert a totalitarian control over the spending behavior of society, which in turn creates political destabilization and the destruction of human produced value throughout inflation. (Ammous)

When we put our blind trust into institutions and later when we perceive it as breached, it goes against common sense expectations that we think is logical and reasonable. Then that trust of ours is breached and it becomes a necessity for us to seek for an alternative that can solve our problem. (Servon; Fukuyama) Therefore, we do not support political parties that lied to us during elections. We change banks when we are overcharged regularly for something that we do not expect. Thousands of Hungarians opt to migrate abroad to another EU countries to seek better employment and higher living standards. A minimum wage employment in Hungary certainly do not allow an individual to afford savings and will certainly resort to loans when a need arises. (Anon1)

But since here we have concluded that the main cause of rising distrust can be attributed in part to Keynesian Economics and Monetary Nationalism, can the problem be solved? Can we change the time preference of society and with that make it possible for people to be able to save money over time from their earnings? Can we stop Central Banks from stealing from us using inflation? (Ammous) Can we find an alternative (Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System) that frees us from the influence and control third parties, like, governments, banks, and central banks? (Ammous)

As of right now, if we would ask this question from experts and academics, they would fail to provide us with a sensible solution that reverses the effects of Monetary Nationalism. (Ammous) The legacy system

that we live in right now, does not has a solution for the almost permanent effects of high time preference. (Servon) This damaging effect have put our planet and society into direct danger and led to the over consumption of goods, excessive production of unnecessary products that further Climate Change and the lack of interest in the research and development of necessary inventions (like new antibiotics) that could counter dangers the future might hold. (Ammous) But while governments control us and enslave us throughout the use of inflation, it is impossible to do anything, and it is certain that we will be rolling down the steep cliff towards the abyss. (Ammous)

While it seems nihilistic (Cheong), the fact is that there is a viable, sound solution (Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System), (that is denied and ignored by many). (De; Ossinger) A solution was already made and created to solve our problems, just about 10 years ago in response to the 2008 Global Financial Crisis. (Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System) It is a solution that many great thinkers like F. A. Hayek, James Dale Davidson and others have predicted, just over ten years before its actual inception. (Davidson and Rees-Mogg)

In the following chapters, we are going to explore this alternative financial system (Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System) and see how it is able to fix our broken system (Pritzker), how it can free us, accelerate growth and global prosperity, and limit down the reach of governments that seek to control and enslave us. (Ajiboye, Buenaventura and Gladstein; Davidson and Rees-Mogg)

II. Bitcoin

Since the advent of the Internet, privacy has become a main frontline of development among members of the cypherpunk¹³ community. As the first formations of cypherpunk movements became apparent, the goal to make communication in the cyberspace censorship resistant has become a primary goal. (Hughes)

Liberational technologies also come to the forefront as end users also gained access to forms of encryptions that allowed communication and data to be hidden from prying eyes. As these technologies has begun to spread, thanks to the internet, everyone was able to encrypt their communication and hide from oppressive governments and from mass surveillance. (Hughes)

The establishment of a cyber currency been in the forefront of this ideology where an independent cyber cash could serve society independent that of centralized government control. (Davidson and Rees-Mogg) Up until 2008, there has been no viable solution created that was able to properly decentralize and make censorship resistant a monetary system that was necessary for liberalization of the individual. (Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System; Davidson and Rees-Mogg) As the internet began to spread across the globe, just within 28 years, in its current form, it has turned into a vital part of our everyday life. As the internet slowly began decentralizing control and governance, it has also begun to speed up the spread of technology globally, new revolutionary technology now able to bring about changes much faster than ever before. (Fukuyama; Davidson and Rees-Mogg) Since the centralized control and issuance of currencies are the main problem that allow the repeated breaches of trust, cyber cash type of currency was proposed to solve it, by creating the separation between state and currency. (Hughes; Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System)

Very few could imagine anything like an independent monetary tool that could function without the control of a government due to the nature of fiat currencies and their role within society. (Ammous; Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System) Their perceived stability and usage also make it harder to disassociate from in the process of value establishment in government issued fiat currencies. No previous currencies like HashCash or BitGold was able to solve the problems of double spending and lacked technological sophistication to operate properly. (Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System)

But this has changed in 2008 and a cascade of events has led to new belief that such a monetary system can exist outside of the reach of government that cannot be inflated at will. A monetary system which can serve as a sound alternative to fiat currencies, that can store human produced value due to its programmed scarcity that eventually creates a non-inflationary environment. A digital money that can also serve as a unit of account and medium of exchange due to its inherent properties. And a system which is reinforced by the complex social defensive organization that is built around it and its core value proposition and fundamental basic beliefs. As it is explained in the book called *“The Sovereign Individual”* a whole line of revolutionary effects could derive from the creation of such form of cybercash, that has the potential of changing the world inside out and liberating the individual from the tyranny of authoritarian governments. (Davidson and Rees-Mogg)

We are going to examine Bitcoin here and look at how this can be related to our problem of trust and whether it can solve that problem.

A. “*Bitcoin: A Peer-to-Peer Electronic Cash System*”

In 2009, an anonymous person, or a group of people, operating under the pseudonym called Satoshi Nakamoto has released a new software called Bitcoin. According to Nakamoto, Bitcoin is an opensource, decentralized digital currency, a form of peer-to-peer electronic cash system that can replace traditional fiat currencies and allow their users to transact without the interference of a third party. Bitcoin is the inventing technology and the main use case of blockchain technology. (Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System)

Bitcoin as part of its original design, was the solution for the long-standing double spend¹⁴ problem that previous creators of digital currencies have unsuccessfully attempted to solve. (Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System)

Satoshi Nakamoto successfully solved this problem by combining technologies that had a proven track record of past operation and with that improving upon past attempts. (Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System)

The Bitcoin Whitepaper was released on the 31st of October 2008 onto the cypherpunk mailing list by Satoshi. He in that email stated that he had been working on an electronic cash system that is fully peer-to-peer that not requires the involvement of third party. On the 3rd of January 2009, Satoshi Nakamoto have mined the Genesis Block of Bitcoin and on the 8th of January the same year, have released version 0.1 of

the Bitcoin software. The genesis block of Bitcoin contained the following message set by Satoshi: *"The Times 03/Jan/2009 Chancellor on brink of second bailout for banks."*

As it is explained in an email release by Satoshi, there are only going to be a total of 21 million bitcoins ever generated and no further coins will be issued. He in the release email clearly stated that the release of bitcoins as reward will cut in half every four years to the eventual point of zero reward per block. Upon the runout of the block reward, he stated that bitcoin transaction fees will eventually replace bitcoin block rewards and might be in the same range based on the increase in fee market competition. (Nakamoto, Bitcoin v0.1 released)

Bitcoin, due to its digital nature, can be easily broken down to its smallest fraction of value, one bitcoin consists of 100 million satoshis¹⁵. In total, there will be a total of 2.100.000.000.000.000 satoshi ever in existence. (Rosenbaum)

Bitcoin network can be accessed by interacting with the Bitcoin protocol on the internet. Users can acquire bitcoin either by exchanging value for bitcoins on exchanges or participating in mining of blocks. We can also earn bitcoins by providing goods or services. (Rosenbaum)

The Bitcoin protocol utilizes public key cryptography, which allows users to transact with each other and spend their bitcoin. A public key is basically a wallet address that can receive transactions. (Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System)

When we are spending from a wallet, we spend directly from addresses by using a public key to generate transactions then after use our secret key to sign these transactions. Bitcoin wallets, ever since the adoption of the BIP39, allow users to generate wallets with human readable secret keys in the form of 12-, 18- or 24-word list with which they can access their coins on the Bitcoin network. This key serves as the master key of the whole wallet which provides complete access to funds stored on addresses. Also, this key generates the extended public key which in fact controls the address generation for wallets. (Antonopoulos) Wallets can come in different forms and shapes, like paper wallets in the form of a brainwallet can be printed out (or memorized internally) that contain both the public and private key of a wallet address. Mobile devices can also be used to store or to transact bitcoin over the internet.

Here we can see a Quick Response code containing the public key of a Bitcoin wallet with the receiving address utilizing the latest bech32 address format. These QR codes can be scanned with mobile wallets and we can initiate transactions to the address.



bc1qgdy5grttcdc6me29lta7ycdkfcwrcjl44e5dz6z

When a transaction is signed it can be broadcasted out to nodes that receive our transaction which is propagated over the entire Bitcoin network within seconds. If anyone seeks to manipulate a signed transaction the master key that signed the transaction is necessary to modify a transaction, in the absence of the private key, it is *nearly impossible*¹⁶ to modify transactions. (Antonopoulos)

Nodes afterwards include our transaction in the memory pool of transactions and dynamically package them into blocks based on the fee of our transaction. When a transaction is included in the mempool, it is queued into blocks according to fee. The fee of a transaction is often dependent upon how large our transaction is and based on that we can set an amount of satoshi that we wish to include as a transaction fee for miners. (Rosenbaum)

These transactions are all transacted on the network and no actual movement happens, only modifications are issued which are recorded on the Bitcoin blockchain. (Antonopoulos)

Transactions are processed via the Proof of Work (PoW) algorithm that miners utilize to process and mine Bitcoin blocks. These blocks contain transactions up to the size of 1 MB, which is the base size which excludes the additional signature data of segwit transactions. (Rosenbaum) With the added headspace of block headers this can be a lot higher per Bitcoin block, up to a theoretical 400.000.000 bytes. (Song) The size and fee of a transaction affects which block it will be included in, due to their dynamic nature, a transaction with a more expensive fee might replace our less valuable fee transaction in a given block and be queued for later confirmation. (Rosenbaum)

Proof of Work uses a hashing function that produces an irreversible hash via the SHA256 hashing algorithm, miners utilize electricity to produce blocks by repeatedly hashing in order to find a number lower than that is calculated by a node's local blockchain. By expending electricity, miners complete the so-called proof of work to find the given hash and the ability to submit a block of transactions onto the Bitcoin blockchain. (Pritzker; Rosenbaum)

When a transaction is committed onto the blockchain, the transaction can be viewed using block explorer services or via our local node via command line function. These transactions can be viewed by anyone on the internet, since Bitcoin is a public and transparent monetary system, it is easy to validate the total amount of bitcoins in circulation and to track the movement of coins within the Bitcoin network. (Antonopoulos)

Ever since Bitcoin's inception, in the early days people began contributing to the protocol and the Bitcoin ecosystem began changing. Experimentations were ongoing and careless users managed to lose over 2 million bitcoins that were mined. Some ways of losses included accidental deletion of the Bitcoin core software and defective hard drives. In the early days, users were motivated by curiosity towards Bitcoin, but in 2010 Bitcoin began to wield value when 10.000 bitcoins were exchanged for two pizzas. Over the years, the price of bitcoin began its dramatic ascend, from a fraction of a dollar to almost 20.000 USD in 2017. (Roberts and Rapp)

Bitcoin from the early days have slowly transformed from an object of curiosity to important monetary tool that can serve as a store of value. The main aspect of Bitcoin's value proposition began transforming as more and more people began to find value within units of bitcoin. As others have elected to hold bitcoins speculatively, the price of bitcoin began to ascend. After the meteoric rise of 2012, a wave of speculative trading began sweeping across Bitcoin, the careless storage of user funds resulted in breaches and loss of funds ever since, with the most notable event of the theft of bitcoins from the Japanese Bitcoin exchange Mt. Gox. Ever since the breach at Mt. Gox, creditors have been unsuccessfully attempting to seek damages from Mark Kerpel, CEO of Mt. Gox. (Ammous)

Today, the total bitcoin market capitalization is about 168 billion dollars, at the price of 9352 US dollar per bitcoin on the 29th of October 2019.

From the early days of experimentation to the present day of active speculation, Bitcoin has grown into a diverse ecosystem that continues to grow without interruption. As the Bitcoin ecosystem keeps growing, it has become apparent that there is some important mechanism ongoing behind Bitcoin that somehow seems to affect human behavior and perception towards fiat currencies while actively lowering human time preference. (Ammous)

Since the genesis block of bitcoin cites the headlines of The Times newspaper, it became apparent that somehow this monetary system was created in response to the 2008 Global Financial crisis that seeks to provide an alternative sound monetary solution for people without a government or a third party actively managing or manipulating the supply and flow of bitcoins. (Ammous)

Researchers are claiming that, due to bitcoin's inherent properties and functionalities that developed on it, it has become a sound form of store of value while still providing abilities for its users to transact like normal monetary unit of account. In 2019 a stock-to-flow ratio was popularized by Saifedean Ammous in *The Bitcoin Standard*, that later other bitcoiners also began speculating about the existence of this stock-to-flow. Others mapped out the stock-to-flow rate of bitcoin for the next 15 years, to show there are certain correlation for the increase in value. (Ammous; PlanB, Modeling Bitcoin's Value with Scarcity; Andersch)

Since bitcoin is an engineered form of scarcity operating on the internet uninterrupted in the past 10 years, we must ask the question: How far this system is able to go? As claimed by a research done by Bayern Landesbank, a stock-to-flow¹² ratio of over 100 is unprecedented in human history and such a monetary standard could have unpredictable effects on societies transacting with fiat currencies. (Andersch)

As bitcoin keeps developing, new and new forms of solutions are found for its scaling problems, since blockchain systems are notoriously difficult to scale, layer two solutions were introduced to speed up

transactions. The system that achieved this is the Lightning Network that allows bitcoin transactions to settle within seconds using invoices and routing, while batch settling LN transactions on-chain on the bitcoin network to better utilize transactions on-chain. With the introduction of instant bitcoin transactions, the Lightning Network also introduced the concept of milli satoshi, further extending the decimals by 3 zeros that a bitcoin can be broken down. (Antonopoulos)

Since bitcoin functions similarly to gold as per its inherent properties, it is often referenced as digital gold that is better in many aspects than gold. (Ammous) Since gold, due to its physical properties, cannot be broken down and transported easily, makes it difficult to serve as a form of currency everyone can easily use. (Caras) But on the contrary a bitcoin can be broken down to its tiniest fraction of a given value and is easy to transport.

Bitcoin is also censorship resistant; no third party can censor transactions that are being transacted, these transactions can only be observed on the blockchain publicly.

Bitcoin can also be transacted offline by transporting it in a way that is invisible to others. If we memorize our private key, we can cross borders without anyone knowing that there are potentially bitcoins being transported across national borders. There are also now attempts to enable the broadcasting of transactions via bi-directional Satellites and the one-way transmission of transactions via radio frequency transmissions to a listening station that broadcasts our transaction out to nodes. Only requirement to move these funds later is to have access to the internet to initiate transactions.

Since human beings can agree on the price of bitcoin through social consensus that is enabled for them by the free market, bitcoin has value. Since the speculative holding of bitcoins are given, people store these coins and give it a speculative demand as a value storage that protects produced value from the inherent inflationary effects of fiat currencies. This process is exactly the same as on par with gold, since gold is also bought by others to speculate on its value, implying that the price of gold could rise or counter the potential effects of inflation. (Ammous)

Those people who buy bitcoin and later store them offline essentially have the same type of effect on the value of bitcoin like those who buy gold and store it in bank vaults or at home. These holders of bitcoin essentially determine the demand price of bitcoin, as more coins are removed from trading and the liquidity of bitcoin becomes more rigid and price movement can be more volatile due to less bitcoins being available on the free market. (Adamant Capital)

Often others call bitcoin a Ponzi or a Pyramid scheme because they claim that only those at the top can gain value as more users put more money into bitcoin and those people essentially can take out that amount and defraud others of their invested money. Claiming that if someone sells bitcoin the price will eventually crash and nobody else will be able to get back their invested amount. (Monaghan; Ossinger) But this is false, because the price of gold functions similarly and the same effect can be re-produced with gold. If we would sell large amounts of gold in a very short amount of time, we could see the price of gold crash rapidly and could potentially not go back to its original price due to the large order that has cleared through the market. The gold market can also be called this way a Ponzi or a Pyramid scheme. Since a given supply and demand determines the price of bitcoin it can in no way be called a scam, but we must

differentiate it from other alternatives that attempt to copy it, all other types of copies of bitcoin are only scams that do not seek anything else other than the enrichment of those who created it.

Since bitcoin appears to fulfill all aspects and properties that a monetary medium must consist of, such as divisibility into the tiniest fraction of a unit and censorship resistance, it could easily be the next step towards the evolution of money. Because of these inherent properties, we are going to examine some of bitcoin's liberating properties.

B. The End of Currency Counterfeiting

Bitcoin's underlying blockchain technology makes currency counterfeiting impossible. No new copies of bitcoins can be produced beyond the set total issuing limit of 21 million bitcoins, and no fake bitcoins can be transacted on the bitcoin blockchain. Alternative currencies cannot be sent to bitcoin addresses because they are not conforming to the consensus rules of the bitcoin protocol, therefore they are automatically rejected. If a bitcoin did not originate from a mined block, every attempt at inflating the supply of bitcoin with fake coins will be rejected by nodes and miners.

This is a long issue of currency that is now finally solved by bitcoin's creation, the problem of fake currency has been an issue of nation states dating back to the first minted monetary metal coins that others attempt to reproduce via forgery. The centuries old issue of counterfeiting is now stands finally resolved.

But let us stop there for a second, because someone could argue at this point that since the introduction of credit and digital money, counterfeiting has been resolved much earlier. In a sense this is correct, because we cannot duplicate PayPal balances, we cannot duplicate our Bank balance, but highly advanced hackers could in theory breach these systems and inflate the balances found on these accounts.

Banks can also duplicate money by issuing credit and maintain a fractional reserve, although there we can also argue that it is a form of fraud because our money is no longer fully there, and we must trust our bank to honor our withdrawal request. Central banks also participate in the duplication of currency that libertarians refer to as a form of counterfeiting by replicating the currency and with that legally increasing the total available count of it. When we refer to counterfeiting there, we must make it in the context of enforced counterfeiting resistance that few currencies can withstand.

The new \$100 USD bank notes were created in response of advanced super copies that were made by North Korea to use it in illicit activities on the open market. These super copies were later deemed very exceeding in ability to bypass checks on its originality; therefore, it became necessary to change the dollar note. From now on, we do not have to worry about the fact that the currency we accept is legitimate or not, because hacked funds on bitcoin addresses can no longer be reversed. We can easily verify the bitcoins that we accept with a full node on or on the bitcoin blockchain.

C. The Separation of State and Currency

As society started transitioning from nomadic lifestyles, the need to exchange goods began to rise, this led to bartering and usage of perishable goods as a form of value for exchange. Later, this transformed as humans started searching for more valuable value storage forms, like glass beads or Yap Stones, but because of their properties they were easy to inflate by those having access to better technology. (Szabo, Shelling Out - The Origins of Money) As modern civilization dawn starting with early Roman Empire monetary metals were issued that established the possibility of determining value in units of coins and exchanging goods and services with them. Today's modern civilization uses fiat currencies that saw their monetary metal backing removed as governments transitioned towards fully decree based issuance of paper money. (Ammous) National currencies are backed by governments and their issuance is managed by national central banks. These currencies enable commerce to continue and allow sovereign national states to compete. Often it is a problem that different currencies have different exchange rates due to their given present value. Because of that, exchange of currencies is required when crossing borders into another sovereign nation. A nation also can uphold its status and rank among other nations with its currency and influence others through it. Over the centuries, money has become an inseparable tool of statehood and a symbol of power. (Ammous) Although, there are nations that operate without their own national currency and use a different nation's currency. In that case their power will be limited, as well as dependent upon another nation's central banking policy. Only when these nations are closely united both politically and economically, can the other currency serve their utilizing members' self-interests. These are the formations of friction-less economies that operate with one currency, for example the European Union's Eurozone utilizes the Euro as a common currency for participating member states. These member states can do cross-border commerce without the need to exchange their currencies for another. (Fukuyama; Davidson and Rees-Mogg) Exchange rates between nations often stand as barriers to cross-border trade and introduce further expenses that a company must deal with if its suppliers or consumers are in another country that uses a different currency. (Ammous)

As bitcoin become a reality, this has become unnecessary, because right now value can be established in a non-reproducible electronic unit that is kept safe by a cooperating network of decentralized, interconnected computers. Value is now possible to be stored on the internet safely without the interference of a third party or a national central bank. There is no longer a need for exchange rates because anyone globally can accept bitcoin as long as there is an internet connection or a solution to relay transactions offline.

This is an important implication because if human beings can reach consensus on the value of a digital unit of a bitcoin, then there is no need for a central bank to issue currency. Bitcoin itself can become a form of money that has inherent value due to its properties. Bitcoin was intentionally designed this way to seeks to separate statehood from the issuance of currency and actively enforce it through its liberating incentives. Since it is extremely difficult to censor or restrict the flow of transactions within bitcoin, it can easily be seen by human beings as a very secure system that they can use to exchange goods and services. Anyone now can send money to anyone, anywhere in the world without there being a third party being able to control the flow of these transactions.

As an independent monetary tool that humans agree on its usage, bitcoin can immediately establish this separation.

D. Freedom from Inflation

As the separation between state and currency is established, another notable effect becomes a reality, namely, the absence of inflation. Inflation is a process that national central banks use to expand the money supply. This expansion of the money supply decreases the value of a currency over time, which leads to less purchasing power present within a fiat currency. (Ammous)

This is often called by others as a form of free money printing, and it is understood by libertarians to serve no other basis as to take away wealth from those who hold fiat currencies. Inflation inherently makes savings impossible and this effect reinforces high time preference and forces human beings to spend this value immediately. (Ammous)

The problem that the printing of money causes creates a trust issue between the user of money and the central bank and its government, because it is the duty of central banks to prevent the devaluation of a national currency. Satoshi himself mentioned it in one of his forum messages with users, that the history of fiat currencies has been full of these breaches of trust, especially related to trust placed into the banking system. (Nakamoto, Bitcoin open source implementation of P2P currency)

Since Bitcoin's money supply cannot be inflated by a third party or a national central bank, the value of it can be constant. Although some would argue that bitcoin is not a safe value storage due to its extreme volatility. They claim that because of this problem it cannot fulfill the aspects of a stable value storage, for the value of a bitcoin can diminish the next day when we place our hard-earned value into it.

This to some extent is true. Since bitcoin is a relatively new technology, only those users with very high tolerance towards this volatility can utilize the technology properly long term. Most speculators often end up withdrawing value from bitcoin when the value "crashes" and with that losing a large amount of their initial investment. These are usually inexperienced speculators who wish to profit from this type of extreme volatility.

In turn, if we examine the recent explanations about the stock-to-flow model of bitcoin, we can see that long-term Bitcoin's value has been relatively stable, absent of catastrophic value losses. The stock-to-flow model of bitcoin seems to hint that in the future the price might stabilize once Bitcoin eclipses the legacy financial system.

Since the issuance of bitcoin is capped at a total of 21 million coins, this introduced the new aspect of programmed scarcity. This way Bitcoin has a programmed limit that can be calculated mathematically based on its past performance and we can also this way attempt speculatively to determine the possible fiat value range of Bitcoin in the future.

Since the value of Bitcoin can stabilize in the future, there will be no observable effects of inflation. Bitcoin is designed to become non-inflationary as the total amount of bitcoins is slowly depleted with the use of mining. Value stored in bitcoin can keep its value constant or be appreciated against fiat currencies that will continue to lose value against it. As more demand is there for bitcoin, the value is expected to continue to appreciate over time. As less and less coins are lost as the storage methods improve, there will be less and less deflationary effects affecting users of bitcoin. Deflation will also not be a matter of

importance to the users of bitcoin because one bitcoin can be easily broken down to the smallest fraction of it.

This inherent ability of bitcoin to show human beings that their produced value can hold value can lead directly to the re-normalization of long-term savings and to the decrease in the usage of credit. Since now anyone can save up money over time to afford better quality products in the future, it is no longer a necessity to reach for credit anymore. In the current system, the line of credit automatically robs consumers from future profits and better products as they attempt to satisfy their immediate needs.

E. Circumventing Authoritarianism with the use of Bitcoin

As governments all around the world slowly become bigger and more controlling of their citizens' lives, the more breaches of freedom and liberty can be observed. Authoritarian governments or those who seek to exert violence on a population can easily enact laws and regulations that allow them to exploit their citizens. Although it is questionable whether all such forms of abuse can be linked to authoritarian establishments, because most of these cases can often happen in democratic countries, too, as we will soon observe it.

For example, in the United States it is not uncommon that transported cash en-route is caught by police and confiscated under Asset Forfeiture Laws. Police in certain states in the United States can confiscate physical cash from individuals under the slight pretense of suspicion from individuals. These cases often come with charges related to money laundering and cash originating from the drug market. As more than 90% of the total circulating supply of physical US Dollars are contaminated with traces of cocaine (Pesce; Pilkington), it is just a matter of time when substances found on paper notes might be used against civilians to assist police in the confiscation of cash. It is also difficult to carry cash across borders; many individuals came across a problem of transporting their wealth across border and witnessed only at the border that their money was confiscated with no possibility of ever getting it back from the US Customs and Border Protection.

In Venezuela the Maduro Regime controls the flow of currency in the country, the usage of the Bolivar is mandated by the government. As the value of the Bolivar is rapidly diminishing over time due to the rapid printing of currency, new forms of barter tools were necessary to use. Locals began using cigarettes and food products as payment options when paying for goods and services, for example exchanging a package of toilet paper rolls for gas on a petrol station. In many senses the power of authority comes from the issuance of currency for most authoritarian regimes and for democratic ones. By inflating the money supply, governments can exert totalitarian control over the population and make their movement and activities centrally controlled.

In South Korea, it is illegal to exit the country with physical bank notes and in Iceland it was illegal to use a different nation's currency for exchanging goods under the Foreign Exchange Act of Iceland¹⁸, which was later amended to allow it. These mandated restrictions on the usage of currencies seem to show a clear tendency towards enforcing sovereign national interest at the expense of citizens. Bitcoin usage in Iceland

is for example was banned, as it was considered foreign because it was not issued by the Icelandic Central Bank and their users faced fines if they break the law. However, the law cannot be enforced because the physical transaction origin of bitcoins can be hidden and only a movement on the blockchain can be observed.

The main problem Bitcoin fixes here is the confiscation and control of flow of value between human beings. It is an **inherent ability** of *Bitcoin to circumvent* all forms of **Financial Censorship**. Due to bitcoin's properties, it cannot easily be confiscated, and its flow cannot be restricted. Bitcoin can also circumvent legal frameworks of nation states. Citizens who do not agree with certain laws or regulations can always decide to opt for civil disobedience (or in certain other situations, straight out resistance against a government) and refuse cooperation with such authorities that try to take away their own wealth that is stored in bitcoin. In a dictatorial state, bitcoin can be used to completely circumvent government control and re-establish individual financial freedom. Although there might be a possibility for a government employing totalitarian surveillance, bitcoin can also provide liberating abilities because it can be used for any means that a government will not be able to censor, therefore it is arguable also that it can restore liberty. If we are oppressed in our own country, we can use, in theory, bitcoin to flee a country and finance our escape with it, if someone accepts bitcoin, then the possibilities are endless.

A bitcoin private key that is protected by a strong passphrase is completely protected against all forms of physical confiscation, as long as the individual is able to access the private key uninterrupted. **Even if physical copies of the private key are stolen, a government can do little to access the bitcoins on an address hidden behind a passphrase.** Even the *decentralization of storage of private keys and usage of multi-signature hardware wallet solutions* provide a further step towards resilience of personal wealth.

Bitcoin in this perspective is a sovereign form of monetary system, because it enables the enforcement of the self-interest for individuals. Governments that seek to interrupt it or ban it, will fail because of the organization of bitcoin's ecosystem and active protection provided by its users. (Taleb, Bitcoin) We will follow up on these aspects in a later chapter.

i. Bitcoin Improvement Proposal 38-39

The Bitcoin improvement Proposal of BIP38¹⁹ (passphrase protected paper wallets) and BIP39 (mnemonic code for generating deterministic keys) was a major milestone in this process of creating a truly sovereign form of money.

The solution that BIP39 provided was the generation of the secret key to a bitcoin wallet in the format of human readable word format that consist of 12-, 18- or 24- word combinations. This list contains 2048 words in total and these can provide strong random variations when creating a key, therefore guessing it is astronomically difficult. Therefore, to guess an address that could contain any amount of bitcoins we would have to find one from the total of 256×204823 which, if we put into a calculator we can see, will be nearly impossible. (Rosenbaum)

The introduction of human readable words also makes it easier to store it, 24 words can be written down and stored safely or even memorized. The introduction of passphrase protected paper wallets also made it possible to introduce a 25th word²⁰, that is the passphrase that can be anything.

The combination of these two features makes bitcoin very resilient to all forms of confiscations.

ii. Wikileaks

In 2011, the whistleblowing news leaks site, WikiLeaks began accepting bitcoin as a method of donation after Bradley Manning leaked secret military files and communications that had shown that members of the US Military murdered civilians and journalists working in Iraq. As sanctions began targeting WikiLeaks founder Julian Assange, financial pressure was put onto the whistleblower website to attempt to halt its operations. Major payment processing companies began blocking donations and in response Julian Assange announced that to counter these attempts at censorship they would be accepting bitcoin donations. A Bitcoinist article speculated that in 2019 WikiLeaks amassed over 4000 bitcoins ever since the donation drive in bitcoin began. (Avan-Nomayo) Since the movement of bitcoins can be verified on its public blockchain, we can personally verify its truth content. It is subject of speculation whether WikiLeaks is still sitting on these funds or have used it to fund its own operations.

The 2011 case of WikiLeaks accepting donations in bitcoin shows how resilient the system is against attempts of financial censorship.

In the next chapter, we are going to look at the programmed protection layers of bitcoin, how they look like and what kind of effect they have on the broader ecosystem. Since now we understand narrowly how bitcoin functions, we can now see how functions of bitcoin and changes that were made to it protect it actively against forms of censorship and third-party interference.

III.Censorship Resistance of the Bitcoin Protocol

Bitcoin often finds itself in the midst of attacks on its network propagated by the actions of financially charged third parties and state actors. Some advancement in its development was created to solve these problems that could arise in the future and to mitigate potential attacks against its users. Since it is implied that Bitcoin is constantly under attack and not just on-chain attacks are possible, any form of social-engineering attacks could also target its users that could disrupt the total cohesion of the ecosystem.

These integrations and improvements exist to make the use of bitcoin safe, secure, and hard to censor, essentially putting power into the hands of the users.

If a government would seek to interfere with the use of the Bitcoin Protocol today, there are many new solutions and advancements built around its underlying core technology that make it censorship resistant.

We are going to look at these notable features relevant to this given problem of censorship and interference in the following sections.

A. “Just pull the plug out, and the problem is solved!”²¹

Due to misconceptions, some non-users think that it is possible to shut down bitcoin by shutting down the network, but this is a false conception. Bitcoin nodes and miners operate decentralized in many countries across the globe and this makes authoritarian attempts to shut bitcoin down nearly impossible. In order to shut down the network, one needs access to every country where nodes and miners are operating, and these countries have different legislations and laws that make it very difficult to process such demands, especially if a country is a hostile one towards another and they are unwilling to cooperate with one another. Corruption can also make it impossible or extremely hard to get authorities shut down the infrastructure to nodes and miners. The system has reached such scales that it can no longer be shut down. Even if it is damaged, it is designed to survive such attacks and continue operations uninterrupted. Therefore, shutting down nodes and miners is extremely difficult if not impossible. (Pritzker) Due to Bitcoin’s inherent properties, it is considered widely among Bitcoiners to be an antifragile monetary system. (Taleb, Antifragile)

B. Bitcoin, Software as a form of Absolute Truth

Bitcoin is unique, it is the only existing system that is built on computers and on the principles of mathematics. Bitcoin itself is a form of distilled truth, an absolute reality not impeded by anyone’s reality. The monetary system’s total capacity, as well as the amount of rewards given to miners, can be mathematically verified. The Bitcoin network can be held to account towards its correctness and truthfulness because the decentralized groups of miners constantly verify and re-verify the total amounts of Bitcoins in circulation. If we attempt to create more Bitcoins the system refuses that and rejects the transactions because they do not originate from a block and the reward was never issued by a node for a miner for the successfully found block. (Ammous)

This total verification model allows us to be in complete possession of truth, just by running a simple computer code on our Bitcoin full-node wallet software.

`bitcoin-cli gettxutsetinfo` - This command here will return us the most recent block height, the Bitcoin blockchain’s total size on the hard drive and the total amounts of Bitcoin released in total up to the last mined block.

`bitcoin-cli getmininginfo` - This command will return the total hash power of the available miners and the block difficulty which governs how difficult it is to find a correct hash to mine a block. (PlanB, Verification of Monetary Supply of Bitcoin)

This way, Bitcoin made it possible for everyone to be able to verify it. This programmed truthfulness is unique in the world because everything in our reality is just a perspectival form of reality that only exists in our own reality, but Bitcoin’s truth is absolute. (Ammous) In turn, we cannot gain access to Banking records, we cannot gain on demand access to financial systems to audit them and hold their operators to account. It is this inability to properly oversee financial systems and institutions that essentially led to the 2008 Financial Crisis. (Servon)

This direct access for the ordinary person to audit the monetary supply makes it essentially an amoral²² form of sound money and allows the user to prosper under its system with the knowledge provided for him on demand. The knowledge creates stability and progress for society as a whole as argued by Friedrich A. Hayek, and can be applied in the context of Bitcoin this way to create a form of sound money that cannot be inflated by anyone, cannot be censored and cannot be impeded upon by anyone in any way. (Hayek, The Use of Knowledge in Society)

i. On-Chain Privacy

Some users of Bitcoin claim that since Bitcoin is a radically transparent monetary system, the privacy of its users can easily be compromised. They claim this is made possible because of the lack of on-chain privacy present in Bitcoin. For, anyone can follow the transaction of users since the history of those transactions permanently stays visible on the public Bitcoin blockchain. Some of these users and developers have been proposing changes to Bitcoin that make these transactions hidden on the Bitcoin blockchain. These proposals would in theory make the complete movement of bitcoins invisible on the blockchain. Certain technologies already exist that make these potentially possible, but with extreme consequences if the technology is faulty or if their implementation could allow malicious actors to compromise the network. One main issue that on-chain privacy creates is the possibility of hidden inflation. Malicious actors could use methods to print bitcoins out of nowhere to inflate the supply of bitcoins without the network or the users of Bitcoin being aware of.

The underlying aspect of absolute truth availability is necessary for the ability to not require initial trust in the usage of Bitcoin. If a technological modification would alter the underlying functionality of this verification process, thereby violating the philosophical principle of fact-fullness, initial trust in the creator of Bitcoin would be ultimately necessary. Only such technologies can be employed and activated on the core layer of Bitcoin that do not violate this given philosophical aspect. If we cannot establish a returned information as being completely factual representing the given state of reality of the present status of the network, then the purpose of bitcoin, which it was created for, ceases to exist.

Of course, if on-chain privacy would ever be proposed, there are many other factors that must be accounted for. One of the most important danger is fragile forms of privacy providing solutions that provide only a false sense of privacy. If quantum computers would be able to undo those protections, the damage done to the privacy of the users would be unforeseeable, with unpredictable consequences.

This is the sole reason alternative solutions, that are proclaiming to be better sound alternatives to bitcoin, fail, because they cannot fulfill this basic underlying principle.

Privacy protecting options already exist for users of Bitcoin that can safeguard their on-chain privacy by providing accountable solutions that do not violate the philosophical principle. In a later section within this chapter we are going to look at these problems and their solutions more in depth.

C. Bitcoin Node

A Bitcoin node is a software or device that runs the Bitcoin protocol, with a software similar like 'bitcoind', and itself can be run on servers and on desktop environments. These nodes contain the full or partially pruned database of transactions all the way originating from the Genesis Block to the latest block height of valid block mined by a miner. In the past, Bitcoin nodes were combined devices that allowed the mining of bitcoin, but due to the infeasibility of such activities because of resource intensity on consumer computers, this was later separated. Notable implementations are the reference Bitcoin Core application that downloads the entire Bitcoin blockchain onto the user's device. Nodes verify blockchain consensus rules by enforcing the core properties of the Bitcoin network. When a miner²³ finishes a proof of work process, it then gets the ability to submit the found block onto the Bitcoin blockchain. Before that happens, nodes must verify that the miner has found the correct hash that was set out as a requirement to find and submit the block that contains the transactions. If everything is in order, then the block is put onto the blockchain, it will attach to the preceding block and all proceeding blocks will be attached to this block. The chain of blocks is called as blockchain. Originally Satoshi Nakamoto referred to this as a time chain but later changed his wording to blockchain. (Graff)

Bitcoin nodes also serve an important role within the Bitcoin ecosystem. Due to their ability to enforce consensus rules, the nodes are of higher authority in the ecosystem due to their voluntary operational basis. Although Bitcoin nodes can no longer mine blocks, they must cooperate with miners in order to include new blocks on the blockchain.

When a miner produces a correct block, it²⁴ receives a reward from the Bitcoin node network for finishing proof of work properly. When a miner attempts to produce false blocks, the nodes reject those blocks and do not provide a block reward for false blocks. Therefore, nodes are essential units of the defense mechanism of the Bitcoin network in relation to transaction processing, and act as a last line of defense against malicious miners. Although a 51% attack could be used to produce blocks, the nature of the proof of work algorithm promotes adherence to the consensus rules to receive block rewards. Attacking the Bitcoin network comes with extremely high costs due to the expended energy that is required to produce the correct hashes that allow miners to submit blocks to nodes to include them on the blockchain.

Nodes other than storage of transactions serve as a defensive layer against coercive enforcement of core layer changes on the Bitcoin protocol. When miners attempt to collaborate to enforce changes to the core protocol of Bitcoin, they can opt via a user activated soft fork to block such attempts and signal for miners that if they proceed with such changes in base function then they will reject their produced blocks, wasting the energy that was used to produce them. During the Segregated Witness protocol upgrade of Bitcoin, node users prevented collaborating miners from enforcing changes on the protocol by opting to proceed with their own change in function. The group of users who collaborated to increase the block size of produced Bitcoin blocks had their attempts countered by the UASF (User Activated Soft Fork) movement when they attempted to impede upon the basic principles of the Bitcoin protocol. Bitcoin Cash raised its block size beyond the amount that Bitcoin node users allowed it to, during the UASF. Essentially afterwards the Segwit Activation was done with the 1MB blocks, the NO2X movement blocked the increase of block size to 2MB blocks.

Since the increase to 2MB blocks would have led to an increase in the total size of the Bitcoin blockchain. (Song) The supporters of UASF and NO2X movement claim that this would have led to less nodes running and more demanding storage requirements for full nodes, with that decreasing the ability of the network to protect against such forms of attacks. When we consider the overall effect of a later hard fork of Bitcoin Cash to BCH ABC and BCH SV, we can see that BCH SV attempted iteration of forked Bitcoin protocol relies on mass centralized storage of the block data in centralized data centers. (Block Digest)

When we examine this effect of centralized operation of Bitcoin nodes, we can realize that these centralizations are a digression from the core principles of decentralization and could be claimed as an attempted attack on the Bitcoin network to further weaken it. State actors that push the node operation out of the hands of the users can now more easily coerce node operations in data centers to push through core protocol or consensus changes in Bitcoin that could weaken the network or allow them to censor or interfere with the whole network. Operation of nodes on centralized datacenters allows third parties or state actors to censor their operation or even shut them down by forcing these datacenters that host them to cut access to them or permanently shut them down. Therefore, such attempts to control the development of the network should be viewed as a form of attack on the core layer of the Bitcoin Protocol.

D. Offline Bitcoin Transactions

Bitcoin can be very similar in some context to paper money transactions, because a brain wallet can be printed out onto paper and later exchanged with another person for goods or fiat currencies without anyone seeing a trace of the transaction on the Internet or the Bitcoin Blockchain.

Similarly, hardware devices (like the OpenDime credit sticks from Coinkite) that contain any amounts of bitcoin can be given away safely without exposing the private key.

A Bitcoin BIP39 private key can also be exchanged with others but this is not recommended because anyone can copy the private key or, if it is directly visible, anyone can potentially move the funds after exchanging goods.

Although, these methods don't come without possible negative consequences. For example, brain wallets could get damaged, especially since most of them are printed out onto paper when exchanged, and the QR codes and private key could become undecipherable if it gets damaged, potentially risking complete loss of funds this way.

Physical attacks during exchanges of bitcoins can also be a risk. There have been confirmed cases of attempted attacks against Bitcoiners who attempted to exchange their bitcoins for fiat currencies during in person meetups in public places.²⁵

Although if we want to move bitcoins from one wallet to another, it becomes necessary at one point to broadcast a transaction onto the internet, but the generation and broadcasting of that transaction can be done isolated from the internet, thus being referred to as an offline Bitcoin transaction while it is not handed over to a network of Bitcoin nodes.

There are also other forms of offline transactions that do not touch the internet in any form in certain stages of its transit, which we will look at next.

i. Partially Signed Bitcoin Transactions

Partially signed Bitcoin transactions are a new isolated way of transaction generation and signing of the generated Bitcoin transaction. A computer software like Electrum²⁶, Wasabi Wallet and mobile wallets like Samurai Wallet's Sentinel application can generate transaction information by using an extended public key of a Bitcoin secret key that contains all the addresses (virtually everything, but only those necessarily that contain amounts of bitcoin) associated with a given secret key. When a transaction is generated, a data file is created that can be moved to another device, this is called as an unsigned transaction file.

After the file was moved to another computer or a dedicated hardware wallet that is capable of transaction signing, it can be signed using the private key of the given address which then generates the final transaction data. Afterwards the transaction, data can be moved back onto a computer again or a broadcasting device that has access to the internet, these files can be then loaded into Electrum Wallet, Wasabi Wallet or the android mobile bitcoin wallet called Samurai Wallet and then it can be loaded and then broadcasted out onto the internet to bitcoin nodes that will put the transaction into the mempool if our transaction is valid.

This is one of the most favourite transaction type among some Bitcoiners because of its most cypherpunkesque method of isolation of the transaction data that makes it very resistant towards man in the middle attacks. The generated transaction file, when signed, can no longer be deciphered preventing others from altering the transaction. The only way to change it is to have access to the private key on the signing device. Without it, it is certainly not possible.

Hardware devices that currently exist, for example the ColdCard Wallet by Coinkite, are the only notable devices right now that can sign such transactions and securely handle its process while being completely isolated from the internet.

Such transactions are also very handy because they can be broadcasted onto the internet in many different ways that can potentially circumvent censorship attempts.

ii. Bitcoin over Satellite

Recent development made the company called Blockstream have made it possible for Bitcoin users to access satellites in orbit via home satellite dishes, that we used for TVs and other devices, and the network of satellites can be now used to sync the Bitcoin blockchain.

At the present time there are a total of 5 satellites covering most major population centers of Earth that can be used for such purposes.

Also, what is not possible is to use these satellites to broadcast messages back onto the planet. This makes it possible also to send signed Bitcoin transactions for others who can afterwards broadcast the transaction onto the internet.

As of today, Blockstream is actively working to make it possible to use their satellites for two-way communication with Bitcoin wallet applications.

The necessary equipment that is needed for communication with these satellites is very inexpensive. About under 60 dollars makes it very affordable to access the satellite network with cheap re-usable equipment which makes it possible to access network after the necessary setup procedures.

This is also a very useful tool to circumvent potential censorship of Bitcoin transactions because satellites cannot be effectively censored by state actors. Users can also send messages to these satellites that get re-beamed back onto Earth by these satellites to receiving users, with the same satellite dishes, who can then read the content of these broadcasts.

a. @SatNode: Blockstream Satellite Transmission Feed

Alternatively, although not a form of Bitcoin transaction, the Blockstream Satellite can also be used to broadcast messages onto the micro-blogging social media site like, e. g., Twitter. Bitcoin users who have a lightning wallet can use the official Blockstream website or the lightning wallet bot called Intxbot on the online chat application Telegram to broadcast messages for a given fee determined in satoshis. After the broadcast was successfully received and broadcasted, these messages get put onto a Twitter bot account, located at the handle @satnode, with the original message and links to the messages on a separate website.

SatNode, which is operated by the Twitter user @notgrubles, had already the bot account suspended multiple times due to some users using the satellites to broadcast profanities targeting users, holders and developers of shitcoins²⁷.

Although the majority of messages are not offensive, this anonymous broadcast ability of instant messages via satellite seems to serve the ultimate purpose of strengthening freedom of speech and providing access to mass communication services to the ordinary citizens, services that can be often censored by democratic and authoritarian governments alike.

iii. Bitcoin over Radio Frequency Signal

Rodolfo, a Canadian Bitcoiner, programmer and hardware company owner was the first recognized person who conducted a radio frequency transfer of the bitcoin transaction data.

The first transaction was made on the 12th of January 2019. It consisted of a bitcoin transaction to an address from a brain wallet on a computer, and the transaction was made over a JS8Call over the 7.077Mhz radio band from Toronto, Canada to Michigan, USA. Later the transaction was returned from the USA using a bech32 native segwit address type.

On the 1st of March 2019, Rodolfo again conducted a transaction, but this time broadcasted a lightning transaction (from now referred to as LN) invoice via an iNet 21 message, from Toronto, Canada to San

Francisco, California. From that location, the other person was able to scan or sweep the invoice into a wallet and send the transaction for Rodolfo. Rodolfo's LN transaction was received by multiple receivers but only one person has sent him a transaction using his onetime usable generated invoice.

This kind of transaction that was made shows that Bitcoin has reached a very extended level of censorship resistance, because not often it is possible to censor such radio broadcasts or interfere with their broadcast. If a country is blocking Bitcoin transactions, the transaction can be just broadcasted over to other countries where listening stations or other people receiving these transactions can broadcast it out from their location in another country onto the internet.

E. Tor Layered Censorship Resistant Bitcoin Integrations

The censorship resistant properties of the Tor²⁸ protocol that anonymize its users is already being used to protect the users of Bitcoin wallets and Bitcoin nodes from third party, government snooping and interference.

While the Bitcoin network cannot be anonymized with the use of Tor, in theory, it can be used to protect end users and node operators. Every Bitcoin transaction that touches the internet can potentially be viewed by third parties and government agents, exposing the IP address and potentially deanonymizing the user.

By using Tor, the origin of the broadcast can be protected, the IP address does not leak out onto the internet, this way protecting the broadcaster of the transaction from having their identity compromised.

When such an integration is created for node operators, they can sync the Bitcoin blockchain and handle all Bitcoin protocol operations via Tor. This way Tor gives an added level of censorship resistance for the Bitcoin Network by protecting the node operators from potential government overreach of power or intentional censorship. By running the nodes through the Tor Network, it becomes harder to find node operators and with that much harder to shut down nodes if a corrupt or authoritarian government would seek to shut it down.

However, the usage of Tor is not a silver bullet because certain communication data can leak out for Internet Service Providers. Data like HTTP/HTTPS requests and DNS queries can be still discovered by our ISP (Internet Service Provider) which then could be reported to the Police or Government Agencies. (BTCPay Server)

Wallet integrations already exist that make use of this technology, like Wasabi Wallet²⁹, Samourai Wallet³⁰ and Blockstream Green³¹. These integrations attempt to make interaction with the Bitcoin network safer for those who might else be censored or have their finances controlled by governments. Although, other applications running on our computer or mobile phone could snoop data and traffic information, invalidating such protections very easily. In the hands of an inexperienced user, these tools could easily be compromised without their knowledge.

There are also 'bitcoind³²' node (and lightning network LND node) integrations that seek to function within a Tor enclosure. For example, these can be found in some of the most notable nodes and node

packages like BTCPayServer³³, MyNode³⁴, Samourai Dojo³⁵. Although only a fully independent installation of Samourai Dojo offers full protection without leaking any HTTP/HTTPS and DNS queries, BTCPayServer might leak such information due to having some of the added extensions and variables outside of the scope of their control.

Bugs in code might also exist and ultimately negatively affect these protections, therefore there is no foolproof solution for completely anonymizing a Bitcoin node.

When such integrations are used, wallets can connect via the Tor network to trusted Bitcoin nodes that make the verification of transactions much more reliable while in theory preventing potential third parties like Chainalysis that seek to associate identities of users with Bitcoin addresses.

Chainalysis runs Electrum Private Servers³⁶ to collect IP addresses of Bitcoin users who interact with Electrum Wallet, with that attempting to completely deanonymize users and link their transactions on the Bitcoin blockchain. Although Electrum can connect through Tor Browser's SOCKS5 proxy, it is still not considered as private when used without a self-hosted Electrum Private Server.

Easy installation of node software is also essential for the full protection of the Bitcoin network, therefore lack of ease of access to node software and packages and very complex installation procedures can be detrimental for the entire Bitcoin ecosystem. Other than Samourai Dojo's full node package, there is no such integration today that would effectively solve the problem of making the operation of nodes completely hidden before the eyes of government.

A perfect theoretical Tor integration would not leak any communication data between the node and the Bitcoin network and would keep all contents of the messages sent between the server and the network encrypted and undiscoverable by outside observers of traffic communication. While this is not entirely possible, some solutions get very close to this, with that aiding the censorship resistance of the Bitcoin protocol and the personal safety and privacy of its users.

F. Bitcoin Privacy, Fungibility and Anonymous bitcoins

As privacy slowly comes to the forefront of debates, the problem of Bitcoin's extreme transparency causes distress to some users who feel that this radical transparency can potentially endanger them in the real world. Since every user's transaction is visible on the blockchain, we can follow the movement of bitcoins. If we are able to identify an owner of certain coins, we can follow the complete path and origin of those funds. For some, this is a catastrophic flaw that allows others to impede upon other's personal financial privacy.

The closure of SilkRoad proves that there was a massive misconception about Bitcoin's privacy capabilities, but since the Federal Bureau of Investigations was able to trace back the origin of certain tainted bitcoins, they were able to shut down SilkRoad's operation and apprehend Ross Ulbricht. This is one reason why terrorists don't use Bitcoin, because they have to be able to withdraw into fiat currencies their earnings and that must be done through some form of exchange which is connected to tax authorities, who can immediately flag their transaction then that allow counter-terrorism forces to

apprehend them. It is highly unlikely that terrorists who use bitcoins are even properly able to understand its basics of value. Instead, it resembles a temporary transaction medium that they can move later to exchange for cash, since virtually nobody accepts coins from them. (Frisby)

In today's world, paper money's functionalities reflect that of anonymity, because when we are exchanging paper money, or coins, their movement is invisible and each USD that is not counterfeit, is basically fungible. Within Bitcoin, this is on the contrary because we can follow the movement of coins and can easily have them "tainted" manually. Exchanges can red flag coins and make their spending extremely difficult on KYC³⁷ enabled exchanges that are required to comply with Anti-Money Laundering³⁸ and Counter-Terrorism Financing directives.

These tainting of coins soon could be causing issues for the users of Bitcoin, who use bitcoins similarly like physical cash. Some users came across unwarranted action by police and the law when getting into touch with tainted bitcoins that somehow touched illegal activities, for example coins that participate in exchange of psychoactive substances that later ended up in the hands of a consumer. It can be speculated that such coins could be considered illegal by certain state's authorities. (Vauplane)

The problem we have already examined in relation to *On-Chain Privacy* within this chapter, is still in the forefront of this debate that many often cite as an important future battleground of Bitcoin that is about to happen. The quest to restore fungibility of bitcoins is now an especially important topic within the online bitcoin space among users.

Some of the earlier proposals like the Mumblewimble (Nicholson) proposal seek to restore this privacy on-chain. However, as it was implemented in different alternative blockchain copies of Bitcoin, it become proven that it is in essence a failed proposal that can't function properly and its perceived privacy benefits are non-existent. (Bogatyy)

Other centralized mixing services³⁹ started operating that promised to mix the coins of users to return their anonymity, but usually these activities were not safe due to their trust requirement and often ended up shut down by Police as part of Interpol operations against these mixers. Users who sent their funds to such mixers that were shut down by police never managed to get their coins back. The case of Bestmixer.io was a notable case in the Netherlands where a multi-country cooperation brought down the site. (Beedham)

One of the most notable way of obtaining anonymous coins is via Bitcoin Automats (BATMs) that accept paper currencies in exchange for bitcoins. If nobody observes our activities, the ownership of the coins is in theory very difficult to establish, even if proper coin control techniques are employed. (Schoenberg and Robinson)

As on-chain transaction analysis started to proliferate, governmental actors began contracting the company Chainalysis to track the movement of bitcoins on the blockchain. They began developing methods to track and de-anonymize users and potentially associate real-life identities. It is a well-known fact that Chainalysis operates Bitcoin Electrum Private Servers in order to track transactions and associate coins with their IP address that they originate from. Chainalysis later can sell the data or offer it as a service for state actors to violate the privacy of unaware users.

Eventually Chaumian CoinJoining came to the forefront of this battle with the first implementation of Join Markets and afterwards the ZeroLink protocol implementation. (nopara73 and TDevD, ZeroLink: The Bitcoin Fungibility Framework) The ZeroLink proposal is very notable because it completely breaks on-chain analysis with that making the work of Chainalysis impossible. Some users although claim that these solutions are not enough and fail to achieve true coin anonymity because of the possibility of being able to calculate the origin of the mixing output. As opposed to that, it is also argued that in order to be able to revert these outputs and deanonymize their origin at least minimum of a quantum computer is required. (Harmat and Molnar)

The ZeroLink proposal has two separate implementations, Wasabi Wallet and Samourai Wallet's Whirlpool, and both have their own distinct way of implementing these coinjoins.

i. CoinJoining

CoinJoining works by mixing multiple individual input transactions and generating an output transaction on the blockchain that contains multiple equally numbered Bitcoin outputs. For example, if we have Alice, Bob, Sam and Lisa who own respectively 0.2, 0.2, 0.3, 0.4 bitcoins, these transactions are broken down via a coordinator's help to 0.1 outputs, generating 11x 0.1 bitcoin outputs all within one transaction. On the output side it is difficult to know which of these transactions came from whom because of the way these were mixed by the coordinator, with that breaking others ability to distinguish their origin. When done, these transactions look indistinguishable on the output side with that restoring privacy to a certain degree for mixed coins.

As the input user count keeps climbing, the higher anonymity sets⁴⁰ can be achieved, further strengthening the fungibility of bitcoins. As these coins have their privacy restored, they are able to function as a form of physical cash since the bitcoins' origin cannot be traced back. However, some would claim this is a form of money laundering, which could be possible because after an output the coins can be spent without anyone knowing which coin belongs to who, it cannot be used to avoid taxes. Tax avoidance is impossible because as we mix coins the tax authority still implies that we own the same amount of coins that we have mixed and during a deposition audit a tax agency can imply that we still own the same amount of coins. (Harmat and Molnar)

Rest of the mechanism of coinjoining is out of scope for this thesis due to their extremely technical nature. Therefore, anyone wishing to learn about coinjoining should read the ZeroLink proposal to understand more.

G. Scaling Bitcoin: The Lightning Network

As transaction on the Bitcoin network began slowing down due to transaction congestion as there was more demand for transaction throughput, users became unsatisfied with the speed of the transactions. When many users attempt to transact on-chain, it takes a bit of time for miners to process all blocks before some transactions can be processed also. It is often the transactions with higher priority or larger size that cannot fit into one block due to limited space. Multiple proposals were created, that we already

touched upon before in the Bitcoin Nodes section within this chapter, that resulted in a long civil war within the space in 2017.

The Lightning Network is a recent Layer 2 invention that utilizes bi-directional payment channels to allow users to route payments. This makes it possible to send almost instant payments to other users. It was created as a solution for solving the very difficult task of scaling bitcoin, because blockchain systems are nearly impossible to scale. In order to send payments, users must allocate channels to others that allow them to make transactions via routing, and payments can go from point A to B through a network of participating lightning nodes without the coins ever being exposed to the possibility of theft or loss. Lightning Nodes that route payments can collect fees for making the transaction of a payment possible. (Antonopoulos)

The term “#Reckless” was created, because as the network started operating people began to use it actively, although the Lightning Network is far from being finished or without critical bugs. Although stable and operational, it can already handle transactions. The Lightning Trust Chain (#LNTrustChain)⁴¹ was started by a pseudonymous Twitter user Hodlonaut who started passing around amounts of bitcoin to users who then passed it onto another, increasing their total amount over time. The point of the Lightning Trust Chain was to promote the use of the Lightning Network and show that it is functional and can handle transactions to places all over the world. The torch took 292 hops reaching the total amount limit of 4.29m satoshis, and as the last hop, it was symbolically donated to @btcven, a charity organization helping people in hyperinflation as it struck Venezuela.

The success of the LN trust chain has shown that the system is already functional, and it can just as easily go peer to peer between users as on-chain bitcoins, with virtually no fees right now. Although in the future fees might increase as the lightning network sees adoption increasing. Today there are a total of 4560 Lightning Nodes with over 30628 channels open. (Acinq)

Since now we can see that Bitcoin is protected by a line of robust technical backing, we must take a look at its underlying social layer that further enhances its protective capabilities. Only by that we will have the full picture of what is happening, because it is not a lone technology that enables these processes and accelerates them. Bitcoin alone is clearly incapable of protecting itself against all forms of attacks. The next chapter will explain the social organizations that are built around Bitcoin and actively advocate for its usage, adoption and education in the space while attempt at the same time to protect the network against most forms of social engineering attacks targeting it.

IV. The Social Layer of the Bitcoin Ecosystem

One of the most important aspects of Bitcoin is the social organizational aspect of it. Bitcoin in this sense is unique, because no monetary tool has ever enjoyed the protective care of its users more than this programmed tool has. The diverse creed of people that gather behind the digital currency is immense. For human beings to unite under the flag of one monetary standard that cannot be censored is unique. This organizational ability has shown us that Bitcoin relies not only on miners to protect the network and on nodes to keep the ledger of the Bitcoin blockchain secure, but also on the protection of those who use it, who hold value inside units of bitcoin. These individuals are the guardians of the network because Bitcoin

rewards them with immense freedoms and liberation from forms of oppression. Those who value these granted freedoms are steadfast to offer their time and skill to continue advancing forward Bitcoin. On the basis of voluntary association, even developers give their free time as service to the community by developing Bitcoin, continuing to provide it with ideas and improvements to make the protocol more stable, safe, and secure to interact with. Some individuals go as far as to sacrifice their own personal safety and financial wellbeing just to help Bitcoin bring about its promise of total liberation.

In some countries, the usage of Bitcoin can be an extremely dangerous activity, especially where social liberties, protections and public safety is not present. It is common that interaction with the Bitcoin protocol can bring about the dangers of physical harm and even the possibility of death. A bitcoin developer called Jameson Lopp was swatted⁴² once due to his affiliation with and professional opinion on the development of Bitcoin, namely, his home was raided by armed police. Other holders of bitcoin were abducted in Ukraine to extract their bitcoin holdings by force, and later ransom was apparently paid to his kidnappers for his safe passage. (Polityuk) As more humans observe value behind units of bitcoins, the chances of crime increase exponentially. Since usage of Credit Cards lowered crimes originally due to no physical cash was anymore necessary to access funds with the presence of credit, physical crime targeting physical cash has decreased, but instead cybercrime has proliferated. Bitcoin in this sense is unique because it can raise back physical crime targeting users of bitcoin. Since Bitcoin is permissionless and transactions on the bitcoin blockchain generally cannot, after 1-3 confirmations, be reversed, therefore this effect does not bring about the same protections as credit cards do, for bitcoins cannot be refunded in the case of theft. As Nation States will soon also begin to feel threatened by the liberational powers of Bitcoin, chances are higher that they will resort to physical violence to exert control over the dissenting population. As explained in *The Sovereign Individual*, even in western democracies, where the freedoms and security for individuals are given within a constitution, the chances of such actions can be expected as those in power become desperate to hold onto it.

The organizational capabilities of Bitcoiners are there in part to protect collectively, in a decentralized way, against such forms of attacks as members of the community develop protective tactics against such forms of potential attacks by not just state actors.

Individuals seek to remove control out of the hands of government and to educate others and organize. Ideologies were formed to create parallel societies⁴³ and organizations that seek to educate others and make the usage of Bitcoin proliferate within communities. The importance of educating users is also emerging as most non-users are very overwhelmed with the user experience provided by Bitcoin. As improvements are made on the user experience (UX) side of Bitcoin, the better the onboarding capabilities slowly become, therefore making it easier to access functions of it over time. These user experience improvements can be anything ranging from making transactions or making backups of our private key.

Since the actions of individuals seem to be motivated by some aspects of freedom, we must investigate these and see how these affect the users of Bitcoin, how these people function within the community and how these community organizations offer a protective net for the Bitcoin ecosystem. In the following sections we are going to examine these effects.

But before we proceed, there is one problem we need to face. Due to the nature of this space, its organization and the participating individuals, data is very scarce. Scientific research is already targeting these individuals to better understand how this space functions, how it forms connections. (Maddox, Singh and Horst) Therefore, our research methodology changes at this point in this chapter. We are going to heavily rely on empirical research based on observations and experiences. **Interviews will be conducted, and places will be visited to informally collect information. Further data will be collected by direct observations of interaction of users in the online space.** Since most **Bitcoiners are very privacy conscious individuals**, they often use pseudonyms or anonymous names they identify on social networks or in the real world to protect their identity against governments and third-party interests. We are going to respect these individuals and not interfere with their privacy, most names used as references are their respective Twitter handles or names they allow for usage.

A. Protecting Bitcoin through Social Organization

The Social Network, Twitter, is the main congregation of socially engaged, active bitcoin users. For those Bitcoiners who are regularly active, Twitter slowly became the norm to use that serves as an instant messaging service that can communicate short messages publicly like a micro-blogging site that allows the immediate publishing of information online. When these messages are posted, connected users can like or share them by re-tweeting these messages. Twitter has come to the forefront in interaction for Bitcoiners because of the instantaneous ability to immediately share messages and valuable information. Developers, users, miners, speculators, entrepreneurs, and others can immediately reach each other on the platform and engage in discourse. This is a very handy tool for Bitcoiners because it serves them also as a debate platform. There is a lack of hierarchy among Bitcoiners due to this instant accessibility of certain users. Whether it be Bitcoiners who started working on bitcoin software in 2009 or those who acquired enormous amounts of coins before the speculative events started, anyone can reach each other. This is an incredibly special aspect of the Bitcoin ecosystem, because anyone can interact with anyone. There are no inhibitions between users, no social status or rank matters. A new user who wishes to get started with acquiring bitcoin and who seeks information about its storage, can immediately converse with veteran users who are very willing to help others out with issues. Developers and programmers who are working on software are also very engageable, users who need help setting up node installations can rely on the community for help. Although, when someone wishes to set up something complex solution like a Bitcoin⁴⁴ full node, manuals are available. However, if that is overwhelming for users, they can also rely on the helping hand of other users and developers who are very engaging in assisting other users with such problems. Although due to the possibility of legal ramifications, users are often wary of providing investment advice to others. This does not stop Bitcoin users from recommending others to try out Bitcoin by acquiring some, either by exchanging, mining, or earning them. Some users provide large databases of knowledge materials online⁴⁵ with their respective links for newcomers that allow better education and risk assessment for individuals.

Nevertheless, Twitter was not the first place where discussions started happening about Bitcoin. The first discussions were held on the Cypherpunk Mailing List and only later migrated to the BitcoinTalk.org forums, since the Cypherpunk Mailing List is no longer around main discourse concentrated on the

Forums. Even today, with over 2.7m registered users there are active discussions ongoing on the site about Bitcoin and other alternative copies of Bitcoin. Satoshi Nakamoto used BitcoinTalk forums to engage interested users who wanted to try out his software. Development discussions are also ongoing even today on these boards where users review or debate certain proposed changes or ideas. Although as the website allowed others to post alternative ideas, the space quickly diluted with those who are not especially interested in Bitcoin.

On Reddit, the r/Bitcoin board has over 1.2m subscribers and is similar in contents to those of the BitcoinTalk forums, yet, here all the threads are within one board as per given feature of how Reddit structures posts. Posts can be up and down voted to give them more visibility.

Based on observations, Twitter is, in sense of engagement and information transmission, is much more relevant in the bitcoin space, while the the BitcoinTalk forums and r/Bitcoin on Reddit are slowly becoming less important even as more users are attracted to the other platforms. Twitter's underlying matching and curating algorithm is partly responsible for this ability to connect better, since connected users on the platform will see content displayed from those who they follow and those people's interaction with other users, therefore engagement can be better created and is faster among users. Localized communities can have hashtags and other messages trending, as users retweet messages, they get displayed also on their page that creates further extended reach for content and communication. Due to the engagement forms within this given segment of Twitter and because of their connectivity, Bitcoiners began calling this part of their social-media space as Bitcoin Twitter.

It is not by chance that socially active Bitcoiners congregate on Twitter, for it provides them with a special ability to protect the social layer of the entire Bitcoin ecosystem. These are important matters, because they give protection to individual Bitcoiners and also provide protections against third-party social engineering attacks that target the Bitcoin Protocol itself. But Bitcoiners do not fully rely on one communication medium. Twitter is obviously not immune to cyberattacks, communication on its platform could be censored or manipulated. Although, disruption in its service would not interrupt individual Bitcoiner's ability to organize. Outside communication tools can also be used and since Bitcoiners actively network with each other they maintain their own personal space with those they trust. Some socially active members of the space are also competent at bypassing attempts of censorship to establish secure encrypted communication with other users. Satellites operated by Blockstream can circumvent censorship and can allow communication to continue.

Bitcoiners are notoriously decentralized, unevenly spread out across the globe, and they are in a sense aligned in political ideology. Although this alignment among Bitcoiners does not shy them away from debates. The community constantly creates debates among its own participating members that can often appear aggressive or toxic⁴⁶. But since Bitcoiners share fundamental basic ideologies (that basically unite them even within disunion), it allows them to actively organize and come to compromises.

i. "There's Bitcoin, and then there's Shitcoin."

Since the spread of alternative copies of Bitcoin started, curiosity led some people to give them a try, since many of those copies have portrayed themselves as a viable alternative that is better and more “superior” compared to Bitcoin. As most of these coins slowly turned out to be a scam or a pump and dump scheme that only attracted investor funds that later stole funds via an exit scam, Bitcoiners slowly began calling these alternative coins as “shitcoins”. This effect went as far as in 2019, Republican U.S. Congressman Warren Davidson on a hearing related to Facebook’s digital currency project, called Libra, included the term: “*There’s Bitcoin, and then there’s shitcoin.*” With that, Warren essentially questioned the quality and feasibility of alternative coins, similarly like how Bitcoiners refer to them with the term.

As shitcoins began to spread, Bitcoiners began calling out these projects and their developers actively. These activities are essentially messages targeting users of shitcoins about the dangers of investing into these currencies. The 2017 ICO (initial coin offering) craze created many pump and dump tokens and scams that created multi-billion dollar losses for unaware investors. Investors who purchased Bitconnect (BCC) tokens saw their investment evaporate as a Texas State Securities Board ordered Bitconnect’s to cease and desist, since Bitconnect was a multi-level-marketing pyramid scheme.

Since the belief spread that anyone can create his own better copy of Bitcoin, over 10000 copies were made so far that proposed to change functions of it or serve other purposes with its “blockchain” technology. Since the sheer existence of these coins is based on the underlying factor of human greed, their efficacy and future survival is questionable. The book written by Melania Swan titled “*Blockchain: Blueprint for a new Economy*” fully describes all “potential” applicable fields of “blockchain” technology, portraying them all as viable solutions that might come about and change the world. At this point, we must ask the question: If we are going to have a cryptocurrency that everyone is portraying as a viable solution to replace Bitcoin, then what is it that prevents others from creating a new alternative that also replaces that replacement?

The answer here is that, **this is impossible**. Those who claim otherwise are outright frauds (or are ignorant) who seek to develop or sell such form of solutions that seek to- or will eventually cause economic damage to others.

The way we can prove the single currency statement as a fact is this way: If we have multiple competing currencies, it is impossible in a long term to uphold their efficacy within competition because one will eventually become far more superior, and if we can keep on inventing new technologies then the invested amount of fiat value will evaporate by that causing massive losses for investors and users. If this is a possibility, then every cryptocurrency is a Ponzi scheme because when a new currency comes with a better solution, then only those will be able to profit who exit first into the new currency when the other is about to collapse, with that destroying the investment of other investors.

The existence of shitcoins is basically a **form of attack against Bitcoin**. Shitcoins are actively seeking to syphon stored value out of bitcoin in order to prop up the price of their coins. Often these coins have pre-mined amounts allocated to users or sold via an Initial Coin Offering, those participating in an ICO often exchange bitcoins in return for other coins. Later these bitcoins are sold by the creators of these shitcoins and used for personal purposes.

This problem of shitcoinery is an actively targeted area of Bitcoiners to further educate users and show them that there's nothing else behind these coins other than scams and frauds who only seek to get rich quick. But because there is very little understanding how value functions and many people only want to make money by trading them, this is a never-ending battle.

Nevertheless, many academics in the Information Technology field claim that alternative currencies have efficacy and since some of the top trading shitcoins have unique technologies behind them that, as they claim, make them viable in comparison to Bitcoin. (Seres) Notably, it is a belief among them that "Bitcoin is the MySpace of the cryptocurrency space." (Seres) with that implying its impending doom, that it will be pushed out of "competition". But the underlying problem with their misunderstanding is the instilled understanding of competition that enables this form of thinking. Since those who are researching alternative technologies think that they can create new innovative solutions that can compete against other products, in this case create the new "better" Bitcoin. It is not possible to replicate the social organization, economic capacity, trust and security of the Bitcoin Protocol in any form.

The fact that there have been no major 51% mining attack⁴⁷ against other shitcoins, for longer periods of time, is just a temporary situation that might evolve in the future as Bitcoin's mining increase and more people will be looking for ways to obtain scarce bitcoins.

This formality of rejecting shitcoins has created a new term within the Bitcoin space, called as Bitcoin Maximalism. This term basically refers to the fact that there are users who avoid all forms of alternative currencies since they do not believe in their capabilities to function properly or to maintain value over a long period of time. Similarly, the term of Toxic Bitcoin Maximalism was created to include those who are completely rejecting all forms of shitcoinery. In the next section we are going to explore this topic further.

ii. Bitcoin Maximalism⁴⁸

The underlying aspects of Bitcoin Maximalism are actually important elements of this organizational capacity that Bitcoin grants for Bitcoiners. The distinction that we can make here between simple users and socially engaged users (Bitcoiners) corresponds to the capacity to go to lengths about educating others about the actual capacities and features of Bitcoin and its ecosystem. This is a form of moral consciousness of users to guide others towards adoption and usage of Bitcoin and heeding of others from alternative solutions that proclaim to be better than Bitcoin. One alternative form of it is Toxic Maximalism the proponents of which are very vocal about their views of Bitcoin, similarly like that of Maximalists, although their discourses with users are not usually constructive due to their educational conversation abilities often resembling that of internet trolls. Derogatory terms and memes are often used by them to communicate their disagreements with others, even among themselves within their own circles.

Bitcoiner's educational activities often involve telling other non-Bitcoin users that they are going to lose their money, or that they are investing into scams that only serve the interests of its creators. The issue of constant theft and scams prompted the community to evolve a rejecting stance towards those who promote such alternative currencies. The sheer size of generated communication posted onto a Telegram

Channel called as “Rekt Plebs⁴⁹” puts on display these losses and questionable activities of other users. Although, the Rekt Plebs group is not especially consisting of Bitcoiners, the main point of the group at this point is to promote the dangers of speculation. The group’s activity seems to promote a sense of understanding of what is the actual result, most of the time, of reckless investing. Since most of the time, investment into alternative solutions (that promote themselves as better alternatives of Bitcoin) result in major loss of investment. Communities built around other solutions either do not have enough users and mostly consist of developers or they are filled with fake accounts (like bots) to make the group seem more popular or populated. These deceptive activities can usually be observed on solutions that especially exist only to scam users into believing that these are working products.

The actions of users during the first Bitcoin Civil War (Block Digest), that ended with the activation of the User Activated Soft Fork (UASF) during the block size increase proposal, can be partially labelled as a form of maximalist behavior norm that seeks to protect the network. As explained in a previous chapter under the section called “Bitcoin Node”, the collective actions of users (who had full nodes running) were able to prevent others from enacting changes on core functions of Bitcoin. Since the proposed changes were that of the interest of larger interest groups that had financial aspirations, they attempted to push through changes that would have changed Bitcoin’s core features. These feature changes would have put these actors into a superior competitive position compared to others if these changes had succeeded.

Without active users within the space, it would have been impossible to protect Bitcoin against it.

Maximalism might not be a term that everyone is actively associating with, but the interest to protect Bitcoin completely falls within aspects of forms of Bitcoin Maximalism. User’s individual interest in Bitcoin’s success essentially prompts them to protect and ensure Bitcoin’s uninterrupted operation. This is unique because no government backs Bitcoin, it is a software run by other individuals that form a network that communicates with other elements of the protocol through the internet. It is entirely unique that this software enables this form of social organization, both in the real world and on the internet.

iii. Pseudonymous Bitcoiners

The social space of Bitcoiners is remarkably interesting because of a prominent level of privacy extremism⁵⁰ that is present within it. Many people who interact online often use pseudonyms or anonymous names that seek to protect their privacy and personal safety. To better understand these individuals and their capabilities, we should take a quick look at some of these differences between anonymous and pseudonymous Bitcoiners.

Anonymous online users often do not wish to involve their real identity online at all, they protect it by using borrowed or invented names. Anonymous individuals often can change names or keep to one to be recognizable within a given social network. These individuals often attempt to avoid outside communication with individuals and avoid socializing in the real world with others with similar interest, except if proper protections can be achieved to conduct these interactions.

Pseudonymity is not much different, people chose invented names that they then keep for themselves as a form of personal identity in the online space or outside of it. Pseudonymous individuals often seek

connection with other users within online space or even outside, like in conferences or meetups. One feature of pseudonymity is that it can end in the outside world or continue without impeding on abilities. The necessity to protect the person's recognizable features is no longer required if the individual is within a space that ultimately shares interest across all individual participants.

The difference that we can see here is that anonymous users will often decline to participate in groups that share closer associations among members. They are more reluctant to open about their persons and with that limit connectivity to just the primary interests and activities of their online presence. If anonymous users reveal information about themselves, then the quality of their anonymity degrades permanently. If an anonymous user would be targeted, the protecting capabilities of the network would be less effective on these individuals because little is known about them. Since this form of identity protection comes with the greatest maintenance costs, it can provide privacy and security, if it is properly maintained⁵¹ by those who are anonymous. If an anonymous user's identity is compromised, there is no way back, the person must either abandon it and change to a new one or stay potentially compromised.

Pseudonymity on the other hand behaves differently in this situation and can be much more flexible. Pseudonymous users do not experience social interaction limitations like that of anonymous users, each individual decides about her level of personal trust that allows these connections to form. Recognizability is much higher and the network effect provides unhindered protective effects of collective actions. When an individual is compromised, the perceived negative effects of it is less severe, therefore it is not necessary to abandon pseudonymous personas. Since here a pseudonym only attempts to protect against the initial general knowledge of one's identity and not the total protection of it, the effects are perceived not as severe. A pseudonymous person might be known by others personally or in private life, therefore it can also relay this ability of identity protection onto others, which is not necessarily a burden. Although, from that point on we must rely on the other person's ability to protect our identity. Anonymous individuals can not establish such intimate levels of trust formations with others in comparison to those pseudonymous.

Pseudonymity is not necessarily a counterbalance against state sponsored surveillance, since governments can use investigating tools or cyber warfare tools to find out the identity of certain users. Although the usage of VPNs and that of Tor is certainly just as popular, pseudonymity only protects against other individuals and serves as a practical insurance against posed threat by others on one's privacy and personal safety.

Pseudonymity is also an excellent tool to remove all inhibitions that might impede on effective information sharing among individuals. Information sharing essentially becomes free of inhibition, lacks control and all forms of accepted norms. Some might argue this can create rampant intolerance, racism, and extremism, which might be correct because these individuals do not have to abide by the accepted norms. But on the contrary, these individuals are much more efficient at communicating ideas, forming connections and organizing. Most socially engaged Bitcoiners also do not wish to abide by already existing social norms because they perceive them as part of the given problem that either enabled or was created by elements of high-time preference.

Individuals who do not display their real-life pictures and hide behind masks are often more inclined to tell the truth, while they are also more inclined to troll others online for their perceived negative actions. Pseudonymous users are also less inclined to brag online about their fame or use their achieved online status as a tool to negatively influence others, rather on the contrary. Countless conversations can be found both on Reddit and Twitter in which pseudonymous Bitcoiners are educating other users about Bitcoin, its safe usage, and its features.

We can therefore establish the fact that pseudonymity is a useful tool that Bitcoiners utilize to enhance the safety of their general online presence and, by being able to associate much closely within the online space, they form much stronger connections than regular named users. In the next section we are going to look at a much distinct form of Fukuyaman trust formation and individual association that is related to this section, because a large majority of its participants are almost all uniquely pseudonymous.

iv. The Bitcoin Plebs

Online spaces for Bitcoiners discussing their views and opinions about Bitcoin are usually public spaces where everyone can view their opinions and ideas. It was a common trend among Bitcoiners that alignment alongside their original goals of Bitcoin adoption, usage and promotion had no other social association-like formations (other than real world Bitcoin meetups). On Twitter, users can send private messages, but those are also reliant on Twitter's Terms of Service and Privacy Policy and they are not overall convenient. If an account would get terminated, a user then loses the ability to communicate with others. Some users also began using alternative applications to make communication possible if a service would be unavailable, some of these were like Telegram, Keybase and Signal. As Bitcoiners slowly formed more closer ties with each other, direct reach to each other has slowly become a necessity, as well as availability to receive messages from anyone. But not all users are so enthusiastic because some claim that those services are centralized and usually can compromise the IP address of a user. Especially voice communication applications are not often used by those wanting to protect their personal privacy.

The Bitcoin Plebs is one of the most notable case of a small Bitcoiner group that seeks to bring others closer together into a more focused environment where they can talk, exchange ideas, debate each other or organize within the greater community. This group was the byproduct of a response to an attack that outside actors perpetrated against a fellow pseudonymous Bitcoiner.

On the 11th of April 2019, a pseudonymous Bitcoiner, called Hodlonaut, has deleted his social media accounts without leaving a reason. Bitcoiners within the space immediately began speculating about what had happened because earlier Hodlonaut deleted his Telegram and Discord accounts and was already unreachable on those platforms. Soon after a news publication was posted online by a media outlet owned by Calvin Ayre. In that post it was described that the owner of the outlet had placed about 5000 dollars' worth of Bitcoin SV (BSV is a forked copy of Bitcoin Cash, which is also a copy of Bitcoin) onto the head of Holdonaut, in order to have his real-life identity compromised. Hodlonaut previously had been a vocal critique of Craig Steven Wright⁵², who claimed to be Satoshi Nakamoto himself. Craig Wright previously asked his business partner Calvin Ayre to de-anonymize the pseudonymous Bitcoiner to be able to sue him in UK Courts.

As information quickly spread about the news online, outrage has spread across Bitcoin Twitter. Everyone was outraged about the attempted attack against a fellow Bitcoiner and waves of angry posts were made targeting Calvin Ayre and other BSVERS who were associated with Craig Wright or Calvin Ayre.

Users soon have begun using hashtags on Twitter like “#WeAreAllHodlonaut” and “#CraigWrightIsAFraud” to voice their support and sympathy towards Hodlonaut. Bitcoiners and businesses, that are building onto the Bitcoin ecosystem, (like that of Media Outlets, Commercial Businesses, etc) have changed their avatars to that of Hodlonaut. Hodlonaut’s avatar is that of a cartoon astronaut space cat with different Bitcoin-oriented motives on its uniform that symbolize previous important milestones⁵³ within the Bitcoin community’s life.

Users all over Bitcoin Twitter were outraged and by changing their avatars they began signaling to Hodlonaut’s attackers’ in a comparable way like that in the Spartacus movie where everyone who were captured by the enemy stood up alongside Spartacus to say that they are also Spartacus to confuse the enemy. They have also started a fundraising to support Hodlonaut’s legal defense, a bitcoin donation site was set up where users amassed over 2 BTC (at that time over \$20,000 US dollars) to provide legal counselling for the pseudonymous Bitcoiner. These events lasted for about 2 months until the eventual return of Hodlonaut onto Twitter.

As a response, Bitcoiners began organizing on Twitter within group direct messages that quickly outgrew its upper 50 user limit and they had to move onto the popular chat service, called Telegram, where they opened a group called as the “BitcoinPlebs”. The original creator’s goal was to organize and provide direct communication connections and a place for everyone to discuss anything. As of today, the group still operates as an open group that anyone can join, whether one be a Bitcoiner or someone who wishes to learn more about it.

Early members began claiming certain morals as group authority that they took as a personal trait of those participating in the Bitcoin Plebs group. Some of these were the following: The avoidance of influencers on Twitter, those who try to influence individuals about acceptable actions or other activities related to buying Bitcoin. They claimed these individuals often sell (or the word used by them “shill”) third-party products or mandatory KYC exchange services. They proclaimed to be the “plebs” enjoying total equality among members, independent of social status or amounts of bitcoins owned, because they are middle- or low-class to that of elite Bitcoiners who have been in the space and have larger amounts of bitcoins. They also proclaimed to be free of selling or promoting products that do not adhere to the norms of Bitcoin Maximalism. They also aim to be ideologically pure through their participation and skin in the game, both active investment in Bitcoin and through long term “hodling” of bitcoins. (Taleb, Skin in the Game)

Most of the users within the Bitcoin Plebs group can be classified as a Toxic Bitcoin Maximalist.

Bitcoiners often face problems related to trust, because not everyone can be fully trusted, and opposing political views or arguments about how Bitcoin should go ahead often serve as something that violates these forms of trust between individuals. These trust related challenges can happen daily among Bitcoiners, but it is an important aspect of social capital building, because it allows individual participants to see who they can trust and whom they can enter voluntary associations with.

The Bitcoin Plebs is more like that of a fraternity organization in this sense because trust is constantly enforced through the common morals of the group. This allows users to associate more easily and later to enter further associations with others as they explore the boundaries of their relations.

The group previously had splinter organization forming due to disagreements between certain Bitcoiners (or “plebs”) who seek to enforce different rules or moral authority. The group called Taco Carnivore Bitcoin Plebs was formed, being much more hostile towards those who did not adhere to the unwritten code of Toxic Bitcoin Maximalism. Although no massive negative impact was created because of the formation of the splinter group, some members still visit both group chats on Telegram.

Both groups are very casual, every day topics are shared in their group. Both groups are still available on Telegram and can be publicly accessed.⁵⁴

The main important lesson this organization capability shows us is that Bitcoiners have reached a higher level of understanding of necessity about voluntary association. Since individual users alone would not be capable against threats, now as part of a group can be more powerful. As the space slowly evolves, connections form and trust build up among users, active association slowly seems to become a necessity. It is apparent that users who band together have a higher total effect within the community against aggressive forms of attacks that target the social layer of the Bitcoin ecosystem. It is only a matter of speculation now how powerful these forms of associations can become in the future as they slowly reach out into the real world where potentially these individuals will later form real life friendships, partnerships or business ventures. It is also now probable that as the value of Bitcoin rises, this will grant more abilities for these individuals, expanding their line of arsenal to provide active protection for members of the greater community and for Bitcoin. (Fukuyama)

The existence of Social Capital has played a key role in enabling this ability of voluntary association. As Bitcoin’s online space of users keeps expanding, the social formations among users also develop. Francis Fukuyama’s book called “*Trust: The Social Virtues and The Creation of Prosperity*” clearly explains some of these expected ways of trust formation among human beings, and we can make a clear correlation between these activities and those among the Bitcoin users. In his book, Francis Fukuyama pointed at the Internet’s capability to start processes towards decentralization and limitation of governments through society’s expanding abilities to control its own freedoms. He referenced Friedrich A. Hayek, claiming that these processes will eventually lead to the liberalization of markets, their restructuring and new formations of social structure among members of society as technology keeps advancing. Social capital allows individuals to network and establish relationships with one another to promote economic growth and enable socio-political organizational abilities. (Fukuyama)

Without the presence of social capital, no form of cooperation and associations would be possible within the Bitcoin space among users. Based on already existing evidence, we can carefully conclude that this effect seems to **derive from the inherent ability of Bitcoin to lower time preference**⁵⁵ which, as an effect, **enables spontaneous sociability**⁵⁶. (Fukuyama)

v. Bitcoin as Socio-Political Basis for Cooperation

As today's world is ever increasingly becoming polarized along social and political lines, damage can be easily observed in the world in relation to it. The processes described in the introductory chapter of this thesis titled "*The Great Chasm of Political Polarization*" clearly shows us a degrading world view that is rife with corruption and hard-liner political interests. Since the effects of Monetary Nationalism deeply affects political organization, it also affects social connections between individuals through it. This is apparent in our world today because of constant political polarization and isolationism of individuals who do not conform to certain political standards of society. This form of rejectionism of alternatives which was instilled in society through the last century, that politicians used to enforce bias through society to keep certain political interests within power. Either by using the Media or other forms of communication tools to keep individuals locked in deep in their own political sphere and conditioning them towards the total rejection of other ideologies. Since politicians are the greatest rent-seekers within society, those who get into government essentially enforce that upon others. This has directly led to Monetary Nationalism becoming a standard that nobody can change because then countries lose their competitive edge. (Ammous)

But based on observations, Bitcoin can bridge this problem for us, because it removes inhibitions towards individual free thought. Since Bitcoin also enables social capital, users began looking for allies for their cause, which in effect lead to seeking of common grounds based on shared beliefs within a new open monetary standard. This effect did not lead to differences in political ideology being accepted by others, but it has effectively created a bridge between opposing political ideologies that allowed them to communicate and organize towards a common goal that Bitcoin proposes. (Fukuyama)

This common ground of cooperation was found within the fundamental basics of libertarian socio-political thought. The protections of liberty, individual financial freedoms, the free market, and personal privacy has become an especially important common factor.

This is an important effect because the protection of Bitcoin is a higher goal of all individuals. The freedoms that Bitcoin restores prompts others to cooperate more and tolerate other's views, as long as those do not seek to collectivize them or enforce political thoughts on them. Individuals within the space are not discriminated based upon their race, religious beliefs, ethnic origin, age, or sexual orientation. They instead judge them based on their actions, participation, and contribution to the space.

The violation of these beliefs and discrimination through other means are not very well tolerated by Bitcoiners.

The participation of users within the community space also strengthens individual connections and fortifies beliefs and potentially also moral standards. Since most Bitcoiners usually perceive that Bitcoin is constantly under attack at every given moment, a sense of vigilance became apparent which prompts for active organization. Previous events described in the "*Bitcoin Node*"; "*Bitcoin Maximalism*"; and "*The Bitcoin Plebs*" sections provided evidence for the deriving effects of these major conflicts⁵² that happened within the Bitcoin ecosystem. These events are especially interesting because certain effects (like that of common experience of perseverance and success after a major battle) serve as a form of (not so virtual) front-line experience for Bitcoiners. This creates camaraderie, shared bonds of trust and cooperation among individuals. As Bitcoiners also meet each other in the real world, these connections grow even

stronger over time. Some usual brandish Bitcoin related or themed clothing in the real world when attending Bitcoin conferences or meetups, which show that a separate cultural formation is also possibly present. It is also possible to find presence of music and art related to Bitcoin that further supports this claim.

As we can see, the social organization of the Bitcoin ecosystem is a very robust formation. It uses technology and social organization to protect it in situations which Bitcoin is not designed to protect itself in. The individuals also protect themselves against interference, they use technologies that protect and liberate them to ensure their uninterrupted participation. Individuals enter voluntary associations or if not, they form strong bonds among each other to be able to achieve that. Since Bitcoin is still a relatively recent technology, the liberating effects are only getting stronger right now. It is in the common interest of its users to protect it and to support Bitcoin in achieving its revolutionary potentials. Individuals will be able to liberate themselves and be able to change the world, permanently, only by that.

In the next chapter, we are going to conclude this Thesis and provide a full collection of findings and observations that support or invalidate claims or theories.

V. Conclusion

As I have embarked on this journey, the question of trust always lingered around like an unknown element that seems to hold the answer for the question of why people are using Bitcoin. Through my research and my travels around Europe in 2019, I have managed to gain insight into the hidden secrets of Bitcoin and Bitcoiners. The original goal of this thesis was to find out whether a link between trust and adoption exists or not, and half-way into the research, the conclusion about the question have formed.

It is a consensus and belief among users of Bitcoin that there is a trust factor at play, a type of loss of trust that somehow drives individuals towards risking their money by acquiring and holding bitcoins long term. Such a young technology has driven financially very conservative users to take part in high-risk speculative activities where they hold a digital currency like bitcoin long term. Although, their reasons about their decision varies to great extent.

Without reasonable doubt, it is not possible to prove whether there is a direct trust link in bitcoin adoption. The decentralized and widely spread nature of Bitcoin and its users make it extremely difficult to collect accurate data that reflect the given situation properly and making predictions based upon it is nearly impossible. It is a limitation of this thesis that we cannot fully shed light onto this question, but neither can we deny the actual role of declining rates of trust in adoption. Therefore, we can only carefully refer to the information we have right now, that adoption is continuously growing, and that there might be a strong link between the abuse of trust and bitcoin adoption.

Some users of Bitcoin argue that the contrary happens, that as more users are entering Bitcoin, their trust is globally challenged, and it lowers their ability to blindly trust others. The so called “Don’t Trust, Verify” term shows that users shouldn’t trust but instead actively verify the information themselves, which results in less initial trust and more inhibition unless the truth content of information can be determined. This gives rise to the re-assessment of present reality, because **the de facto world view is now**

challenged by Bitcoin. As people embark onto the journey of learning more about Bitcoin, they gradually manage to find out how the financial system works and discover its present flaws. Since knowledge about the financial system and how money function is not especially a well-known subject within society, the discovery of the facts can shock those unaware. This creates an accelerated destruction of general trust that prompts people to attempt to verify the truth content of information that is out there. The avenues of doing that is to read about these, speculate actively about their inner meaning and to exchange information with other Bitcoiners. This directly enables **the questioning of reality**. Since Bitcoin can form absolute forms of truth, it creates an imminent need to achieve this also in those spaces that can only return perspectival forms of reality.

Also based on the findings in the Edelman Barometer, support for a continuously declining trust cannot be established, because rates of trust can go higher as public opinion changes over time.

It is not possible to quantify or measure the adoption of Bitcoin, because of the nature and origin of its users. They are heavily decentralized, widespread globally and only a fraction of its users are online in cyberspace.

Although globally it is difficult, regionally we can measure the rate of adoption. This is although incomplete, because we will receive back information that does not cover most users and from region to region this can vary greatly. Most Bitcoin users are not interacting online, they often follow the news but do not engage in the public discourse for a wide range of reasons. Only later, once the space sees enlargement of its userbase, will targeted surveys become more relevant.

As to how this thesis has developed over time, the original hypothesis began evolving as added information was studied and more new information surfaced about Bitcoin, with that directly altering the course of the research and the contents of this Thesis.

This Thesis so far concluded with the following findings about Bitcoin and its effects ever since its inception:

1. Bitcoin is a form of money
 1. Because it holds value independent of governments, it cannot be inflated, the system is designed and has evolved to be able to defend itself. One bitcoin can be easily broken down into its smallest fraction of value and because of its digital nature can be transacted without the interference of a third party.
2. Bitcoin is a peaceful revolution
 1. The decision made by society to change to an alternative financial system is in fact a peaceful revolution. It does not require the users of the new financial system to go out and protest, because the new system can take over and supersede the already present legacy financial systems with extraordinarily little physical input. The change of system would lead to fall of governments and the total transformation of statehood with a transition towards service offering libertarian governmental structures.
3. Bitcoin generates organic culture in its initial stages of adoption

1. Due to its revolutionary nature, bitcoin in its initial stages uniquely generates anthropological evidence of its existence. It organically creates arts, music, culture, and social organization. No financial tool ever before created organic culture, it is unique in form and organization within human history. Previous monetary metals were just objects within culture and not aspects that initiated culture generation or transformation.
4. Bitcoin bridged the left and right political ideologies
 1. Due to its apolitical nature, Bitcoin seems to have enlightened political opponents and created consensus among disagreeing sides on the political spectrum that have united both liberal and conservative users of Bitcoin. Their ideology is debated and reached through consensus and held on a newly formed libertarian basis. This basis allows the spectrums to cooperate and reach common goals that bitcoin have enabled for them. For example, the unrooting of political corruption, transformation of the monetary tool and the cessation of the central banking system.
5. Bitcoin liberates the individual
 1. Due to the censorship resistant nature of bitcoin, full financial freedom leads to a fulfilled free individual who is responsible for his own individual self. Because now an individual can transact without interference, the possibility of entrepreneurial spirit is now unleashed, with its full positive and negative consequences. These freedoms accelerate the need for the expansion of other freedoms within society, for example with the spread of 3D printed weapons, the freedom for self-defense and protection of one's private property. Since Bitcoin is a digital monetary tool, but with physical storage requirements, it is exceedingly important to physically protect against unwanted physical attacks, therefore the requirement to expand protections of private property is a direct consequence of it.
6. Bitcoin made possible the separation between state and currency
 1. Because now it is no longer a government maintaining a monetary standard, but the social consensus of human beings through the added power of the free market, fiat money has become redundant and may become obsolete. The separation between state and currency is now a reality, human beings who agree on a given value of a bitcoin can transact freely without the interference of a state entity or a non-state third party.
7. Bitcoin makes taxation difficult
 1. Since the private keys and associated passwords cannot be taken away, taxation will be extremely difficult if human beings decide to refuse to pay taxes. Governments will have to incentivize taxation and operate it on a voluntary basis.
8. Hyperbitcoinization can potentially cause a hyperinflationary demonetization event
 1. A sudden increase in the stock-to-flow ratio of bitcoin can lead to established markets moving assets into physically settled bitcoin derivatives that could result in a catastrophic collapse in their valuation and therefore an astronomical increase in the price of bitcoin. This sudden market movement would be done within seconds, not hours or days and bitcoin would begin to gradually lose its US Dollar perceived value as more human beings establish it as a much more valuable monetary unit.

9. Bitcoin lowers the time preference of human beings
 1. Since human beings now able to re-evaluate their work's value production, they can observe that their produced value over time remains stable and they are able to afford more products in the future if they work harder for their goals. As human time preference lowers, immediate gratification of needs becomes less pressing and can be delayed to later obtain more superior services or products for the produced value. As more time is expended, more human produced value can be stored within Bitcoin, through which it can maintain its value permanently due to its non-inflationary⁵⁸
 2. It can also be argued that Bitcoin is an actual solution for high time preference that fiat currencies cause with their inherent inflationary abilities. As central banks often breach the trust of people, that, not to debase a currency, Bitcoin reinforces this statement and eliminates the possibility for an inflation after the block reward runs out. Since fiat currencies are so deeply woven into the cultural and organizational fabric of society, a high time preference environment is reinforced throughout its usage that penalizes those who attempt to function with a low time preference. Since, for example, savers would see their savings diminish over time because of inflation. Since a non-inflationary property re-introduces the incentives to savings, time preference lowers, and the negative effects of high time preference slowly dissipate.
10. Bitcoin re-incentivizes the aspects of long-term savings
11. As money becomes a much more stable store of value, it becomes more important again for human beings to save money. As time preference lowers over time because of bitcoin, the demand for loans will decrease. As of today, there are little in savings available for the average citizen, especially in Hungary and the United States. But since fiat currencies are bad store of value due to their inflationary property, they lose value quickly over time and their purchasing power decreases. But since bitcoin does not lose value, it serve as a primary savings catalyst for the lower and middle classes.
12. Bitcoin will re-accelerate the rate of global technological innovation
13. As time preference lowers, a re-shuffle of shareholders will lower company time preference. This will cause shareholders to enforce their own time preference expectations on the operation of companies. This will immediately lead delayed gratification of profit seeking, which will lead to normalized production, improved research and development cost allocation. This will create better products in the future and allow a company to operate more self-sustainably. The problem raised by Jonathan Huebner will be resolved and global innovation will resume to gradually increase over time as new inventions are created again in search of the new. More focus will be also put onto the production of life saving medications and the research of anti-biotics as the new shareholders of pharmaceutical companies will enforce more society conscious principles and morals based on their own low time preference.
14. Bitcoin will halt climate change and potentially reverse it
15. Since climate change can be directly led back to the increase in human time preference, bitcoin is able to reduce the effects of consumerism and put an immediate end to human overconsumption and end-user produced greenhouse gas emissions. Food waste will be minimized as consumption

will focus on savings and conscious spending of produced value. Less electronic waste will be produced since more efficient products will be demanded that do not break every year. Environmentally damaging production will be shut down, forcing the re-training and re-allocation of work force into different industries. More efficient, longer lasting, and environmentally friendlier technologies and products can become more profiting for companies as more consumers will be able to afford (and demand) those products over time as savings slowly become widespread again, with that more monetary capital is available by that time for their purchases in the future.

16. Bitcoin will radically restructure society and the way we live
17. Since the separation between state and currency has become apparent, a complete transformation of society is now possible. As in the early days of Bitcoin's inception, a mass value transition happens from wealthy individuals towards those who early on caught onto the revolutionary aspects of Bitcoin. These individuals are in a sense incredibly lucky and wield extraordinary mental capacity towards changing the world for the better with the help of Bitcoin. As the new intelligentsia once again becomes the fore runner and messenger of the harbinger of change, it becomes ever apparent that these individuals will help reshape society as we know it. Since taxation will be difficult, governments will have to reform healthcare systems, the education systems, and services they provide for members of the public. Upon a change of system, these institutions might become disrupted for periods of time, but as part of any revolution that brings about a societal change are considered normal. As responsibility now shifts towards the individual, entrepreneurial spirit can be unleashed and a reacceleration in capital production can be achieved. The social structure will also be re-shuffled because of the newly formed Bitcoin users who entered the space early in its inception. These individuals will be potentially at the forefront of this movement and play a key role at restructuring companies and forming new business with others from among their circles.
18. Bitcoin forces governments to turn into service offering institutions
19. As governments become unable to provide free services, they must transition towards a for profit (or voluntary) entity that serves the population. These services will make it possible for citizens to choose their countries, either in countries where there are better living conditions, reduced tax burdens or better business and work opportunities. As claimed in the *Sovereign Individual*, citizens will become solely responsible for their own wellbeing as governments will no longer be able to provide enough social safety nets for their citizens.
20. Bitcoin limits down government's abilities in waging infinite warfare through the inflation of the money supply
21. Since Bitcoin makes taxation difficult, governments around the world will come across the issue of lack of funding for wars. Soldiers will no longer accept payments in fiat currencies. In order for a country to begin a war, it will be required to tax its citizens first, for without taxation a government will quickly run out of money and will be unable to fund its war operations, potentially collapsing itself in the process. Inflation will no longer be possible as a tool to fund potential wars by warring countries, and citizens will highly be likely to seek making war efforts impossible.

22. Bitcoin's social layer defends the Bitcoin Protocol and its users against attacks
23. Social organization around the Bitcoin Protocol makes it extremely difficult for outside attackers to effectively engage the Bitcoin Protocol and its users. The prime examples of the UASF (User Activated Soft-Fork), #NO2X and the #WeAreAllHodlonaut events suggest that Bitcoiners have larger than average social capital. The UASF and #NO2X movements have shown that Bitcoiners can impede potential attacks against the Bitcoin Protocol that are questionable in nature and want to put other entities with self interest in more advantageous position. The problem was solved by using User Activated Soft-Forks on Bitcoin Full Nodes when node users demanded that miners follow their lead else face that their produced blocks will get rejected and their expanded electricity will be wasted in the process. The #WeAreAllHodlonaut movement saw the more socially organized members of the Bitcoin community to organize in defense of its pseudonymous members who are in a difficult situation threatened by outside actors for their anti-scammer morals. The pseudonymous twitter user @Hodlonaut received legal threats and later doxing attempts by Calvin Ayre who put 5000 US Dollars in form of BSV to find out the identity of the pseudonymous user. This resulted in Hodlonaut deleting his social media accounts and going dark out of fear for his personal safety. The community response was overwhelming as outrage was observed over their actions and users began changing their avatars to Hodlonaut's space cat picture to symbolically defend the user similarly like in the film featuring Spartacus where enemies were looking for Spartacus but his kins stood up alongside to confuse the enemy about the true identity of Spartacus. In response to the legal threat, a donation drive was organized to engage the serial scammer and self-declared bitcoin creator Craig Steven Wright who is a business partner of Calvin Ayre. The donation drive received over 2 bitcoins (at that time over 20.000 US dollars). This action has shown that Bitcoiners know no limits to their social capital and even the most dormant observer users were prompted to take defensive action to protect their interests.
24. Only one single version of Bitcoin can exist, no alternatives are feasible
25. Since the widespread usage of the internet only took about 27 years for reaching its current form to become an inseparable part of modern civilization, life in its current format would be impossible. Since bitcoin is a similar technology that operates on the internet, that requires users to upkeep the system, it can easily become just as inseparable part of civilization as the internet is today. A form of money that humans can use and agree universally on its price, that knows no national boundaries, gives limitless potential for global growth. Although some would argue that the technology can be improved upon and that it can be altered to create new forms of digital money, this is highly unlikely since human organization can only sustain one functional system that they universally agree on. The fact that the hash power of bitcoin reaches new all-time highs and alternative currencies barely reach a tiny fraction of it, seems to show that there is small appetite for securing other competing blockchains. Bitcoin's initial start can no longer be re-produced, and competitors are immediately exposed to the potential danger of 51% double spend attacks. This factor shows that it is not feasible for human civilization to upkeep multiple different competing monetary systems similar to that of Bitcoin.

26. Bitcoin will make it necessary to extend rights that make self-defense and the protection of private property possible
27. Since Bitcoin is a digital form of currency, it is especially difficult to protect it. Users must be in possession of their own private key to own and store bitcoins, and the protection of a private key against third-party inference is necessary. The spread of hardware wallets that can store the private key securely can isolate it against some forms of electronic attacks but not all, and the main problem that still stands is the physical protection of that secret. Electronic devices that are isolated from the internet can generate these secrets, they can be written down or stored on fire resistant materials that make them virtually indestructible, but they remain vulnerable to physical theft. The proliferation of 3D printed weapons and their easy access is a byproduct of self-defense and is intensified in its importance by making protection of private property possible for users of Bitcoin. This allows them to defend their wealth with the use of deadly force. Bitcoin is a permissionless sovereign money, it is not possible to revert finalized transactions, therefore it is vital to defend the secrets which allows us to access and manipulate stored value on the Bitcoin Blockchain. Since Bitcoin can be used to store any amount of dollars' worth of value on its network, potentially in the future, as the US Dollar value of bitcoins rise, physical attacks by governmental, non-governmental and individual actors will target those who possess bitcoins. Therefore, users of the Bitcoin Protocol will be more inclined to support the expansion or establishment of constitutional rights that allow individuals to possess and bear arms. If this is forbidden by a state and the given environment is deemed unsafe by those who use Bitcoin, they will be highly likely to relocate to other nations that permit the right to self-defense and protection of private property with the use of firearms.

We can also conclude the basic reasons of adoption among users. It can be easily approximated due to the public discourse within the bitcoin space on social media. We should differentiate between two groups existing within the ecosystem: speculative traders and long-term "hodlers". The following can be observed:

1. Financial gains are a complete priority among most traders, but not a complete goal among holders. a. It is observable that most of the Maximalists also prefer financial gains, but not always in the terms of fiat currencies but instead of gaining more bitcoins. Their rate although perceived to be small since most holders of bitcoin experienced losses when they began trading their coins speculatively. Although everyone still uses the US Dollar as a comparison medium for value, the focus has been on stacking satoshis.
2. Long-term holders can also have other primary goals while having financial gains as secondary driving factor. Some of these are the following: a. Use bitcoin as a store of value to circumvent the effects of inflation. b. To subvert government currency controls, especially in authoritarian countries like Venezuela where the local currency lost its value due to hyperinflation. c. And in some cases, to bring about bitcoin's revolution.

It is a conclusion that the last two mentioned reasons, namely, the anti-authoritarian and revolutionary aspects of adoption, will eventually merge and become a primary reason and main driving force of adoption in the future.

Bitcoin's previous driving factors are no longer present due to the perception of value formation that Bitcoin holds. Previously, between 2009 and 2011, users were more interested about the underlying technology and not in its possible monetary gains that a future appreciation of its value could bring about. This has been rapidly phased into the background as speculation comes to the forefront among users. During this period users destroyed countless bitcoins, either by accidentally deleting wallet data files, throwing out private keys into the trash or encountering a catastrophic hardware failure. At that time the value was so marginal that there was no such sense of loss present when bitcoins were lost forever.

The largest discovery of this Thesis is the interwoven effect that fiat currencies have on human behavior, which appears to naturally raise human time preference. This can be explained by the fact that fiat currencies are extremely well integrated into western societies and **there is no** (government approved) **usable alternative**.

The effect that monetary nationalism has on society, through fiat currencies, is profound and extremely spread in the developed western world. The main problem that enables this effect is the **lack of choice**. When in a supermarket, we are swamped with the endless line of choices that are different in quality, size, and value. We are not limited to one bank account, we have choices, we can go with an expensive bank or a cheaper one where we don't have to pay high monthly fees. Of course, these will have different drawbacks and different terms which the bank will serve us by. Even browser software monopoly held by Microsoft on the Windows XP operation system was deemed unfair by the European Consumer Protection Agency, it has ruled that Microsoft must provide usable alternatives that fulfill all necessary criteria for protecting users and providing an adequate level of choice.

Negative effects can also be observed when we remove the option of choice among consumer products. For example, rural American farms with limited infrastructure often face the fact that they only have one internet service provider that provides extremely limited, inferior service for consumers. Medical products that don't have alternative generic forms, often have higher prices, or if a pharmaceutical company has a monopoly or a patent on a medical product it has the incentive to ratchet up the price to produce profits. Similar has happened with the EpiPen and Daraprim in the United States. (Pollack; Rapaport)

There is a very similar effect in relation to lack of choice with fiat currencies. Due to state nationalism, the usage of currency is mandated by a sovereign nation. The sovereign nation exercises its right to self-determination and existence as a country through the issuance of a national currency. This is done through a national central bank that manages the currency and its issuance. When the currency is issued, then the usage of that currency is enforced by that sovereign nation's military.

When a currency has its stability manipulated, extremely negative effects can be observed. The hyperinflation of the German Mark and that of the Venezuelan Bolivar prove that there are direct consequences when the value diminishes from within a currency. Social structure breaks down and

occurrence of a revolution becomes a possibility. But these only become apparent when the effect of value diminishment is faster than how an economy can adapt to the changed situation and valuation of a currency. When a currency has its value slowly decreased, lack of savings becomes the norm among members of society, which in return accelerates the usage of credit. Consumer credit, especially in the United States, is an important aspect of participation in the economy. Banks often base their decisions on these credit ratings and set their fee structures and offers accordingly for individuals. The US Dollar keeps losing value and interest rates are ever increasingly cut, it becomes less feasible to save money. Since banks are operating under a total reserve ratio set by a central bank, the endless cycle of issuance of currency is accelerated.

The United States Dollar has lost over 95% of its value since 1913, and this is not a coincidence that correlates with the establishment of the US Federal Reserve Bank. As of today, inflation rates are marginally kept under control while the printing of money keeps happening to fund government operations by expanding the debt ceiling. When a currency loses this much of its value, extremely low rates of inflation can cause problems also. For example, this effect can be observed in the rise of the price of consumer products or in the loss of value of a national currency towards another currency.

The gradual decline creates an environment where immediate profit is necessary for the functioning of an economy, where everyone must produce money constantly and keep up spending. This is accelerated by credit lines where individuals can drive up their debt to be able to fulfill their immediately needs. The economy within an inflationary environment is designed to operate in a profit-oriented manner that seeks to gain profit by all means necessary. Shareholders demand profits from companies and because of that high-time preference environment were created to enforce the spending habits of consumers and to influence that further through company policy enforced by shareholders will and vote.

This directly creates overspending, defaults for individuals on loans and less economic stability for an individual to function within society. Since money is required for the proper functioning of an individual in society, safety nets providing individuals with fiat currencies further act as a destabilizing factor.

Next Stop: Terminus

“Change here to the Moon and beyond.”

The system we live in is designed to work like this since governments do not know other alternatives to be able to compete against other competing states. As of today, Keynesian Economics is taught all around the world in higher education as the de-facto standard of the basis of the global economic world order. If a nation attempts to step outside the boundaries of that system, then the consequences are immediate and will negatively affect its citizens. Since the rules of competition is based upon these standards, the participants must organize themselves along the lines that can keep an economy functioning while increasing the GDP constantly. It is not possible to determine whether this system was designed with malice, but evidence within this Thesis seems to suggest the fact that this system was engineered to keep members of society under control. We can also see that as the system was built out, the goal to become superior has become the forefront goal of countries. This is deeply rooted in the ability of the United

States to manipulate its currency and use its economic and political might to exercise control over the political order of the world. As the gold backing of the US dollar was manipulated slowly and then removed suddenly, it started off a cascade of events that keeps leading us towards economic bubbles and extreme polarization of society and politics.

The only solution that could solve this problem is to return to a monetary system that is based upon a sound monetary medium. But this is not possible anymore. Since a return to the gold standard could potentially give the competitive edge to a hostile nation that another might not want to happen, therefore, this becomes an impossible choice for a government. Return of the gold standard would also change consumer behavior, and a complete change of the economic model and how the world produces goods would be also required. Moreover, the possibility of a failure of such a process is extremely high if it is not professionally managed by a government. Communism's failure in the Soviet Union clearly shows that governments are especially bad at managing centrally planned economies and they are destined to failure.

One of the possible solutions for this problem is to abolish the usage of paper currencies all together and to return to an economic model based on bartering. But because of the advanced state of civilization where most human beings in western societies live in large population centers where land is limited, it is no longer possible to produce products to barter with them, except in the services sector. Therefore, a return to such a system is impossible.

The only alternative that remains to fix this problem is the total abolishment of the central banking system and the creation of separation between state and currency. Governments although would never allow such change to happen, because it removes too much power from them and places it back into the hands of the people. Therefore, the solution must come from the people who can initiate this change; only the people can bring about a global restructuring and reformation of the socio-economic-political order.

But fortunately, even if governments would not want it, this reformation of the world's socio-economic-political order is already underway as a direct effect of the digital sovereign money⁵⁹ that operates on the Internet under the name Bitcoin with the trade ticker BTC (or XBT). This process has reached the point of no return and can no longer be stopped by anyone. Slowing down the process is certainly possible, but just temporarily. If anyone would attempt to attack Bitcoin, one of the protective layers of its ecosystem will eventually enact mutations to the system (just like a virus would mutate through DNA proof-reading as it copies itself) and it will become stronger and more resistant to further attacks, incurring more higher costs and more time to make further attempts.

Any form of attack can target Bitcoin, but as long as there are people out there who are willing to acquire bitcoins and hold them long term, with that giving value for each individual coin, which is limited at 21 million coins, the effects of bitcoin will continue and will go on until Bitcoin eventually changes the world, permanently.

Due to National Central Banking becoming an obsolete institution, with that immediately phasing out Keynesian Economic norms, no further analysis of the trust problem (related to fiat money) is required, because *Bitcoin fixes this*.

Appendix 1: The Bitcoiner's Lexicon

Satoshi Nakamoto Pseudonymous programmer and cypherpunk, creator of Bitcoin. Has disappeared in 2014 and no plausible evidence exists that he ever attempted to communicate with anyone afterwards. His whereabouts are unknown to us all.

Hal Finney Hal Finney was the first recipient of bitcoins mined by Satoshi Nakamoto, he has worked and communicated with Satoshi Nakamoto in the past. The term “running bitcoin” was coined by him when he tweeted that he is running Bitcoin software for the first time. Hal Finney was battling Amyotrophic lateral sclerosis, after death was frozen by the Alcor Life Extension Foundation and his body is being cryogenically preserved for a potential later revival.

Hodl Hodl comes from a possible miss-spelling of the word hold, which means holding bitcoins in this context. Some users argue that the intoxication of a forum user on the BitcoinTalk forums were the origin of this coined term when he misspelled it, others claim that it is a complex acronym of “hold on for dear life” aka hodl. Hodl in this concept reached a form of cultural behavioral norm where users of bitcoin are expected to hold bitcoin long term to enforce the network effect on the price of bitcoin by removing bitcoin liquidity from exchanges with that tightening the order books that contain available traded bitcoins on offer. The basis of “hodling” seems in some sense to provide the basic price of bitcoin, because a bitcoin can be owned physically if someone is within possession of his own private key and can verify that his coins are present on those addresses associated with his private key.

1 BTC = 1 BTC This refers to the fact that 1 BTC will always equal 1 BTC because there is no central authority to inflate the money supply of Bitcoin. Therefore 1 BTC will always worth 1 BTC on the Bitcoin Protocol.

‘Sup Freaks A catch phrase used by Marty Bent on the Tails from the Crypt Bitcoin Podcast.

Sovereign Individual A person that is independent that of nations and not restricted by borders, a true free individual who is in control his own destiny within the free market economy.

Brrr It is the sound that a money printer machine makes when it prints new money. This have become popular during the 2019-2020- COVID-19 Pandemic. The United States’ Federal Reserve have begun its quantitative easing program in response to battle the global COVID-19 pandemic, this resulted in the creation of multi-trillion dollars and the expansion of the money supply. (IMRD)

Don't Trust, Verify. A techno-philosophical approach towards the verification of aspects of reality, not just within computer science. It heeds users of Bitcoin to don't trust information they see and instead go to extra lengths to verify their truth content by themselves.

Stacking Sats Stacking Sats was a term used by Marty Bent on the Tails from the Crypt podcast where he references the repeat purchases of bitcoins in its fractional units, satoshis as a process of stacking these units into larger stacks.

Toxic Bitcoin Maximalist Individuals who advocate for the rejection all forms of alternative currencies; they fully support the use of Bitcoin only. They advocate for the development of the technology and endlessly educate potential users about its use and efficacy.

Bitcoin Plebs Common ever day users of bitcoin, (mostly bitcoin maximalists), who reject ideologies spread by influencers on the internet. They support self-education and self-awareness in the bitcoin space. The Bitcoin Plebs group was started on Twitter in response to the doxing attempt against the pseudonymous bitcoiner Hodlonaut, the group later moved onto Telegram where it operates uninterrupted even today. The Bitcoin Plebs are active users of Twitter. Their group can be accessed with this link: t.me/BitcoinPlebs

Taco Carnivore Bitcoin Plebs A splinter group that decided to form a separate Telegram group after the decentralization attempts of the original Bitcoin Plebs Telegram group. Their members advocate for the total rejection of all forms “shitcoinery”. They often engage other bitcoiners also who they perceive as not adhering completely to the expected standards of bitcoin maximalism. This has led to many members of the group separating based on ideological lines. Most users in this group are also still members of the original Bitcoin Plebs group. Their group can be access with this link: t.me/TacoCarnivoreBitcoinPlebs

O.G. Bitcoiner Original Gangster. It is an acronym that come to mean that someone is a long-time participant individual who is unique in every aspect within the Bitcoin community.

Influencer A person who influencers people in the real world with their speeches and activities, attempting to influence their activities and behaviours. They often run Podcasts.

UASF Was titled the User Activated Soft-Fork as part of Bitcoin Improvement Proposal 148. It is often mistaken for the abbreviation of the US Air Force. It mentioned the first militarization of the community that stood up against third party attackers that seek to profit from the bitcoin protocol’s forceful changes.

NO2X The No 2X movement was a community action by bitcoiners who refused to comply with miners demands to activate Segwit-2MB block increase, the miners lost the war and it was never activated.

#WeAreAllHodlonaut Was a campaign by Bitcoiners on Twitter in response to the doxing attempts against Hodlonaut who deleted all his social media accounts due to fears of safety for his physical safety and to protect his identity. Bitcoiners changed their avatars to the avatar of Hodlonaut, which is an Astronaut Space Cat, with that symbolically defending Hodlonaut.

Myth of the Bitcoin Time-Traveler The story of the Bitcoin Time Traveler titled “*I am a time-traveler from the future, here to beg you to stop what you are doing.*” is a message posted onto the popular message board Reddit by a non-existing anonymous reddit user. On the post, the user describes the effects of bitcoin on the future and talks about how it is going to end up causing a damaged dystopian future. The post initially was called into question, if it can be a considered a credible warning since the reddit user’s account could not be loaded anymore. Based on a popular myth, if the user changed the effects of history by describing the future, the outcome of the future potentially has changed and that could be a reason for the missing account. Since the time traveler did not have to return back to the past, then the account is was never created. On the 27th of October 2019, the reddit post was modified describing the dangers of reckless

investing, the account's profile is still leading to a non-existent page, some speculate that this might have been manipulated by twitter moderators to downplay the message's importance.

bcash Is a derogatory slang name of Bitcoin Cash, but alternative forms are also used like: *bcrash* and *btrash*.

Bitcoin Citadel The concept of Bitcoin Citadels originates from the reddit post of the Bitcoin Time-Traveler who described fortified gated communities as quasi citadels where bitcoin users concentrate to protect themselves from those that are hostile towards users of Bitcoin. As of today, there are many discussions about the existence of these citadels and has become a quasi-meme among bitcoiners. Pseudonymous Twitter user FartFace2000 (FF2K) has pledged that if the value of bitcoin rises up again, he will re-structure his construction business to specialize in the planning and building of real-life bitcoin citadels.

Antifragile Antifragile is the antonym of fragile, a state that when put out to effects of shocks and damage, it becomes better instead of breaking apart. It is also the title of a Book popular among Bitcoiners that was written by Nassim Nicholas Taleb. The book also talks about the effects of antifragile systems that benefit from disorder, such system like Bitcoin. (Taleb, Antifragile)

6.15 BTC 6.15 BTC, pronounced as six-point-five bee-tee-see, is a meme created on the online discussion board Reddit by a Twitter user @american_hodl (currently running under @hodl_american username on Twitter because of a repeated suspension), who has been previously banned multiple times on the social media platform due to his repeated breaking of rules because of his persistent issues with his obsessive defiance disorder. His coining of the term created an over sexualized version of immense reward of bitcoin ownership in perspective of the future. As @american_hodl claims, the 6.15 BTC equals infinite riches and "big titty bitches". This sexualization of bitcoin ownership coincides with previous version of Lamborghini ownership as a sign of success within the bitcoin space.

Paralel__n__i Polis Paralelní Polis is a bitcoin café, hackerspace and cryptoanarchist hangout in Prague-Holešovice, Czechia. They only accept cryptocurrencies as payment option. It gives home to the annual Hacker's Congress. Founded by Slovakian hackers and Artists and Activists from Czechia to advocate for liberation of society and use of advanced technologies that help this process. Can be found at Dělnická 475, 170 00 Praha 7-Holešovice

Hacker's Congress Paralel__n__i Polis Is a major cryptoanarchist conference in Prague, Czechia. The conference often brings about a large bases of users (annually since 2014) who are interested in the topics related to Bitcoin, cryptocurrencies, hacking, cryptoanarchy, liberty, science, libertarianism, and privacy. Hacker's Congress is now a large international event attracting attendees from all over the world. The congress often partners with La Fabrika to provide conference space for the event.

Paralelná Polis Paralelná Polis is a bitcoin café, hackerspace and cryptoanarchist hangout in Bratislava, Slovakia. It was founded by some of the original Slovakian hackers who also helped found Paralelní Polis in Prague. They also strive to advocate the liberation of society and the use of technologies that help achieve these goals. Can be found at Kominárska 1552/3a, 831 04 Bratislava

Boating Accident Bitcoiners often joke with the term boating accident, when referring to losing their wallet. Often this is used as plausible deniability, claiming that they lost their wallet and there are no more copies of their private key to access their funds.

BTFD Buy the Fucking Dip is a slang term used by Bitcoiners when the price of bitcoin goes lower or crashes more in USD price, with that telling each other to buy more bitcoin.

Not your keys, not your coins Is a term that refers to the ownership of the private key, custodial exchanges do not provide the private key to users therefore they are not in possession of their own coins because the custodial is in possession of it while providing an IOU (I owe you) type of bitcoin substitute that buyers can possibly withdraw from exchanges. Exchange hacks often results with the exchange's bitcoins becoming stolen, if someone doesn't hold their own private key then they simply don't own their coins.

Bitko Bitko, the Bitcoin Monster, the Apex Predator of Fiat Currencies. Imaginary Bitcoin monster drawn by the artist Bitko Yinowsky. The creature is a funny B figure with a single eye in the upper hole of the character B and the lower hole is his mouth, he have a long tongue and likes to feast on fiat currencies.

Satoshi's Place It is an online drawing board where users can donate satoshis over the lightning network and can place coloured pixels onto the board.

Satoshi Games An independent game developer studio creating creative games that can interact with the lightning network. They create browser-based games that can be played on the internet.

Lightnite A Battle Royale like 3D action game that gives rewards for player in satoshis for activities that they can withdraw from the game. It is still currently in development.

Shitcoin Shitcoin is a derogatory term that attempts to display disdain with the existence of alternative cryptocurrencies that were created to attempt to replicate the effects of bitcoin. Since bitcoin over the years seen massive appreciation of value, those with capabilities to alter the source code of bitcoin began developing alternatives and "improved" iterations of the original bitcoin. This has led to a massive economy of "shitcoins" of over 10000 cryptocurrencies and tokens circulating on their own respective blockchain networks or glorified MySQL databases. As programmable additions were created also under the so called smart-contract variant blockchains, it has enabled and accelerated the creation of scam tokens and speculative assets that saw their prices being pump and dumped as speculators began using them to produce profits on their volatility. Since most of these alternative blockchains have very little proof of work securing their blockchain, a direct attack by a nation state or even by a bitcoin miner with larger E/Hash mining power, they could potentially destroy these chains by participating in a 51% double spend attack on these networks. Since "shitcoins" do not enable anything else other than the advancement of the inherent human greed. Bitcoiners coined the term "shitcoin" for their identification since they are in quality and property are much more inferior to that of bitcoin. Shitcoins also can be a form of attack on the bitcoin ecosystem, because whenever a new coin is created, new speculators are pulled into it and with that potentially removing more available value flow from bitcoin, with that slowing down its adoption process. The word can also be used as an adjective to refer to those who use shitcoins.

Room 77 Is a café in Berlin that accepts Bitcoin as a currency and regularly hosts the biggest regular Bitcoin meetup in Berlin, Germany. Can be found at Graefestraße 77, 10967 Berlin

When Moon? The phrase When Moon in the bitcoin community refers to expected profits with the USD price of bitcoin. Since trading platforms often utilize candles to trade, their increments often symbolize rocket spaceship like lift-offs that seem like the price of bitcoin is headed towards the moon. Therefore, speculator users began coining the term when moon or mooning to describe either a question of potential lift-off in price or the currently ongoing positive price changes of bitcoin.

When Lambo? When Lambo and When Moon are terms associated with the impending profits experienced by speculating individuals. Usual behavior can be observed in chat rooms and online discussion boards and the social media site Twitter. Lamborghini ownership within the bitcoin space began symbolizing immense success within the space. As the astronomical rise in the USD price of bitcoin made it possible for many early holders of bitcoin to be able to afford iconic creations of the Italian super sports car manufacturer Lamborghini. Often owners of Lamborghinis placed custom license plates on their cars brandishing their origin of wealth or affiliation towards bitcoin.

Faketoshi Self-proclaimed Satoshi Nakamoto and serial fraudster Craig Steven Wright⁶⁰ received this nick due to his repeated claims to be the bitcoin inventor Satoshi Nakamoto. Faketoshi is now also used as a term for anyone who claims to be Satoshi Nakamoto, it is widely understood by bitcoiners that Satoshi Nakamoto has left the space this way to protect his creation against interference that wants to use him to destroy it.

Babies are dying! It was a viral phrase Roger K Ver bcash (BCH) founder have uttered during a conference claiming that the original Bitcoin is killing babies in war and famine torn countries. Bitcoiners were quick to turn it into a meme online.

Two weeks™ A phrase often associated with software that is built upon bitcoin, it means that something will be ready when it is ready. Usually not within two weeks.

Vires in Numeris Strength in Numbers. It is the official latin motto of Bitcoin Protocol.

Bitcoin fixes this It is a term used to refer to problems that can be solved by Bitcoin, due to Bitcoin's overwhelming effect on politics, society and economics, the problems that Bitcoin can fix seem to make up a very long and diverse list, therefore Bitcoiners often use this term liberally.

Appendix 2: Cryptographic Proofs

Author's Previous Versioning Attestation via OpenTimeStamps.org

Name: FORRELEASE-2020-Thesis.docx
Size: 423185 bytes (413 KiB)
SHA256: A1E266FDC3689FE9C59981381981563E087CAD922167BD47E05D01DDEF39DFF7
Author: Karo Zagorus
PGP of Author: 8E06 CD76 ACE6 1F00
Latest Bitcoin Block:
000000000000000000000000c4cd95acf70721608cc93c938a46e09f2a2a02f785abc



Art by Koridian Lionell



Art by Koridian Lionell

References

- Abramson, Alana. *Hillary Clinton Officially Wins Popular Vote by Nearly 2.9 Million*. ABC News, 22 Dec 2016. Web. 15 Oct 2019.
- Achenbach, Joel and Scott Clement. *America really is more divided than ever*. The Washington Post, 16 July 2016. Web. 02 August 2019.
- Acinq. *Lightning Network Explorer*. n.d. .
- Adamant Capital. *Bitcoin in Heavy Accumulation*. Adamant Capital, 18 April 2019. 19 April 2019.
- Adler, Robert. "Entering a dark age of innovation." 02 July 2005. 06 Jun 2019.
- Ajiboye, Timi, et al. *The Little Bitcoin Book*. 2019.
- Ammous, Saifedean. *The Bitcoin Standard, The Decentralized Alternative to Central Banking*. John Wiley & Sons, Inc., 2018.
- Andersch, Manuel. "Megatrend Digitalisation, Is Bitcoin outshining gold?" 2019.
- Anon1. *Erste Bank has ruined my life* Karo Zagorus. 10 Jun 2019. Telephone.
- Antonopoulos, Andreas M. *Mastering Bitcoin, Programming the Open Blockchain*. O'Reilly Media Inc., 2017.
- Arnott, Jonathan. *Will outrageous EU interference in British democracy ever end? European Parliament's beastly bid to block Brexit*. RT, 10 Oct 2019. Web. 24 Oct 2019.
- Avan-Nomayo, Osato. *Wikileaks have received more than \$46 million in bitcoin*. Bitcoinist, 07 July 2019. 07 July 2019.
- Barlow, John Perry. *A Declaration of the Independence of Cyberspace*. Davos, Switzerland, 08 Feb 1996. 01 March 2019. <eff.org/cyberspace-independence>.
- Barr, Caelainn. *The areas and demographics where the Brexit vote was won*. The Guardian, 24 Jun 2016. Web. 24 Oct 2019.
- Bashir, Masooda, Beth Strickland and Jeremiah Bohr. "What Motivates People to Use Bitcoin?" 19 Oct 2016. 01 May 2019.
- Bayer, Lili. *Viktor Orbán's former BFF vows to take down Fidesz*. Politico, 28 06 2017. Web. 05 Sept 2019.
- BBC Trending. *The country where Facebook posts whipped up hate*. 12 Sept 2018. 06 Jun 2019.
- Beauchamp, Zack. *It happened there: how democracy died in Hungary*. 13 Sept 2018. Web. 14 Sept 2018.
- Beedham, Matthew. *\$200M cryptocurrency mixing operation dismantled by Eurocops*. The Next Web, 23 May 2019. Web. 23 May 2019.

Bialik, Kristen. *State of the Union 2019: How Americans see major national issues*. Pew Research Center, 04 Feb 2019. Web. 09 Feb 2019.

Biggs, John. *What You Need To Know About The Liberator 3D-Printed Pistol*. Techcrunch, 06 05 2013. Web. 24 Oct 2019.

BigTanGringo. #Liberator12k ZZ6-12. 24 July 2019. Twitter. 10 Aug 2019.
<twitter.com/BigTanGringo/status/1153834924438257666?s=20>.

BitMEX Research. "Anatomics of the Next Global Financial Crisis." 12 February 2019. 29 May 2019. —. "The Economics of the Difficulty Adjustment." 15 September 2017. 29 May 2019.

Block Digest. *SHI256 #2 - UASF & NYA*. Prod. @brian_trollz Shinobi. 01 Aug 2019. YouTube. 01 Aug 2019. <youtube.com/watch?v=MdG3BgoKWVE>.

Bogart, Spencer. *Bitcoin is a Demographic Mega-Trend: Data Analysis*. 30 April 2019. 01 May 2019.
<medium.com/blockchain-capital-blog/bitcoin-is-a-demographic-mega-trend-data-analysis-160d2f7731e5>.

Bogatyy, Ivan. *Breaking Mimblewimble's Privacy Model*. 18 Nov 2019. Web. 18 Nov 2019.

Bohr, Jeremiah and Masooda Bashir. "Who Uses Bitcoin?" *2014 Twelfth Annual Conference on Privacy, Security and Trust (PST)*. Urbana, USA, 2014. 01 May 2019.

Bomberger, William A. and Gail E. Makinen. "The Hungarian Hyperinflation and Stabilization of 1945-1946." *Journal of Political Economy* 91, no. 5 (1983): 801-824. Document. 12 March 2020.

Borger, Julian. *Journalist Pelin Ünker sentenced to jail in Turkey over Paradise Papers investigation*. 09 Jan 2019. 09 Jan 2019.

Brown, Ben. 'There's Bitcoin and Then There's Shitcoin (Libra)'. *Congress Finally Gets It*. CCN, 19 July 2019. Web. 19 July 2019.

BTCPay Server. *About TOR and BTCPay Server*. 28 Feb 2019. Web. 10 Oct 2019.
<medium.com/@BtcpayServer/about-tor-and-btcpay-server-2ec1e4bd5e51>.

Caldwell, Leigh Ann. *New year, same stalemate in Congress on government spending, DACA*. NBC News, 03 Jan 2018. Web. 03 Jan 2018.

Capital Creators. *One Dollar or One Bitcoin - College Students Asked What They Would Accept*. 20 May 2019. YouTube. 29 May 2019. <youtube.com/watch?v=whrORgwyLE4>.

Caras, Michael. *Bitcoin Money: A Tale of Bitville Discovering Good Money*. Lightning Source UK Ltd., 2019.

Castillo, Michael del. *Bitcoin's Last Gunslinger*. 03 Jan 2018. 03 Jan 2018.

CDC. *CDC funds 34 innovative projects to combat antibiotic resistance*. Center for Disease Control and Prevention, 06 Oct 2016. Web. 23 10 2019.

Chang, Alvin. *The Facebook and Cambridge Analytica scandal, explained with a simple diagram*. Vox, 02 May 2018. Web. 02 May 2018.

Chappell, Bill. *Supreme Court Declares Same-Sex Marriage Legal In All 50 States*. NPR, 26 June 2015. Web. 26 June 2015.

Cheng, Evelyn. *Bitcoin bubble dwarfs tulip mania from 400 years ago, Elliott Wave analyst says*. Ed. CNBC. 20 Jul 2017. 04 Jan 2018.

Cheong, Ian Miles. *Rebel Against the Extinction Rebellion*. Human Events, 22 10 2019. Web. 23 10 2019.

Chomsky, Noam. *Email Conversation* Karo Zagorus. Redacted Redacted Redacted. Email.

CNBC. *Disruptors are 'clearly shaking the system,' IMF's Lagarde says*. CNBC, 10 April 2019. 10 Apr 2019.

CNN Politics. *GOP Texas state Rep. Briscoe Cain tweeted at Beto O'Rourke saying, "My AR is ready for you Robert Francis," in response to O'Rourke's mandatory gun buyback proposal*. 13 Sept 2019. Twitter. <twitter.com/CNNPolitics/status/1172480899939799041>.

Cohan, William D. *How Wall Street's Bankers Stayed Out of Jail*. The Atlantic, Sept 2015. Web. 10 March 2019.

Cull, Nicholas J., et al. *Soviet Subversion, Disinformation and Propaganda: How the West Fought Against it*. LSE Consulting, October 2017. Web. 15 Oct 2019.

Davidson, James Dale and Lord William Rees-Mogg. *The Sovereign Individual, Mastering the Transition to the Information Age*. Touchstone, 1999.

Davies, Alex. *General Motors Is Going All Electric*. Wired, 02 10 2017. Web. 23 10 2019.

De, Nikhilesh. *'A Real Bubble': Billionaire Warren Buffett Doubles Down on Bitcoin Doubt*. 26 Oct 2017. 28 Dec 2017.

Deener, Will. *No one went to prison after the 2008 financial crisis - and the fault lies with us*. Dallas News, 13 Feb 2017. Web. 05 Jun 2019.

Denber, Rachel. *Russia Is No Safe Place For Independent Journalists*. Human Rights Watch, 23 Oct 2017. Web. 20 Oct 2019.

Deterrence Dispensed. *FGC-9*. CTRLPew, 28 March 2020. YouTube Video. 28 March 2020. <youtube.com/watch?v=1zabSOHd0Ag>.

Dimbleby, Kitty and Bel Mooney. *'Mum and I will never understand each other's views on Brexit'*. The Telegraph, 04 Sept 2019. Web. 11 Sept 2019.

Dodds, Laurence. *China floods Facebook with undeclared coronavirus propaganda ads blaming Trump*. The Telegraph, 05 April 2020. Web. 05 April 2020.

Doherty, Brian. *Bitcoin: If It Ain't Dead, It Should Be Because It's All About "White Privilege"*. 27 Feb 2014. Web. 10 Jan 2019.

Edelman. "2008 Edelman Trust Barometer." 2008. PDF. 16 Jun 2019.

- "2009 Edelman Trust Barometer." 2009. PDF. 16 Jun 2019.
- "2010 Edelman Trust Barometer." 2010. PDF. 16 Jun 2019.
- "2011 Edelman Trust Barometer." 2011. PDF. 16 Jun 2019.
- "2012 Edelman Trust Barometer." 2012. PDF. 16 Jun 2019.
- "2013 Edelman Trust Barometer." 2013. PDF. 16 Jun 2019.
- "2014 Edelman Trust Barometer." 2014. PDF. 16 Jun 2019.
- "2015 Edelman Trust Barometer." 2015. PDF. 16 Jun 2019.
- "2016 Edelman Trust Barometer." 2016. PDF. 16 Jun 2019.
- "2017 Edelman Trust Barometer." 2017. PDF. 25 August 2018.
- "2018 Edelman Trust Barometer." 2018. PDF. 03 March 2019.
- "2019 Edelman Trust Barometer." 2019. PDF. 03 March 2019.

Eisinger, Jesse. *Why Only One Top Banker Went to Jail for the Financial Crisis*. The New York Times, 30 Apr 2014. Web. 08 Oct 2018.

Emese, Fekete. *Így lett Magyarország devizapokol*. Origo, 22 08 2011. Web. 23 02 2019.

English, Carleton. *Nouriel Roubini says Bitcoin is 'bulls-t'*. 02 May 2018. Web. 25 Jan 2019.

European Center for Disease Prevention and Control. *Combined resistance to multiple antibiotics: a growing problem in the EU*. ECDC, 17 Nov 2017. Web. 23 10 2019.

Europol. *Multi-Million Euro Cryptocurrency Laundering Service BESTMIXER.IO Taken Down*. 22 May 2019. Web. 22 May 2019.

Federal Reserve Bank of St. Louis. "Banking Act of 1933." 1933. Web. 12 Jan 2020.

Fischer, Tibor. *Happy 10th birthday, bitcoin. It's amazing you still exist*. 03 Jan 2019. Web. 03 Jan 2019.

Frean, Alexandra. *Bitcoin will become the world's single currency, Twitter chief says*. 21 March 2018. 30 August 2018.

Frisby, Dominic. *Bitcoin, The Future of Money?* Unbound, 2014.

FuggGunControl. *Fuck Gun Control 9 Carbine*. 03 Oct 2019. Twitter. 03 Oct 2019.
twitter.com/FuggGunControl/status/1179792028021989376.

- *Plastikov 3D Printed AK Receiver*. 23 Oct 2019. Twitter. 23 Oct 2019.
twitter.com/FuggGunControl/status/1185642575551782918.

Fukuyama, Francis. *Trust: Human Nature and the Reconstitution of Social Order: The Social Virtues and the Creation of Prosperity*. Free Press Paperbacks, 1995.

Gladstein, Alex. "Why Bitcoin Matters for Freedom." 2018. *TIME*. 28 12 2018.

Glahn, Richard Von. *Fountain of Fortune*. University of California Press, 1996.

Glenski, Maria, Emily Saldanha and Svitlana Volkova. "Characterizing Speed and Scale of Cryptocurrency Discussion Spread on Reddit." 27 May 2019. 09 Jun 2019.

Goldblatt, David and Daniel Nolan. *Viktor Orbán's reckless football obsession*. The Guardian, 11 Jan 2018. Web. 23 10 2019.

Golumbia, David. *The Politics of Bitcoin, Software as Right-Wing Extremism*. University of Minnesota Press, 2016.

Graff, Garrett M. *Did Satoshi Nakamoto Write This Book Excerpt? A WIRED Investigation*. Wired, 01 January 2018. Web. 10 March 2020.

Grym, Aleks and Bank of Finland. "The great illusion of digital currencies." 2018.

Gurgutz, Dr. Zeynep, Prof William Knottenbelt and Imperial College of London. "CRYPTOCURRENCIES: OVERCOMING BARRIERS TO TRUST AND ADOPTION." 2018.

Halasz, Julia and Juli Boros. *Ők azt gondolják, 1 migránsból lesz 6 migráns, 6-ból meg 12, és a végén elfoglalják egész Ócsényt, egész Magyarországot*. 444.hu, 28 Sept 2017. Web. 28 Sept 2017.

Harmat, Balint and David Molnar. *Interview with the creators of Wasabi Wallet Karo Zagorus*. Budapest, 28 Oct 2019. Notes.

Hayek, Friedrich A. *The Road to Serfdom*. Routledge Press, 1944. —. "The Use of Knowledge in Society." *The American Economic Review*, Vol. 35, No. 4 (Sep., 1945), pp. 519-530 n.d. 05 Jun 2019.

Hayes, Arthur. *Two sides of the coin: the bifurcated near-future of money*. 03 Jan 2019. Website. 03 Jan 2019.

Henley, Jon. *What is the current state of the migration crisis in Europe?* The Guardian, 21 Nov 2018. Web. 05 May 2019.

Hertig, Alyssa. *Bitcoin Devs Are Feeling More Optimistic About MimbleWimble*. 23 Jan 2017. 03 Jan 2019.

Hodlonaut. *The Bitcoin Plebs Interview 1* Karo Zagorus. 15 11 2019. Chat.

Huebner, Jonathan. "A possible declining trend for worldwide innovation." 10 September 2005. 01 May 2019.

Hughes, Eric. *A Cypherpunk's Manifesto*. 9 March 1993. 07 Feb 2019.
activism.net/cypherpunk/manifesto.html.

Hutton, Will. *Britain is being led to an epic act of national self-harm over Brexit*. 03 Jun 2017. The Guardian. 08 Jan 2019.

IMRD. *Money printer go BRRR*. Internet Memetic Research & Development, 2020. Web.

Jacobs, Ben. *Trump defends Mexican rapist claim during conspiracy-laden speech*. The Guardian, 05 April 2018. Web. 05 Jun 2019.

jimbo. *Orange Coin Good: The Value of Bitcoin*. Early Access by Author. 2020.

Jones, Owen. *Feel no pity for Theresa May. She has been the worst prime minister in modern times*. The Guardian, 24 May 2019. Web. 25 May 2019.

Kasher, Prof. Asa, et al. *The Migration Wave into Europe*. Ed. Fiamma Nirenstein. Jerusalem Center for Public Affairs, 31 Mar 2019. 06 Jun 2019.

kasnykm. *Végigbüntette az MNB a behajtócégeket*. 29 Sept 2015. 14 Jun 2019.

Krawisz, Daniel. *Why Bitcoin Will Continue to Grow*. The Nakamoto Institute, 01 Feb 2014. Web. 12 Feb 2019.

Krawisz, Daniel. *Hyperbitcoinization*. The Nakamoto Institute, 29 March 2014. Web. 12 Feb 2019.

Krieg, Gregory. *How did Trump win? Here are 24 theories*. CNN. 10 November 2016. 27 Jun 2019.

Kyodo. *Number of newborns in Japan fell to record low while population dropped faster than ever in 2018*. 07 Jun 2019. Web. 23 10 2019.

Langlois, Shawn. *How biased is your news source? You probably won't agree with this chart*. MarketWatch, 21 Apr 2018. Web. 20 Oct 2019.

Lee, David. *The tactics of a Russian troll farm*. BBC, 16 Feb 2018. Web. 24 Oct 2019.

Lenard, Dr. Rita. "Vulnerability and chaos in the Hungarian healthcare system." 2018. Web. 10 March 2020.

Li, Chanel and Ragnar Lifthrasir. *2: Behind Enemy Lines - A.G. Leaks*. Guns n' Bitcoin, 03 Sept 2019. Web. 25 Sept 2019. gunsnbitcoin.com/podcast/ep2/.

- *5: Come and Print It - Ivan The Troll*. Guns n' Bitcoin, September 2019. Web. 01 October 2019. gunsnbitcoin.com/podcast/ep5/.
- *7: BitcoinGun Lawyer Part I*. Guns n' Bitcoin, 08 October 2019. Web. 15 October 2019. gunsnbitcoin.com/podcast/bitcoin-gun-lawyer-part-i/.

London Real. *Andreas Antonopoulos - The Death of Money - PART 1/2* London Real. 15 Jan 2017. Web. 9 July 2019. youtube.com/watch?v=DuoE5CXlIdY.

Maddox, Alexia, et al. "An ethnography of Bitcoin: Towards a future research agenda." *Australian Journal of Telecommunications and the Digital Economy* 4.1 (2016). 18 March 2020.

Magyar, Hajnalka, et al. *Van egy magyar Magyarország*. 16 Jun 2018. Web. 16 Jun 2018.

Magyari, Peter. *Tudományosan bizonyították, hogy Orbán Viktor egyre inkább paráztat*. 444.hu, 04 July 2018. Web. 04 July 2018.

Márk, Herczeg. *Ellenzéki képviselők együtt kezdeményezik a kilakoltatási moratórium meghosszabbítását*. 444, 18 Apr 2019. Web. 27 Jun 2019.

Mason, Rowena and Peter Walker. 'Surrender act': Johnson ignores calls to restrain his language. *The Guardian*, 29 Sept 2019. Web. 30 Sept 2019.

McCammond, Alexi. *Beto ignites split among 2020 Democrats on guns*. AXIOS, 03 Oct 2019. Web. 24 Oct 2019.

McCann, Kate and Tom Morgan. *Nigel Farage: £350 million pledge to fund the NHS was 'a mistake'*. *The Telegraph*, 24 June 2016. Web. 24 June 2016.

McKay, Hollie. *Moscow feels vindicated in the wake of "no collusion"*. *Fox News*, 25 March 2019. Web. 25 March 2019.

Ministry of Finance and Economic Affairs of Iceland. *Progress of the Plan for Removal of Capital Controls*. Government of Iceland, 25 Oct 2017. Web. 01 Dec 2019.
<government.is/library/Files/greinargerd_okt17-2_enska.pdf>.

Monaghan, Angela. *Bitcoin is a fraud that will blow up, says JP Morgan boss*. 13 Sept 2017. 28 Dec 2017.

Mozur, Paul. *A Genocide Incited on Facebook, With Posts From Myanmar's Military*. 15 Oct 2018. 6 Jun 2019.

MTI. *ELFOGADTÁK A KILAKOLTATÁSI MORATÓRIUM MEGHOSSZABBÍTÁSÁT*. Magyar Idok, 31 Oct 2017. Web. 25 Sept 2018.

Myers, Jolie and Monika Evstatieva. *Meet The Activist Who Uncovered The Russian Troll Factory Named In The Mueller Probe*. NPR, 15 March 2018. Web. 15 March 2018.

Nakamoto, Satoshi. *Bitcoin open source implementation of P2P currency*. 11 Feb 2009. Web. 01 Dec 2019.
p2pfoundation.ning.com/forum/topics/bitcoin-open-source.

- *Bitcoin v0.1 released*. Nakamoto Institute, 08 January 2009. Web.
satoshi.nakamotoinstitute.org/emails/cryptography/16/.
- "Bitcoin: A Peer-to-Peer Electronic Cash System." 2008.

Nardelli, Alberto. *Are there really 8 million foreigners in Britain?* *The Guardian*, 26 Aug 2015. Web. 10 Oct 2019.

Nicholson, Catheryne. *MimbleWimble: Silly Sounding Tech Could Seriously Reform Bitcoin*. 30 April 2017. 03 Jan 2019.

Nirenstein, Fiamma. *The Immigration Crisis in Europe*. Jerusalem Center for Public Affairs, 31 Mar 2019. Web. 06 Jun 2019.

nopara73 and TDevD. *ZeroLink: The Bitcoin Fungibility Framework*. 28 July 2017. Web. 02 January 2019.
nopara73. *Samourai vs Wasabi Mixing Architecture*. 25 Oct 2019. Web. 25 Oct 2019.

O’Kane, Sean. *Tesla posts back-to-back profits for the first time*. The Verge, 30 Jan 2019. Web. 23 10 2019.

Oliver, John. *Brexit III: Last Week Tonight with John Oliver (HBO)*. HBO, 18 Feb 2019. 15 April 2019.
[youtube.com/watch?v=HaBQfSAVt0s](https://www.youtube.com/watch?v=HaBQfSAVt0s).

Ossinger, Joanna. *Roubini Says Bitcoin Is the ‘Biggest Bubble in Human History’*. 02 Feb 2018. Web. 02 Feb 2018.

OTP Bank. “Üzletszabályzat a természetes személyek adósságrendezéséről (Magáncsőd) lakossági ügyfelek részére.” 25 May 2018. Web. 27 Jun 2019.
otpbank.hu/static/portal/sw/file/Magancsod_USZ_LAK_20180525.pdf.

Peck, Morgen E. *Bitcoin: The Cryptoanarchists’ Answer to Cash*. 30 May 2012. Web. 16 Jan 2019.

Perez, Yessi Bello. *Why Bitcoin’s Star is Rising in the Czech Republic*. 12 February 2015. Web. 09 Jan 2019.

Pesce, Lyn. *This is exactly how often cocaine and feces show up on your dollar bills*. MarketWatch, 11 July 2017. Web. 28 Nov 2019.

Pew Research Center. *Political Polarization in the American Public*. 12 June 2014. Web. 15 March 2019.

Pilkington, Ed. *Traces of cocaine found on up to 90% of dollar bills in American cities*. The Guardian, 17 Aug 2009. Web. 28 Nov 2019.

Pinsker, Joe. *Why Aren’t Any Bankers in Prison for Causing the Financial Crisis?* 16 Aug 2016. 06 Jun 2019.

PlanB. *Modeling Bitcoin’s Value with Scarcity*. 22 March 2019. Web. 25 March 2019.
medium.com/@100trillionUSD/modeling-bitcoins-value-with-scarcity-91fa0fc03e25.

- “Verification of Monetary Supply of Bitcoin.” *I just personally verified #bitcoin monetary base*. 14 Jun 2019. Tweet. 14 Jun 2019. twitter.com/100trillionUSD/status/1139519771190484993.

Polityuk, Pavel. *Ukraine kidnappers free bitcoin analyst after \$1 mln ransom paid*. Reuters, 29 Dec 2017. Web. 07 March 2020.

Pollack, Andrew. *Drug Goes From \$13.50 a Tablet to \$750, Overnight*. New York Times, 20 Sept 2015. Web. Sept 2015.

Portfolio.hu. *Bedőlt lakossági hitelek tízmilliárdjait adja el a magyar Erste*. Portfolio.hu, 28 Oct 2016. Web. 10 Feb 2019.

Prentice, Ben and Heavily Armed Clown. *WTF Happened in 1971?* 2019. Web. 10 09 2019.
wtfhappenedin1971.com.

Pritzker, Yan. *Inventing Bitcoin*. Middleton, DE, 2019.

Prokop, Andrew. *Cambridge Analytica shutting down: the firm's many scandals, explained*. Vox, 02 May 2018. Web. 02 May 2018.

Rapaport, Lisa. *Another look at the surge in EpiPen costs*. Reuters, 27 March 2017. Web. 08 Sept 2018.

Resnick, Brian. *The science behind why fake news is so hard to wipe out*. Vox, 31 Oct 2017. Web. 27 Jun 2019.

Roberts, Jeff John and Nicolas Rapp. *Exclusive: Nearly 4 Million Bitcoins Lost Forever, New Study Says*. Fortune, 25 November 2017. Web. 11 March 2020.

Rosenbaum, Kalle. *grokking Bitcoin*. Manning Publications Co., 2019.

Rosenberg, Eli. *Chart: Libertarianism Is on the Rise*. The Atlantic, 20 Jun 2011. Web. 24 Oct 2019.

Rothbard, Murray N. *Man, Economy, and State*. New York: D. Van Nostrand, 1962.

Sacchetti, Maria. *U.S. asylum officer say Trump's 'Remain in Mexico' policy is threatening migrant's lives, ask federal court to end it*. The Washington Post, 26 Jun 2019. Web. 26 Jun 2019.

Saphiro, Ben. *Antifa and the Alt-Right, Growing in Opposition to One Another*. National Review, 15 Aug 2017. Web. 10 Jan 2018.

Sarkadi, Zsolt. *Hiába állítja Mészáros, hogy semmi köze a Népszabadság felvásárlójához, nem mond igazat*. 444.hu, 27 Oct 2016. Web. 10 Oct 2019.

Scannell, Kara and Richard Milne. *Who was convicted because of the global financial crisis?* 09 August 2017. Web. 06 Jun 2019.

Schoenberg, Tom and Matt Robinson. *Bitcoin ATMs May Be Used to Launder Money*. Bloomberg, 14 Dec 2018. Web. 09 March 2020.

Seres, Istvan Andras. Interview. Karo Zagorus. 17 Dec 2019. Email.

Servon, Lisa. *The Unbanking of America: How the New Middle Class Survives*. Houghton Mifflin Harcourt Publishing Company, 2017.

Sharma, Gaurav. *Trump Vowed To Save Coal But U.S.' Largest Mining Basin Remains In Decline*. Forbes. 14 Apr 2019. Web. 20 Jun 2019.

Shuster, Simon. *The U.K.'s Old Decided for the Young in the Brexit Vote*. TIME, 24 Jun 2016. Web. 27 Sept 2017.

SIXX. *Magyar Helsinki Bizottság: A kormány szócsöve lett a közmédia*. 26 06 2015. Web. 09 Oct 2019. comment.blog.hu/2015/06/26/magyar_helsinki_bizottsag_a_kormany_szocsove lett_a_kozmedia.

Song, Jimmy. *Understanding Segwit Block Size*. 03 July 2017. Web. 27 Nov 2019. medium.com/@jimmysong/understanding-segwit-block-size-fd901b87c9d4.

Steil, Benn. *The Dangers of Monetary Nationalism*. Real Clear Politics, 09 Dec 2010. Web. 08 02 2019.

Steinmetz, Katy. *This Bitcoin-Trading Family Man Faced Years in Prison. Now He's Telling His Story*. 1 March 2018. Web. 28 Dec 2018.

Stewart, Heather. *Theresa May announces she will resign on 7 June*. The Guardian, 24 May 2019. Web. 24 May 2019.

Stockler, Asher. *BETO O'ROURKE SUGGESTS POLICE WOULD 'VISIT' HOMES TO IMPLEMENT PROPOSED ASSAULT WEAPONS BAN*. Newsweek, 16 Oct 2019. Web. 19 Oct 2019.

Strasser, Annie-Rose. *Bitcoin: By The Privileged, For The Privileged*. 27 Feb 2014. Web. 10 Jan 2019.

Strickland, Patric. *What is the future of Greece's neo-fascist Golden Dawn?* Al-Jazeera English, 17 Apr 2018. Web. 05 Jan 2019.

Subramanian, Samanth. *Inside the Macedonian Fake-News Complex*. WIRED, 15 Feb 2017. Web. 10 July 2017.

Swan, Melanie. *Blockchain, Blueprint for a New Economy*. O'Reilly Media Inc., 2015.

Synchrhon Lizing Zrt. *Adósságrendezési eljárás (Magáncsőd)*. 2019. Web. 27 Jun 2019. synchronlizing.hu/magancsod.

Szabo, Nick. *Bit gold*. December 2005. Web. 16 Jan 2019.

- *Shelling Out - The Origins of Money*. 2002. Web. 20 Aug 2018.

Szmigiera, M. *Number of Blockchain wallet users globally 2016-2019*. January 2020. Web. January 2020. statista.com/statistics/647374/worldwide-blockchain-wallet-users/.

Taiberg, Michael. *A New Report Shows People Are Warming Up to Bitcoin*. Bitcoin Magazine, 01 May 2019. Web. 01 May 2019. bitcoinmagazine.com/articles/new-report-shows-people-are-warming-bitcoin/.

Taleb, Nassim Nicholas. *Antifragile*. Penguin Books, 2012.

- *Bitcoin*. 22 Jan 2018. 08 Aug 2018.
- *Skin in the Game*. Penguin Random House UK, 2018.
- *The Black Swan*. 2nd. Penguin Random House, 2010.

The Economist. *Attitudes towards the mainstream media take an unconstitutional turn*. 02 August 2017. Web. 15 Sept 2017.

The Guardian. *Cambridge Analytica a year on: 'a lesson in institutional failure'*. 17 March 2019. Web. 17 March 2019.

The Swede. *Bull Bitcoin – Protecting Against Financial Censorship And Reclaiming Customers' Privacy, One Coinjoin At A Time*. 04 July 2019. Web. 04 July 2019.

The Tor Project. *History of the Tor Project*. n.d. Web. torproject.org/about/history/.

U.S. Food and Drug Administration. *Combating Antibiotic Resistance*. FDA, 15 11 2011. Web. 23 10 2019.

Vauplane, Hubert de. *The debate on the fungibility of Bitcoin*. 22 Sept 2018. Web. 20 Feb 2020.

Wagner, Kurt. *Here's how Facebook allowed Cambridge Analytica to get data for 50 million users*. Vox, 17 Mar 2018. Web. 18 Mar 2018.

Wallet, Samourai. *Diving head first into Whirlpool Anonymity Sets*. 24 Oct 2019. Web. 24 Oct 2019.

Walt, Stephen M. *The Collapse of the Liberal World Order*. 26 June 2016. Web. 21 Jun 2019.

Weise, Elizabeth. *Russian fake accounts showed posts to 126 million Facebook users*. USA Today, 01 Nov 2017. Web. 01 Nov 2017.

Wheeler, Brian, Paul Seddon and Richard Morris. *Brexit: All you need to know about the UK leaving the EU*. BBC. 10 May 2019. Web. 10 May 2019.

World Bank. *Gross domestic savings (% of GDP) - Japan*. 2017. Web. 23 10 2019.
data.worldbank.org/indicator/NY.GDS.TOTL.ZS?locations=JP.

Yeginsu, Ceylan. *N.H.S. Overwhelmed in Britain, Leaving Patients to Wait*. The New York Times, 03 Jan 2018. Web. 22 Oct 2019.

Yglesias, Matthew. *There's actually lots of evidence of Trump-Russia collusion*. Vox, 11 Jun 2018. Web. 05 July 2018.

Footnotes

<https://github.com/libbitcoin/libbitcoin-system/wiki/Axiom-of-Resistance> [2]

<https://github.com/libbitcoin/libbitcoin-system/wiki/Consensus-Property> [2]

<https://github.com/libbitcoin/libbitcoin-system/wiki/Fedcoin-Objectives> [2]

<https://bitcoin.org/bitcoin.pdf> [2]

<https://github.com/libbitcoin/libbitcoin-system/wiki/Cryptoeconomics> [2] [2]²

According to the book by Lisa Servon about 128 million US Citizens are struggling daily to make a living. (Servon) [2]

We must note here that often these concepts are deeply associated with being a refugee. The conceptualization of the word “refugee” has transformed in Hungary and are now fully associated with other meanings like migrant, muslim, illegal immigrant, rapist and terrorist. The example of events in the town of Ocseny shows that these concepts are now more closely tied together than before. (Halasz and Boros) [2]

Troll Farms (especially in Russia) are state funded institutions that engage in Social Media manipulation by releasing falsified information or running propaganda campaigns in foreign countries. [2]

Lajos Simicska was a teenage friend of Hungarian Prime Minister, Viktor Orban. Due to their friendship deteriorating, they have entered a political feud that prompted Lajos Simicska to buy news outlets and wage a political media war against Viktor Orban. Orban in response has begun personally discrediting and smearing Simicska for cooperating with the billionaire speculator George Soros. (Bayer) [2]

During the Obama Administration, a landmark ruling was passed by the US Supreme Court that allowed Americans to marry others of the same sex in all 50 continental US States. (Chappell) [2]

Monetary Policy, referred here as Monetary Nationalism, is a sovereign State's ability to issue its money and control its monetary policy, money supply and its functions as a sovereign Nation. Either through a ruler like a king, emperor, dictator, or through an independent national central bank. (Ammous; Steil) [2]

Time preference is a behavior trait that determines how we will decide about actions where we might demand instant gratification for our needs. A high time preference trait makes us want to fulfill our needs immediately, while a low time preference makes us defer these actions later into the future. Individuals with low time preference tend to save more money and defer from spending it immediately while those with high will reach for lines of credit, overspending without any possibility of savings. (Rothbard) [2]

A person who uses strong cryptography to communicate online on the internet and who advocates for the usage of surveillance circumventing encryption standards and Bitcoin. [2]

A double spend is a form of malicious action by someone who attempts to spend their value twice. In different digital currencies preceding bitcoin, it was possible to commit double spends. [2]

Satoshi is the smallest fractional unit of a bitcoin. 1 BTC = 100.000.000 sats. On the Lightning Network, 1 BTC can be broken down to 100.000.000.000 millisats (msats). [2]

Transaction malleability although exists within older version of Bitcoin, with legacy transactions, since the network is backwards compatible, malicious nodes (or attackers) could interfere with the script of a transaction and modify it in a way that the transaction would fail or become invalid. An attacker could re-order the fields on a transaction, that would produce a functionally identical but different ID. This problem was solved by the activation of segregated witness proposal. Due to the technical complexity of the segregated witness improvement, it is out of scope for this paper. (Rosenbaum) [2]

Stock-to-flow here means two things, stock is the amount of metal held by others, and flow means the inflation of the supply that the incoming new metal is expanding the supply with. Gold has a stock-to-flow of just over 50. (Ammous; Andersch) [2]

The Foreign Exchange Act of Iceland was enacted in response to the 2008 Financial Crisis and sought to prevent the outflow of capital from Iceland to foreign countries. Essentially the use of Bitcoin in commerce was prohibited until the law was amended in 2017. (Ministry of Finance and Economic Affairs of Iceland) [2]

This is an example of a mnemonic key: 1. VISA 2. EXIST 3. FLAG 4. DEPOSIT 5. ESCAPE 6. CONVINCE 7. FUNNY 8. CLIFF 9. STEP 10. CRYSTAL 11. FEATURE 12. OWN 13. PACT 14. MAIL 15. HARVEST 16. SADNESS 17. SEARCH 18. GHOST 19. OFFER 20. INCH 21. MERGE 22. FEW 23. TIRED 24. SNOW [2]

The 25th passphrase word can be anything up to 100 characters long. [2]

Referenced as spoken by Professor Laszlo K. [2]

As in lacking morality that could impact human life, since it is in its purest form Bitcoin is only a monetary tool that serves human beings as a payment system. [2]

A miner is a computer software that hashes repeatedly to find a bitcoin block. [2]

'It' is used here because miners are automated computer software running on computers or application specific integrated circuits. In shorter name ASIC is a computer specifically designed for a given computational task to perform, here in this case ASIC miners are used to mine Bitcoin to be more cost effective and profitable. [2]

Jameson Lopp maintains a database of crimes committed against bitcoiners and those transacting with bitcoin on a github repository that can be found by following this link: <https://github.com/jlopp/physical-bitcoin-attacks/blob/master/README.md> [2]

Electrum is a lightweight Bitcoin wallet. [2]

Alternative cryptocurrencies that are inferior to Bitcoin. We will discuss the origin of this word in a later chapter. [2]

The Onion Router was developed by employees of the US Naval Research Laboratory to protect that of US intelligence operative's online communication. (The Tor Project) [2]

Wasabi Wallet is a desktop Bitcoin wallet that also allows coinjoining through its coordinator. [2]

Samourai Wallet is a mobile Bitcoin wallet that allows coinjoining through its Whirlpool service. [2]

Blockstream Green is a Bitcoin mobile wallet that also allows access to Blockstream's Liquid Network. [2]

"bitcoind" is the first node software and protocol that implemented remote procedure call (RPC), it is also the runtime for many Bitcoin nodes and Bitcoin full stack environments like BTCPay Server. [2]

BTCPay Server is a self-hosted full-stack business solution for bitcoin accepting businesses and private individuals. [2]

Is a Bitcoin Node full stack with many additional functionalities. [2]

Samourai Dojo is a private Bitcoin server for Samourai Wallet users that allow self-hosted interaction with the Whirlpool coordinator without exposing our IP or xpub keys. [2]

An Electrum Private Server is a private node that can receive connections from Electrum clients, which in return allows private queries of blockchain headers and other blockchain data. It makes the querying of

transactions for wallets more private by concealing the IP address of the desktop wallet from other servers. It can also relay transactions and this way no xpub information leaks out onto the internet. [2]

Know Your Customer is a mandatory financial regulation that forces businesses to profile their users for legal compliance reasons. [2]

Anti-Money Laundering directive that seeks to halt all forms of money laundering and some also applies to halt illegal financing of terrorism. [2]

Mixing services are (often) trusted third party services that mix bitcoins with other coins to the point that they can not be traced to their origin. One notable mixer was BestMixer.io which was shut down by Dutch Police and Europol in 2019. (Europol) [2]

Anonymity set is a debated term due to their wording and usage of the term, which is supposed to refer to the strength of anonymity given for one unspent bitcoin transaction within a UTXO that went through a coinjoin like in Wasabi, Whirlpool or JoinMarket. Samurai Wallet developers argue that there is no central anonymity set possible to determine since every coinjoin is different in shape and size to draw parallels or standards. (nopara73 and TDevD, ZeroLink: The Bitcoin Fungibility Framework) [2]

The Author of this Thesis was the 25th participating member of the #LNTrustChain. [2]

Is the act of hoax calling the police and claiming that a serious incident is happening that will eventually result in armed police storming the premises. [2]

Two examples of these parallel societies can be found in Europe, one in Prague, Czechia called Paralelní Polis and the other in Bratislava, Slovakia called Paralelná Polis. Both communities call themselves cryptoanarchist and actively utilize Bitcoin as the primary form of unit of account and medium of exchange. [2]

BitcoinD is the Bitcoin protocol implementation for remote procedure call (RPC), it functions as part of Bitcoin full nodes. There are other alternatives also like Libbitcoin and BitcoinJS the latter which runs on node.js programming framework. [2]

One of this list of resources is maintained by Jameson Lopp at www.lope.net [2]

Toxic here means that a user of Bitcoin can be unwilling or unaccepting towards other ideas or intolerant towards ideologies of other users or their behavior. These behaviors can range from casino like gambling with alternative currencies or other behaviors that seem to suggest ideology-based changes to bitcoin, we will examine this within Bitcoin Maximalism section within this chapter later. [2]

A 51% mining attack is when someone owns 51% of the total Hashing power of Bitcoin and uses that to mint coins or to alter transactions. [2]

The term Bitcoin Maximalism originates from Vitalik B. who used the term to derogatorily refer to toxic users of Bitcoin. Later Bitcoiners adopted the term and turned it into an integral part of the community

vocabulary. For more terms adopted by Bitcoiners, for a limited list see Appendix 1 in the end of this Thesis. [2]

It is possible to access the group on the popular communication application Telegram by following this link: t.me/rektplebs [2]

Privacy extremism refers to the usage of privacy protecting or enhancing tools or software to protect one's real world identity either online or in real life. [2]

Good online privacy, the usage of virtual private networks (VPNs) and proxies and the Tor network's anonymity layer can all help maintain proper privacy hygiene. Although most services other than Tor comes at a cost if we wish to protect our privacy. [2]

Bitcoin users refer to Craig S. Wright as Faketoshi because his claims that he is Satoshi Nakamoto are unsubstantiated and unproven. [2]

Like the User Activated Soft Fork (UASF) often portrayed as the US Air Force's insignia, intended as a pun to portray superiority of their action and the #NO2X acronym that was used in tweets by those who opposed the 2MB block size upgrade. [2]

Links to these groups can be found in Appendix 1. [2]

This can be attributed to Bitcoin's ability to re-introduce savings and normalize them, with that prompting individuals to delay gratification and think in long term goals. (Ammous) [2]

For more information about spontaneous sociability, please refer to Francis Fukuyama's "*Trust: The Social Virtues and The Creation of Prosperity*" pp. 26-29. [2]

Like that of the UASF (User Activated Soft Fork), #NO2X block size increase and the #WeAreAllHodolonaut events all constitute as one. [2]

Bitcoin in its initial stages, rely on inflation to expand the money supply towards the goal of 21 million bitcoins. This is a process called as block rewards that miners receive for producing blocks through proof of work. As the block reward is halved roughly every four years, bitcoin will become deflationary for the time being until the price of bitcoin stabilizes. From that point on, Bitcoin can become a non-flationary currency void of inflation and deflation. As it will become ever increasingly easier to break down a bitcoin to the tiniest fraction of a unit, deflationary effects will not be possible to observe anymore. In theory, only catastrophic losses of coins will be able to cause massive deflationary value explosions, but as it becomes easier and much more secure to store bitcoins, the chances of such catastrophic human errors decrease over time. This is very apparent after the 2009-2011 period of exploratory usage of the Bitcoin protocol when its users were very reckless with the storage and handling of bitcoins. (Ammous) [2]

A form of money that cannot be confiscated or controlled by governments and cannot be impeded upon by any law, judges, or sovereign nation's military. This is because of the provided option for individuals to refuse cooperation by imposed violence. If an individual refuse to hand over the private keys or passphrases, extraordinarily little can be done outside of the avenues of physical violence to coerce its

extraction. Even if such physical violence is exercised, tricks can be employed to trick attackers to think there are limited amounts of bitcoins available for extraction from one individual's possession, this is called as 'plausible deniability'. [2]

It was proven in US district of Florida court that Craig S. Wright multiple times mislead the court about his claimed identity, showing forged documents, manipulated screenshots of applications, and claiming that aged shelf companies were holding his genesis block coins that a bonded courier were supposed to bring him that allows him to access the coins. [2]

Disclaimer:

WORDS

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

This Journal does not contain reference to any of the investment products or services currently offered by the operator of the journal, that means any business I am associated with. Bitcoin, shitcoins, and related technologies can be volatile. Don't buy what you can't afford to lose and please do your own research.

Bitcoin has paved the way for some VERY radical technology AND it's very confusing. Read more. Ask questions. The purpose of this Journal is to provide archive and curate the best commentary and culture in the bitcoin space.

Nothing within this Journal constitutes investment, legal, tax or other advice. This Journal should not be used as the basis for any investment decisions which a reader may be considering. Any potential investor in bitcoin or shitcoins, even if experienced and affluent, is strongly recommended to seek independent financial advice upon the merits of the same in the context of their own unique circumstances.

Share this journal early and often. Engage the authors and tell them what you think. We sharpen our position through discourse and debate.

DYOR | HODL | BTFD | OCG | NGU | BFT



I hope you enjoy this project. I'm on a mission to archive the great works of Bitcoin thinkers. Onward!

Read **WORDS**

- @_joerodgers