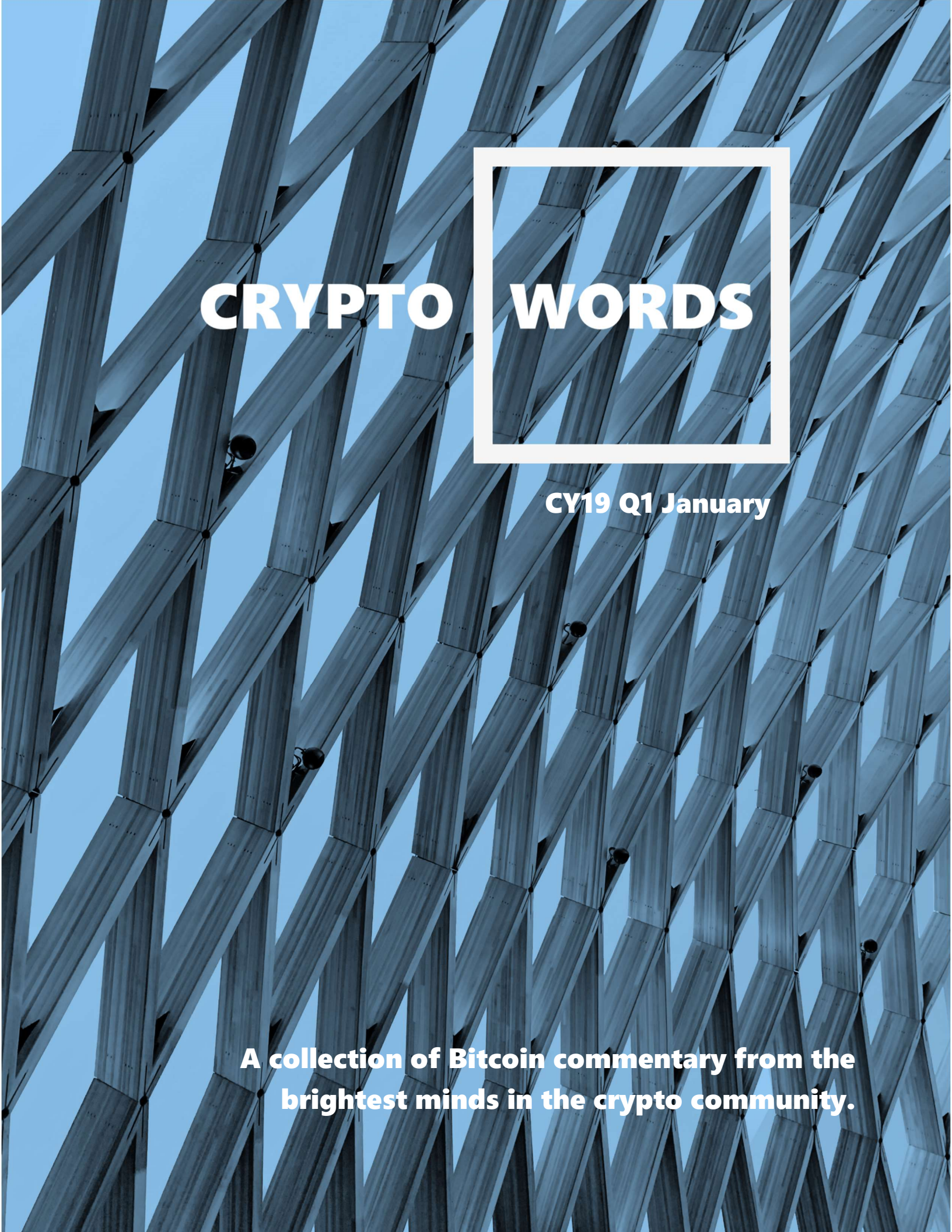


CY19 Q1 January

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

Contents

Goals and Scope

Crypto Words is a quarterly journal of cryptocurrency, or crypto, established February 13, 2019. Its purpose is to document and advance commentary and research in disciplines of particular interest to the crypto community. The journal is broad in scope, publishing content from original research, essays, blog posts, and tweetstorms from a wide variety of fields, especially governance, technology, philosophy, politics, and economics, but also legal theory, history, criticism, and social or cultural analysis. Its broader mission is to capture the conversations and think pieces in the crypto space for current and future researchers. *Crypto Papers 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 crypto publishing. For authors with commentary and scholarly papers on crypto topics, the choice of publication outlets is relatively limited. The number of journals that serve as outlets for crypto research is in any event too small, as the number of crypto thinkers continues to grow with every market cycle.

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

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

Cryptocurrency: The Canary in the Coal Mine

What Crypto Can Tell Us About Macro Markets in 2019

By Jill Carlson

Posted Jan 1, 2019

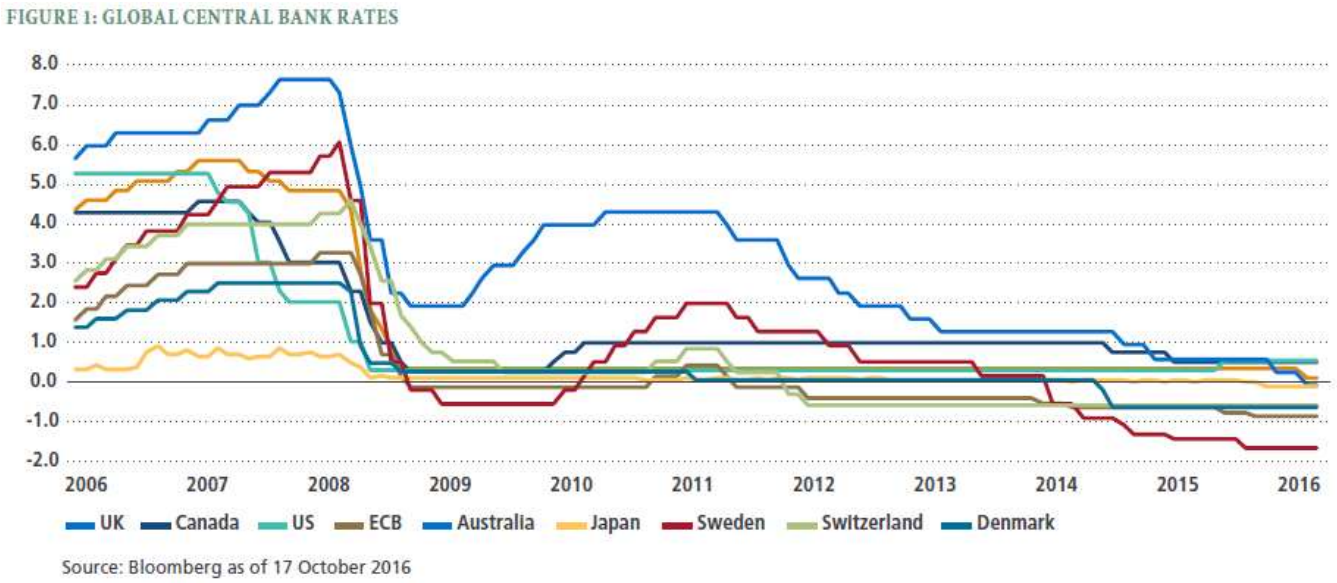
Over the last quarter, the market has rejected risk assets across the board in a sudden reversal of the year's trend. The S&P 500 erased its 9% gain over a matter of weeks in October. The Nasdaq index retraced from an 18% gain to end the year down 5%.

But no market has felt more pain recently than that of cryptocurrencies. The aggregate market cap of cryptocurrencies, which topped out at $830 billion last January, has since crumbled to $130 billion. Much of this unwind has occurred only in the last two months, with the crypto market as a whole getting marked down over 40% quarter-to-date.

The cryptocurrency market is admittedly miniscule relative to other asset classes. Cryptocurrency (no matter how big the drawdown) is unlikely to have any impact on broader markets any time soon. Bitcoin has demonstrated no substantial correlation to any other asset, whether equities or gold. Nonetheless, what has been happening with this nascent asset class over the last year may reveal some important macro trends.

Two years ago, at the end of 2016, the cryptocurrency market stood at $15 billion in value. Trading volumes across all cryptocurrencies hovered in the double-digit millions. What led to the asymptotic spike in prices over the course of 2017? While it may be possible to point to certain headlines and technology developments as catalysts, most would probably dismiss the phenomenon as a speculative bubble. They may not be wrong in this characterization, but they may also miss the macro context in which all of this occurred.

We have seen many search for yield trades play out over the last 8 years. With central banks around the world pumping liquidity into the economy, traditionally risky assets have seen their premiums sucked out of them. Emerging markets stocks, bonds, and currencies have benefited from this trend. High beta equities, most notably in the tech sector, have boomed with the FAANG stocks leading the way. This trend has also driven money further out along the risk spectrum into alternative asset classes, ranging from art to cars to venture capital.



With rates like these, who needs hedges? Image from Pimco's 2016 Negative Interest Rate Report. https://global.pimco.com/en-gbl/resources/education/investing-in-a-negative-interest-rate-world

The cryptocurrency boom of 2017 may have been the illogical conclusion of this global search for yield. It certainly followed this trend, starting as money poured into the relatively lower beta cryptocurrencies (like bitcoin and ethereum). Over time capital found its way into brand new assets as well, the products of initial coin offerings (ICOs) into which investors dumped an estimated $20 billion in the last year and a half, often with little in the way of investor rights or protections. Talk about "risk on"...

But the story has changed since then. If you bought bitcoin at the peak last December and sold today you would be realizing an 80+% loss. Many of bitcoin's brethren, including many ICOs, have performed far worse with some cryptocurrencies getting marked down 95+% this year. The last major legs lower of this correction in October and November have coincided with the broader market sell off.

Perhaps cryptocurrency, the last mover on the way up, is the leading indicator of a broader market fall. If the cryptocurrency boom of 2017 was partly the result of the longest expansionary period the economy has seen in a century, perhaps the bursting crypto bubble of 2018 is the canary in the coal mine that the search for yield has run its course.

The recent downturn across asset classes has been blamed on a global growth slowdown, rising interest rates, and continued political uncertainty. Whether this plays out in 2019 remains to be seen, but if it does, it will manifest first as capital leaves what it perceives to be the riskiest assets.

Tweetstorm: Bitcoin's 10 Year Anniversary

By Vijay Boyapati

Posted January 2, 2019

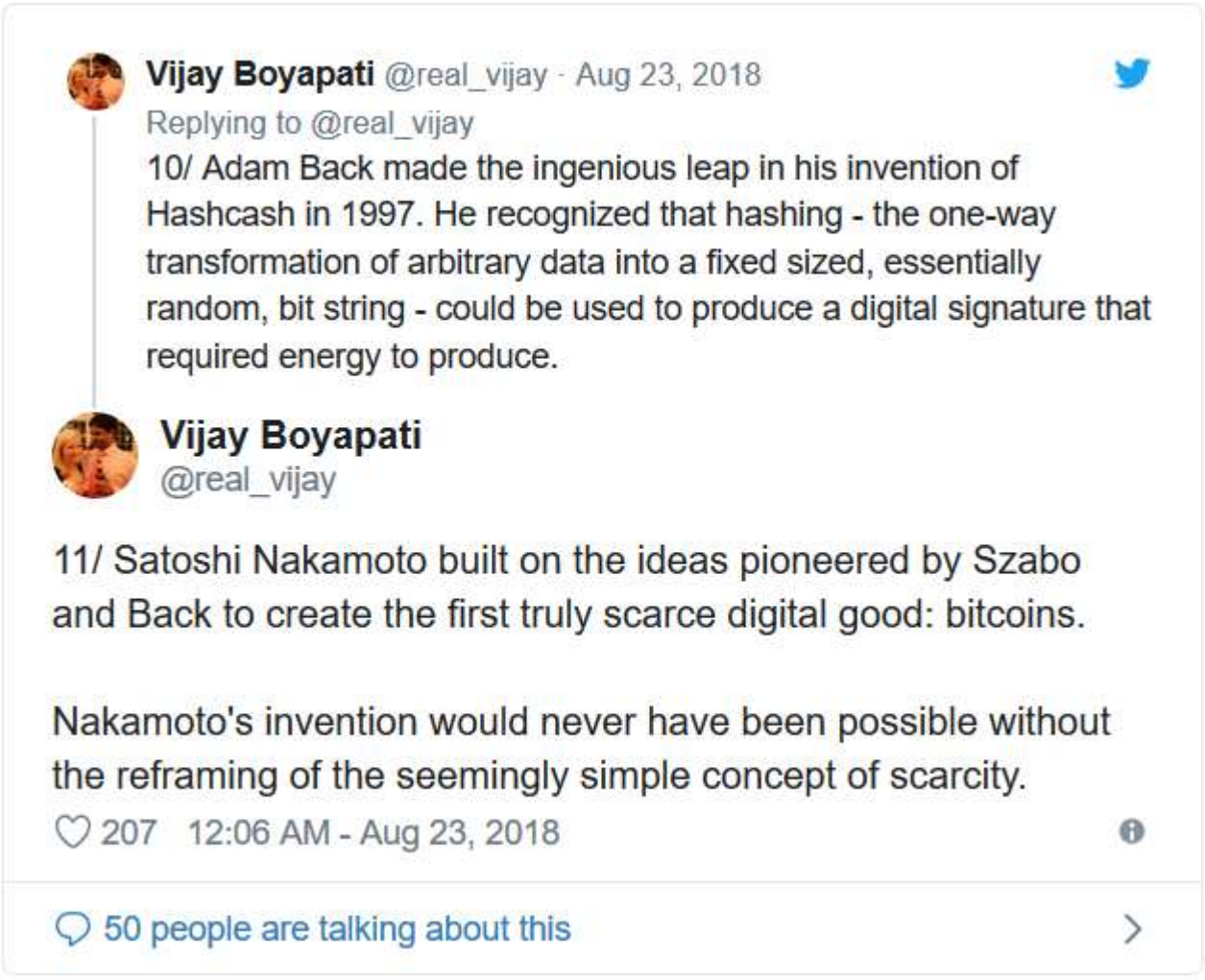
1. 10 years ago today, in an unknown location, a mysterious figure whose identity is still unknown, tapped a key on his keyboard, spurring his CPU into action. In doing so, Satoshi reified his vision for a decentralized digital cash that he'd published 3 months earlier.
2. The fan in his computer began spinning to keep the CPU, burning from the burden of work it had been given, from overheating. The CPU in Satoshi's computer was searching for a special pattern, much like a digital needle in a haystack, that would secure #Bitcoin's first block.
3. Here is that needle:

```
1 - 0x000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f
```

   It is the hash of Bitcoin's "Genesis Block", which created the first 50 bitcoins ever to be mined (by a quirk of Bitcoin's protocol these 50 bitcoins can never be spent).

4. With a brilliant leap of imagination, Satoshi had done what no one else had been able to do, and which many thought impossible. He had ingeniously incorporated @adam3us's Hashcash design as a way of securing transactions on a network not controlled by anyone.
5. By burning energy in search of digital needles-in-haystacks, Satoshi's proof-of-work design allowed, for the first time ever, scarcity to be brought to the digital

realm:



6. Since the creation of Bitcoin's genesis block on January 3rd, 2009 at 6:15pm (GMT), the Bitcoin network has seen the steady and remarkably reliable creation of blocks for a decade, allowing millions of people to store and transfer value without let or hindrance.
7. While many are obsessed with making price predictions about #Bitcoin in 2019, one thing we can actually predict with high certainty is that Bitcoin blocks will continue to be created approximately every 10 minutes with remarkable reliability.
8. As the Bitcoin network continues to function reliably well into the next decade, there will be near-universal confidence that it will be available forever, much as people believe the Internet is a permanent feature of the modern world.
9. Slowly but inexorably the world's population will come to recognize the benefit of opting out of the status quo monetary order and returning to a world of true individual financial sovereignty.
10. 10 years hence we will look back at the now 20 year old Genesis Block and recognize its creation as the beginning of a new monetary epoch. With the tap

of a key on his keyboard Satoshi set in motion a sequence of events that set our world financially free.

Addendum: If you're interested in learning more about the genesis block I highly recommend the fantastic 2013 post by the brilliant @SDLerner .

Bitcoin: Two Parts Math, One Part Biology

By Hugo Nguyen

January 3, 2019

This is Part 5 of a 5 part series

"The Times 03/Jan/2009 Chancellor on brink of second bailout for banks"

Ten years ago today Satoshi Nakamoto immortalized these words by embedding them in Bitcoin's very first block—the genesis block. They are a solemn reminder of the unfair and broken system we all live under, and likely the reason Satoshi created Bitcoin in the first place: to wrest control of money back from governments and central bankers [1].

The last 10 years has been nothing short of a miracle. The Bitcoin network has been up 24/7, boasting an impressive record of 99.98% uptime [2]. What is most amazing is that Bitcoin achieved this without anyone being in control.

Bitcoin is a unique invention because it uproots the very foundation of our society: it redefines money. Money, together with language, are considered the 2 most important tools we humans use to cooperate and build civilizations.

My personal journey into Bitcoin has also been extremely rewarding. Very few things are as intellectually stimulating as Bitcoin. Grokking Bitcoin means going down the rabbit hole that is finance, money, history, economics, computer science and biology. It means retracing the footsteps of giants such as Cardano, Pascal, Turing, Plato & Aristotle, Locke, Hume, Adam Smith, Nash, Kahneman & Tversky, Darwin, John Maynard Smith, Dawkins, Diffie, Hellman & Merkle, Szabo, to name a few. It means asking fundamental questions about the nature of the world we live in—much of which we often take for granted. Bitcoin sends you on an exhilarating and never-ending quest for truth.

Over the last several months I have written a series of articles—which I have called the Bitcoin Fundamentals series. My goal is to go down the rabbit hole as far as I could, to see what Bitcoin is really made of.

Writing these concepts down also forces me to articulate my thinking and helps my understanding of Bitcoin. I hope they will help others as well. The rest of this article will sum up what we have learned in the series.

Full index of the series:

Part 1 - The Anatomy of Proof-of-Work

Part 2 - Bitcoin, Chance and Randomness

Part 3 - How Cryptography Redefines Private Property

Part 4 - Bitcoin's Incentive Scheme and the Rational Individual

Part 5 - Bitcoin: Two Parts Math, One Part Biology

The three sublayers of Bitcoin

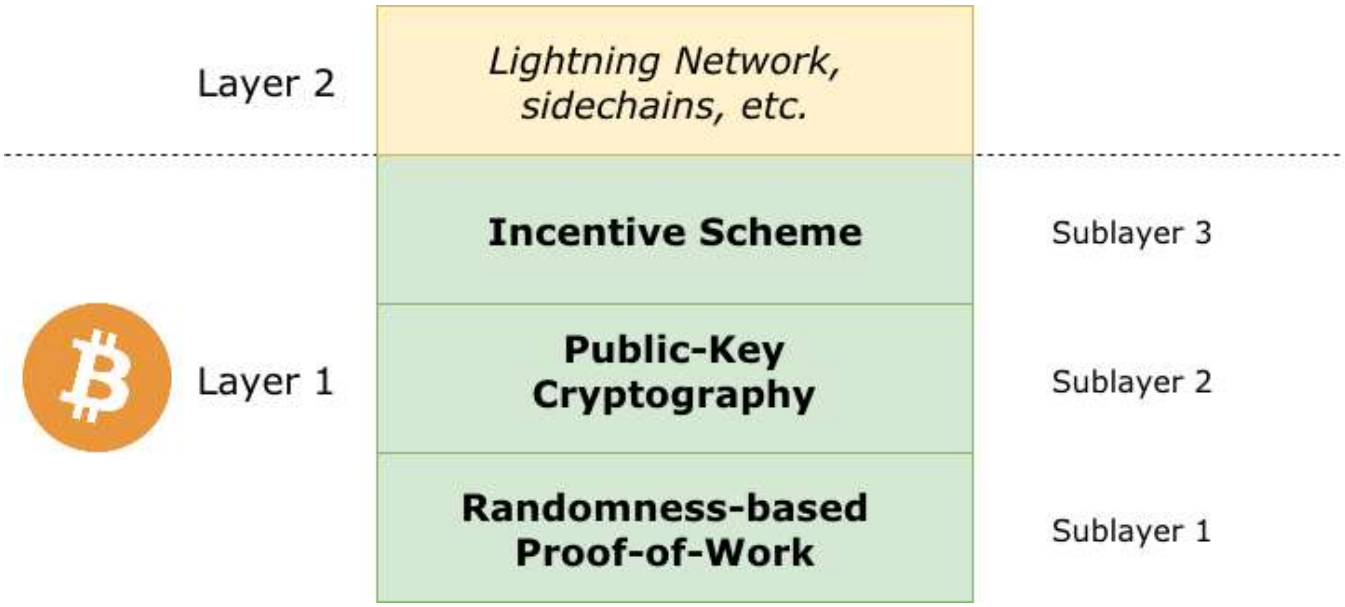
Bitcoin is composed of 3 fundamental building blocks:

(i) Randomness-based Proof-of-Work

(ii) Public-key cryptography

(iii) Incentive scheme

If we consider Bitcoin as a base layer upon which further layers can be built upon (such as the Lightning Network, TumbleBit or sidechains), then these building blocks can be viewed as sublayers within the base layer.



The 3 sublayers of Bitcoin base protocol

There is an implicit hierarchy among these sublayers. That is:

Sublayer 1: Proof-of-Work (PoW) forms the first sublayer. PoW approximates energy burnt and is the bridge between the digital world and the physical world. PoW gives digital blocks—which are just strings of 1s and 0s—real-world significance. With PoW, the Bitcoin ledger becomes an unforgeable and costly asset, with real weight behind it.

Sublayer 2: Public-key cryptography (PKC) forms the second sublayer. If PoW enables a new digital asset, then PKC and specifically digital signatures "tokenize" that asset, chopping it into pieces. Individuals can then store these pieces privately and exchange them with each other.

Sublayer 3: Finally, Bitcoin's incentive scheme forms the third sublayer, which sustains the system created by sublayers 1 and 2. Bitcoin is a dynamic network. It resembles a living organism whose heart beats roughly every 10 minutes. Bitcoin's incentive scheme provides the engine for this heartbeat, and is built on the token natively generated by sublayer 2.

Sublayer 2 wouldn't matter without sublayer 1. Sublayer 3 wouldn't matter without sublayers 1 and 2.

These sublayers together form the three-legged stool that is the foundation of the entire Bitcoin ecosystem. [3][4]

Two Parts Math, One Part Biology

From the exploration in the series, we have also learned that under the hood:

- Randomness-based PoW is based on math
- Public-key cryptography is also based on math
- Incentive scheme is based on human behavior

It can be said then, that Bitcoin is two parts math, one part biology.

It's worth noting that both randomness-based PoW and PKC rely on the same mathematical concept underneath, namely one-way function, but they form very distinct parts of the system. PoW creates the digital asset, while PKC tokenizes it.

The third sublayer of Bitcoin, incentive scheme, is arguably Bitcoin's weakest link. Unlike the first 2 sublayers, it relies on human behavior, which is less consistent and rigorous than mathematical principles. Human behavior exhibits bounded rationality, which is coded at the gene level, but imperfect. Humans are prone to miscalculations and occasional irrational behavior.

It remains to be seen whether Bitcoin's incentive scheme would be strong enough to hold the network together for the long term.

Final Words

I would like to close out the series by saying that in no way does this constitute a complete understanding of Bitcoin. But I hope it will serve as a good starting point for someone who is new to Bitcoin. Some of the content in this series are my own personal opinions. The reader would do well to do his or her own research and form their own opinions. "Don't trust, verify" works equally well in Bitcoin and in learning.

Acknowledgements

Special thanks to Nic Carter, Steve Lee, Jimmy Song, Hasu, Murad Mahmudov and Dan Held for their extremely valuable feedback in the writing of this series.

[1] The genesis message also doubled as proof that Satoshi did not unfairly premine before January 3rd, 2009.

[2] Bitcoin has experienced a dozen hours of "downtime": a combined total of 77 blocks where the network accidentally split, from 2 incidents in 2010 and 2013. This record is as impressive if not better than that of AWS, Google Cloud and Microsoft Azure.

[3] The term "cryptocurrency" derives from the use of public-key cryptography (sublayer 2), which ironically captures only one of many crucial aspects of this technology.

[4] These are the high-level building blocks. In practice the high-level building blocks are implemented using even smaller blocks. This includes hardware devices, software components, and communication protocols such as TCP/IP — each one bringing their own unique set of challenges.

Thanks to Dan Held.

Planting Bitcoin - Season (2/4)

Central Banks and the 2008 Financial Crisis

By Dan Held

Posted January 6, 2019

This is part 2 of a 4 part series

- Part 1: Planting Bitcoin - Species
- Part 2: Planting Bitcoin - Season
- Part 3: Planting Bitcoin - Soil
- Part 4: Planting Bitcoin - Gardening

"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. Banks must be trusted to hold our money and transfer it electronically, but they lend it out in waves of credit bubbles with barely a fraction in reserve."—Satoshi Nakamoto

Introduction

In my last article, "Species," I covered why Satoshi's design of Bitcoin's genetic code made it the best species of money ever created.

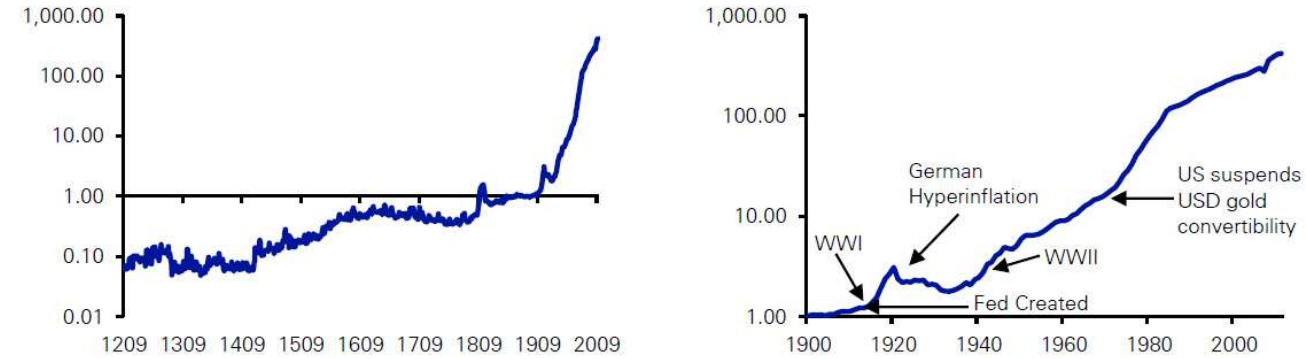
Satoshi had begun crafting Bitcoin's genetic code in 2007 but had waited for the right moment to plant the seed, the right moment in which the world would understand and embrace what he had created. In this article, I will dive into the moment in which Satoshi precisely chose to plant the Bitcoin seed.

Central Banks

From the founding of the Bank of England, central banks have been used as a means for states to fund their policies without risking the popular ire caused by direct taxation. When the capital provided by central banks is misallocated by either the state or in a market distorted by artificially low interest rates, an inevitable collapse occurs. The central bank is the root of these periodic market dislocations.

"I believe the root cause of every financial crisis, the root cause, is flawed government policies"—Henry Paulson (US Treasury Secretary during the 2008 financial crisis and former Goldman Sachs CEO)

Figure 18: Global Median Inflation Series since 1209 (left) and 1900 (right)

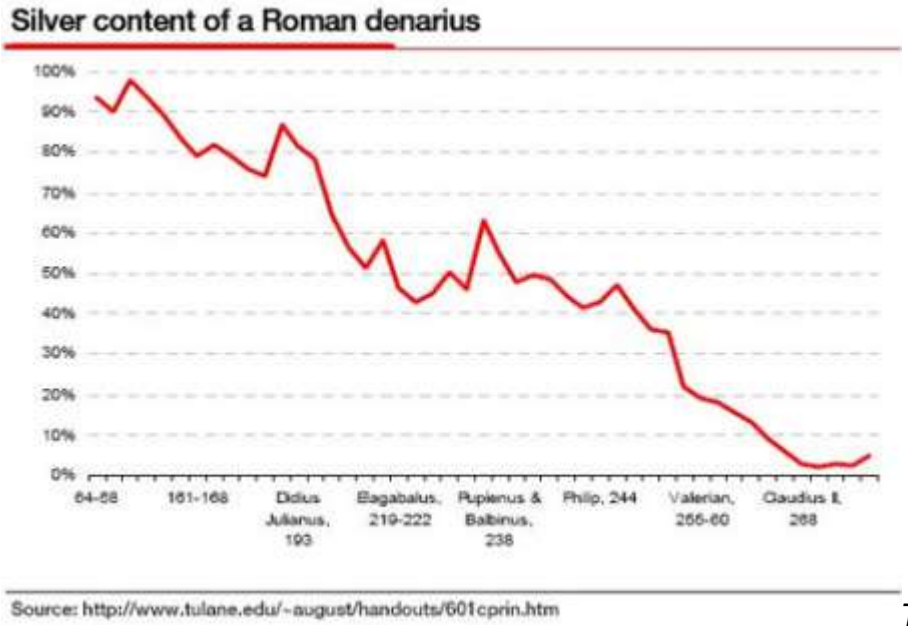


Source: Deutsche Bank, GFD

There hasn't been a year of global deflation since 1933

With the recent market dislocation, investors were bailed out. Unfortunately, you cannot subsidize irresponsibility and expect people to become more responsible. Prior to the 20th century, ordinary people could always flee to gold to save themselves from the effects of the failed, inflationist, policies of the central bank. This ended across much of the world in the 20th century as gold was outlawed.—Vijay Boyapati

"In the absence of the gold standard, there is no way to protect savings from confiscation through inflation. There is no safe store of value."—Alan Greenspan (Former Chairman of the Federal Reserve)



The standard Roman silver coin

Early 2007

Satoshi Nakamoto, after years and years of research, starts coding up Bitcoin.

2008 Financial Crisis

"The problem had grown so big that the end was bound to be cataclysmic and have big social and political consequences"—Michael Lewis (Big Short)

January

Fed tries to stop the housing bust

The Federal Market Open Committee began lowering the fed funds rate (to 3.0%). There were 57 percent more foreclosures than 12 months earlier

February

Bush signs tax rebate as home sales continue to plummet

February 13: President Bush signed a tax rebate bill to help the struggling housing market. The bill increased limits for FHA loans and allowed Freddie Mac to repurchase jumbo loans.

March

Fed begins bailouts

March 14: The Federal Reserve held its first emergency weekend meeting in 30 years.

March 17: The Federal Reserve announced it would guarantee Bear Stearns' bad loans.

March 18: The Federal Open Market Committee lowered the fed funds rate by 0.75 percent to 2.25 percent. It had halved the interest rate in six months. That same day, federal regulators agreed to let Fannie Mae and Freddie Mac take on another $200 billion in subprime mortgage debt.

April – June

The Fed buys more toxic bank debt

June 2: The Fed auctions totaled $1.2 trillion. In June, the Federal Reserve lent $225 billion through its Term Auction Facility.

July

IndyMac bank fails

July 11: The Office of Thrift Supervision closed IndyMac Bank. Los Angeles police warned angry IndyMac depositors to remain calm while they waited in line to withdraw funds from the failed bank.

July 23: Secretary Paulson made the Sunday talk show rounds. He explained the need for a bailout of Fannie Mae and Freddie Mac. The two agencies themselves held or guaranteed more than half of the $12 trillion of the nation's mortgages.

August

August 18: Satoshi registers Bitcoin.org through anonymousspeech.com

September *Global panic*

September 7: Treasury nationalizes Fannie and Freddie and will run the two until they are strong enough to return to independent management. The Fannie and Freddie bailout initially cost taxpayers $187 billion.

September 15: Lehman Brothers files for chapter 11 bankruptcy, the largest bankruptcy filing in U.S. history with over $600B in assets. The bankruptcy triggered a one-day drop in the Dow Jones Industrial Average of 4.5%, the largest decline since the September 11, 2001 attacks. Later that day, Bank of America officially announced it would purchase struggling Merrill Lynch for $50 billion.

"It's terrible. Death. Like a massive earthquake."—Kirsty McCluskey a Lehman trader in London

September 16: Fed buys AIG for $85 Billion. The company had insured trillions of dollars of mortgages throughout the world. If it had fallen, so would the global

banking system. On that same day, the Reserve Primary Fund "broke the buck." It didn't have enough cash on hand to pay out all the redemptions that were occurring.

"I asked my wife to please go to the ATM and take as much cash as she could. When she asked why, I said it was because I didn't know whether there was a chance that banks might not open."—Mohamed El-Erian (One of the most powerful economists/leaders in finance)

September 17: Economy on the brink of collapse. Panic spreads. Investors withdrew a record $144.5 billion from their money market accounts. During a typical week, only about $7 billion is withdrawn. If it had continued, businesses couldn't get money to fund their day-to-day operations. In just a few weeks, shippers wouldn't have had the cash to deliver food to grocery stores.

October *Bailouts*

October 3: Bitcoin whitepaper PDF likely created (not the first time it was written, but the first time it was prepared for publishing)

The same day, the bank bailout bill allowed Treasury to buy shares of troubled banks. It was the fastest way to inject capital into the frozen financial system. Despite this, global stock markets continue to collapse.

"Just as our politics are falling apart, our portfolios are falling apart, too."—Ben Hunt

October 7: The Federal Reserve agreed to issue short-term loans for businesses that couldn't get them elsewhere, to the tune of $1.7 Trillion.

October 13: Treasury Secretary Hank Paulson sits down with 9 major bank CEOs. The total bailout package looks more like $2.25 trillion, well more than the original $700 billion available.

"September and October of 2008 was the worst financial crisis in global history, including the Great Depression"—Ben Bernanke

October 14: The governments of the EU, Japan, and the United States again took unprecedented coordinated action . The EU committed to spending $1.8 trillion to guarantee bank financing, buy shares to prevent banks from failing, and take any other steps needed to get banks to lend to each other again. This was after the UK committed $88 billion to purchase shares in failing banks and $438 billion to guarantee loans. In a show of solidarity, the Bank of Japan agreed to lend unlimited dollars .

Debt/GDP ratios are at wartime highs. Central banks haven't unwound their 2008 trade

October 21—Fed lends $540 Billion to bail out money market funds which are continuing to meet a barrage of redemptions.

"People feel like nothing in the country is working—the president, Congress, corporations." (October 15, 2008) Reuters

October 31: Satoshi publishes the Bitcoin whitepaper

Walking on the street in a city Satoshi looks around and notices a businesswoman on her blackberry, hailing a cab. He passes a newspaper stand and sees Miley Cyrus' (known as Hannah Montana) controversial photos in Vanity Fair, she's 15.

George Bush's approval rating is at a record low of 21%, Congress is at 10%—just above its all-time low. Lehman Brothers had just collapsed a month prior.

"Is now the time? Is the world ready?" Satoshi thought to himself. He had spent the last few years coding up Bitcoin then writing the whitepaper. He had patiently

waited to release it to the world, but the moment had to be right... there was only one shot at this. “Is the whitepaper easy enough to read? I want to make sure this resonates with the cypherpunks, I’m hoping *cash* will be most understandable to the other members on the mailing list who have previously created e-currencies.”

“When the moment is ripe, a fanatic leader galvanizes the ripe population and pushes it to a point of no return. The leader translates the ideals published by the “men of words [cypherpunks]” into doctrines [whitepaper] promising sudden and spectacular change.”—*Eric Hoffer, author of “ The True Believer ” (via Tony Sheng)*

He returned to his home and reviewed the whitepaper for any glaring mistakes the 47th time, he couldn’t find any. He leaned back and stared at the wall. He realized this was the moment, it was time to plant the seed. He popped open his e-mail client, checked the draft e-mail to the cryptographer (cypherpunk) e-mailing list and pressed send. There was no going back.

“Indeed, Bitcoin rose like a phoenix from the ashes of the 2008 global financial catastrophe—a catastrophe that was precipitated by the policies of central banks like the Federal Reserve.”—Vijay Boyapati

With the 2008 financial crisis, trust had been lost in a world that ran on trust.

Bitcoin was launched in a time of absolute necessity, Satoshi planted the seed at precisely the right moment.

Planting Bitcoin - Gardening (4/4)

By Dan Held

Posted January 6, 2019

This is part 4 of a 4 part series

- Part 1: Planting Bitcoin - Species
- Part 2: Planting Bitcoin - Season
- Part 3: Planting Bitcoin - Soil
- Part 4: Planting Bitcoin - Gardening

Introduction

In my last article, "Soil," I covered the Cypherpunks or the "Soil" in which he planted the Bitcoin seed giving it the best chance for survival.

Satoshi's design of Bitcoin's genetic code made it the best species of money ever created, he waited for exactly the right moment to plant the seed, and had planted it in the most fertile soil. Now it was time to nurture Bitcoin's development.

Early Development

"The project needs to grow gradually so the software can be strengthened along the way."—Satoshi Nakamoto

Satoshi chose to be anonymous, which fit the ethos of the Cypherpunks. **People can project hopes and dreams on an anonymous individual, ensuring maximal narrative fit** . That's why a book is often better than the movie. His anonymity was a critical component of the founder story—dev worship is a dangerous thing for an open source project aiming for decentralization. Volunteers need to rely on trusting the objective reality of the code, rather than focusing on the merits of the project leader.

"It is high time for everyone involved in BTC to stop concerning themselves with the question of the identity of Nakamoto, and accept that **it does not matter to the operation of the technology, in the same way that the identity of the inventor of the wheel no longer matters**"- Saifedean Ammous

As a subtle jab to central banks, and as a nod to his admiration of the gold standard, **he chose his birthday (on his p2p foundation website profile) as the date the US made gold ownership illegal** through Executive Order 6102, April 5th. And he chose 1975 as his year of birth which is the year when the US citizens were allowed to own gold again.

"[with Bitcoin] **we can win a major battle in the arms race** and gain a new territory of freedom for several years."—Satoshi Nakamoto

In his public statements, he usually focused on ordinary, mainstream, users, with his tone sometimes even excited in suggesting many ways bitcoin could be made more convenient or useful for commerce or other things. Satoshi was practical, which made interactions very easy and comfortable. He tended to avoid philosophical discussions and political arguments.

Additionally, Satoshi took steps to signal to the Cypherpunks, and future members, that Bitcoin wasn't a scam. The conservative deescalation of his mining contributions, never spending any of his coins, nor using his influence for any purpose, shows that he wanted the world to make up their own mind about his

project and judge it on its own terms. **And unlike every other founder in history, Satoshi never cashed out.**

“Bitcoin benefited from an extremely rare set of circumstances. Because it launched in a world where digital cash had no established value, they circulated freely. That can’t be recaptured today since everyone expects coins to have value. Not only was it fair, but it was historically unique in its fairness. The immaculate conception.” Nic Carter

Many of the early Cypherpunks became core developers in the Bitcoin protocol like Hal Finney and Adam Bach. The caliber of the early development team attracted talented (soon to be “core”) developers.

“Gifted people tend to want to work with other top people and work on something that matters, that they believe in. **Motivation matters** . Protocol design and coding is partly an artistic, aesthetic endeavour; people do their best work on a mission: uncensorable global internet money”—Adam Bach

The Gardener Leaves

Satoshi showed a great level of restraint and took a long-term perspective on issues, as when Satoshi resisted the calls for bitcoin to market itself as a funding mechanism for Wikileaks after PayPal famously froze its account. This, Satoshi argued, would only bring down legal and regulatory hammers that much faster. Satoshi recognized the need to carefully cultivate Bitcoin.

“I make this appeal to WikiLeaks not to try to use Bitcoin. Bitcoin is a small beta community in its infancy. You would not stand to get more than pocket change, and **the heat you would bring would likely destroy us at this stage** .”—Satoshi Nakamoto

The connection to Wikileaks at such an early stage, at the height of what could be called public resistance against the Iraq war, probably gave Bitcoin a very different dimension. So he did not mince his words nor hide his intention for leaving in what can be called the last public statement where he says the US government was headed towards Bitcoin.

“It would have been nice to get this attention in any other context. WikiLeaks has kicked the hornet’s nest, and **the swarm is headed towards us** .”—Satoshi Nakamoto

In April 2011, Gavin Andressen notified Satoshi that he was meeting with the CIA. **Any further involvement might give away his identity which would endanger the long-term success of the project** . Bitcoin now had enough support that he could walk away, and so he did.

"Satoshi left because he didn't want its influence to affect the protocol development creating a single point of failure. The very idea of "Satoshi Vision" itself is against Satoshi's vision for Bitcoin"—Frederico Tenga

Social Scalability

Satoshi was able to walk away because Bitcoin had trust minimization baked into the protocol. This is what made it socially scalable.

"Power and scale breed conflict and corruption, that the purest part of any revolution is the beginning."—Dhruv Bansal

It is easy to start with good intentions, however as things scale that becomes harder and harder to maintain. **Bitcoin was specially architected to be trust minimized** . Satoshi set it up so that there is no one person or group whose power can be coveted, usurped, or broken.

"Bitcoin is a social breakthrough, not a technological one" — Alex Hardy

Bitcoin needed to be the universal language for money . You are communicating with strangers worldwide, which you neither know nor trust that agree you own an abstraction of value.

"Bitcoin is a distributed incentive structure we collectively engineer and freely opt-into. It's political technology, the first of its kind. This leaderless-ness is one part of what gives Bitcoin—in particular, beyond other cryptocurrencies today—such robustness."—Dhruv Bansal

HODLing, the Hero's Journey

"In the beginning of a change the patriot is a scarce man, and brave, and hated and scorned. When his cause succeeds, the timid join him, for then it costs nothing to be a patriot."—Mark Twain

Satoshi built Bitcoin for the believers in a new financial system, the HODLers, the revolutionaries. The ones who were disenfranchised with the existing financial system. The ones who would be attracted by the prospect of sudden and spectacular change in their life.

We must heed the call for a Hero's Journey (the HODLer) that is rooted in HODL. **It's not just a meme, it is representative of foundational values upon which stronger cultural memes are eventually developed** . This supports Bitcoin's cultural foundation.

"Over and over again, the financial system was, in some narrow way, discredited....The rebellion by American youth against the money culture never happened."—Big Short

The Hero at the beginning of their Journey has values that do not agree with the values that the Hero ends up with at Journey's end. That is the entire point of undertaking the Journey, but is also what makes it so frightening. **The Hero must let go of his/her former self in the pursuit of this transformed version of themselves.** The Journey's end is unknown, but what is known is that the Journey inspires the acquisition of new knowledge, the relinquishing of outdated paradigms and the abandoning of the familiar.The HODL Journey in Bitcoin sketches a map that becomes clearer with the acquisition of knowledge.

Satoshi needed to bootstrap the network with an incentive mechanism—the block reward which (a) controlled currency supply of Bitcoin and (b) created an incentive for people to participate in the network. **Each cycle brings aboard a new set of true believers; a new set of HODLers** . They, in their turn, become strong advocates for the adoption of Bitcoin as a store of value. Contagious Freedom. Vijay Boyapati

" **Hodling bootstrapped Bitcoin into existence.** Hodling increases value, which increases demand, hash rate, and network security, which, in turn, attracts new hodlers and devs. This self-reinforcing feedback loop drives Bitcoin's network effects, security, and value."—@TobiasAHuber

Satoshi had encoded in Bitcoin DNA a mechanism to incentivize the participants, through the shared belief in Bitcoin manifested via HODLing.

"In this sense, it's more typical of a precious metal. Instead of the supply changing to keep the value the same, the supply is predetermined and the value changes. As the number of users grows, the value per coin increases. I **t has the potential for a positive feedback loop; as users increase, the value goes up, which could attract more users to take advantage of the increasing value.**"—Satoshi Nakamoto

Early HODLers believed in Bitcoin despite overwhelming negativity and false information (ex: labeled as a currency for money launderers and drug dealers, price fluctuations). HODLers had stronger risk appetite to weather the volatility of being a first mover. They're practitioners of skin in the game.

In terms of the Hero's Journey, "HODL!" is the mentor's advice to the Hero in his Journey . Its roots are firmly based on the futility of trying to beat the market (Efficient Market Hypothesis and Hayekian Distributed information both dictate that the market can't be systematically outperformed).

The increase in Bitcoin's price has corresponding virality. And as it expands, HODLing becomes popular with people with a lower risk appetite, pulling in more and more network effect into the Bitcoin black hole—Dan McArdle

Via the Lindy Effect, the longer Bitcoin remains in existence the greater society's confidence that it will continue to exist long into the future. **It slowly seeps further into the psyche of those in charge.**

"Protocols die when they run out of believers."—Naval

The faith in a new financial system is what binds everything together. Bitcoin is not just a software project. It's a method of coordination for a large group of people who face powerful adversaries. Bitcoin isn't just a technological breakthrough, it's also a social one.

"When people are ripe for a mass movement, they are usually ripe for any effective movement, and not solely with a particular doctrine or program. All mass movements are competitive, and the gain of one in adherents is the loss of all the others....A stable and sustainable ideology must be the foundation of all cryptocurrencies. **No amount of cryptography, or consensus protocol development will help a cryptocurrency with an unstable and bankrupt ideology. Stable ideologies allow communities to thrive**". Kay Kurokawa

A simple example in religion is the Christian tenet that "there is one true god". This belief strengthens the religion because it weakens membership in competing religions. **Communities with unstable ideologies will eventually collapse.**

"Unlike Bitcoin, nobody needs to explain why gold is valuable. Gold is simple. Bitcoin is complicated. So in the long run, the argument goes, Bitcoin can never replace gold... It's true that the stories we tell matter, but those stories can change. **Stories don't win over everything. Eventually, raw utility supplants tradition. Bitcoin is a serious improvement over gold and starts to displace its role, the market will respond and re-price accordingly**... To the digital native of the future, Bitcoin wallets will probably seem more natural than vaults full of useless metals painstakingly drilled out of the earth."—Haseeb Qureshi

Money is a winner-take-all technology, driven by network effects. The crypto with the most HODLers, therefore, is the most demanded by consumers and will be the ultimate winner.

"Bitcoin is digital gold in the eyes of [HODLers]. To some extent this group already operates on a Bitcoin Standard: investments are evaluated on their ability to yield a return in Bitcoin." Tuur Demeester

HODL forces us to extend our gaze beyond the present. It forces our present selves to contend with an alternate reality. **HODL asks us to reconfigure our present set of preferences to permit the consideration of a future Bitcoin-based digital economy.**

HODL is a noble basis for a Journey. Through the sacrifice of current consumption, **HODLing is a net benefit for everyone as it increases every coin's purchasing power.**

"No Hero fights alone; All for one, one for all. Your call to HODL need not be the same as mine; indeed, they can be very different. Yet, in the end, they all redound to the benefit of each other."—Prateek Goorha

Bitcoin promises an alternative for citizens across the world to keep their savings in a form of money that can neither be confiscated nor diluted. If Bitcoin grows much larger, it may force governments to become a voluntary organization. **Through HODLing, we may finally be free.**

"The secret to happiness is freedom; the secret to freedom is courage"—Thucydides

Those who opt-in to Bitcoin, are trading something abundant for something scarce, **trading the past for the future, trading financial dependence for financial sovereignty.**

Conclusion

Satoshi architected the perfect genetic code necessary to a new species of money, Bitcoin. He then waited for the precise moment to plant the new species, the 2008 Financial Crisis. At that moment, he distributed the whitepaper to the only group that cared—the Cypherpunks. And finally, he nurtured Bitcoin to a stage where it no longer needed him.

Many digital cash systems came and went over the years before Bitcoin and after Bitcoin . Most were just whitepapers, some wrote and developed code, some even built a community, but it will be extremely difficult to repeat the success of Bitcoin's planting.

"Let the future tell the truth, and evaluate each one according to his work and accomplishments. The present is theirs; the future, for which I have really worked, is mine."—Nikola Tesla

---

Planting Bitcoin — Soil (3/4)

By Dan Held

Posted January 6, 2019

This is part 3 of a 4 part series

- Part 1: Planting Bitcoin - Species
- Part 2: Planting Bitcoin - Season
- Part 3: Planting Bitcoin - Soil
- Part 4: Planting Bitcoin - Gardening

Introduction

In my last article, "Season," I covered the precise moment in which Satoshi planted Bitcoin, the 2008 Financial Crisis. In this article, I cover the Cypherpunks or the "Soil" in which he planted the Bitcoin seed giving it the best chance for survival.

Cypherpunks

Sending the Bitcoin whitepaper to the cryptography mailing list on October 31, 2008 was the obvious choice. This was the right group to gather feedback from, the right channel to engage with. The list was predominately populated by the Cypherpunks * who were activists advocating widespread use of strong cryptography, as a route to social and political change.

"Cypherpunks" is a play on the word 'cipher' or 'cypher', for encryption; and cyberpunk a genre of sci-fi.

The group was originally comprised of Eric Hughes, Tim May, and John Gilmore. At first, the meetings were in-person meetings in the San Francisco Bay Area, but they decided to expand the group via the cryptographer mailing list which would allow them to reach other Cypherpunks. The mailing list was a place to exchange ideas freely through the use of encryption methods, such as PGP, to ensure complete privacy. The basic ideas behind this movement can be found in the Cypherpunk manifesto written by Eric Hughes in 1993. The key principle which underpins the manifesto is the importance of privacy and finality in transactions—PetriB

"Therefore, privacy in an open society requires anonymous transaction systems. Until now, cash has been the primary such system."—A Cypherpunk's Manifesto

We want the ability to ensure that others cannot use the information in the history of our transactions against us . For example: a purchase indicating that someone is wealthy, an embarrassing purchase, or one that would make you subject to spam or harassment. We do not want our financial purchase to haunt us further down the road. We want an endpoint beyond which we do not have to worry about further contingencies. **In the world of payments, this is closely related to the concept of**

"finality"—ideally we want to be able to state with certainty that at some point the payment has been made, the debt has been cleared, and the funds are secure. But recent developments have increased the ability for more powerful parties to clawback funds (via trusted third parties, legal funds, etc).

We hope that existing laws would provide protection against these difficulties. However, we can remove that moral hazard by not having to trust third parties or more powerful adversaries which can revert transactions solely based on their capabilities. This is what the Cypherpunks were fighting for with cryptography. They were the "Men of words," or anti-establishment intellectuals that laid the foundation for individuals like Satoshi to come along.

"The words of **anti-establishment intellectuals sow the seeds for revolution** . They present ideas and sometimes discredit the establishment, **paving the way for a charismatic leader to package their thinking into a movement** ."—Tony Sheng

Elliot Alderson, the "Cypherpunk" in the fictional show "Mr. Robot." He joins a group that aims to destroy all debt records by encrypting the financial data of the largest conglomerate in the world, E Corp.

Elliot Alderson, the "Cypherpunk" in the fictional show "Mr. Robot." He joins a group that aims to destroy all debt records by encrypting the financial data of the largest conglomerate in the world, E Corp.

The first attempts at making an anonymous transacting system were made by Cypherpunks on that cryptographer mailing list, including:

- Adam Back, the inventor of hashcash, the proof-of-work (PoW) system used by several anti-spam systems. A similar PoW system is used in bitcoin
- Nick Szabo, designed a mechanism for a decentralized digital currency he called "bit gold." Bit gold was never implemented, but has been called "a direct precursor to the Bitcoin architecture"
- Wei Dai, who published "b-money", an "anonymous, distributed electronic cash system"
- Hal Finny, who created the first reusable proof of work system before Bitcoin (And in January 2009 he became Bitcoin network's first transaction recipient). He was also a developer of the secure communication method known as Pretty Good Privacy (PGP)
- David Chaum, founded DigiCash (1989) as a form of centralized "electronic money" that deployed the same kinds of cryptographic protocols—public key cryptography—that support the nature of bitcoin transactions. It is often called "Chaumian eCash."

Satoshi cites many of these Cypherpunks in the Bitcoin whitepaper and references their influence on Bitcoin's development in public statements made post code launch.

"Bitcoin is an implementation of **Wei Dai's b-money** proposal... and **Nick Szabo's Bitgold** proposal"—Satoshi Nakamoto

In fact, Satoshi thought he was late to cryptocurrency! While the Cypherpunks had attempted many times to genetically code a species of money that would survive, none had been successful.

"A lot of people **automatically dismiss e-currency as a lost cause because of all the companies that failed since the 1990's** . I hope it's obvious it was only the centrally controlled nature of those systems that doomed them. I think this is the first time we're trying a decentralized, non-trust-based system."—Satoshi Nakamoto

He had written the whitepaper to fit his target audience, the Cypherpunks. That's why he uses the words "electronic cash", "proof-of-work," etc. which was previously used terminology in the other Cypherpunk whitepapers. He uses an ecommerce example to make it easier for everyone to comprehend. He's crafting a narrative that will resonate with the Cypherpunks, to get them interested and involved. **Bitcoin was the holy grail — it had solved the problem of finality and provided a small measure of privacy.** The source code implementation was his product spec.

"The **functional details** are not covered in the paper, but the sourcecode is coming soon."—Satoshi Nakamoto

The following things not described in the whitepaper, but are included in the source code: 21M hard cap, 10 minute blocks, 1 MB block caps. Those were incredibly important components of Bitcoin. The whitepaper was merely a teaser.

"If the Bitcoin Whitepaper is the **Declaration of Independence**, the Source Code is the **Constitution**"—Pierre Rochard

In true Cypherpunk fashion, the publication of Satoshi's whitepaper (October 2008) was quickly followed by code release in January 2009. The notion that good ideas need to be implemented, not just discussed, is very much part of the culture of the mailing list.

" **Cypherpunks write code** . We know that someone has to write software to defend privacy, and since we can't get privacy unless we all do, we're going to write it. **We publish our code so that our fellow Cypherpunks may practice and play with it** . Our code is free for all to use, worldwide... **We know that software can't be destroyed and that a widely dispersed system can't be shut down** ."—A Cypherpunk's Manifesto

Importantly, Satoshi didn't premine any Bitcoins. Satoshi gave the Cypherpunks a two month heads up before mining the Genesis block. To prove fairness, he included a proof of no premine timestamp in the Genesis Block of the Bitcoin blockchain. It carried a strong political message. What he was trying to accomplish was clear—they were building a new financial system. Bitcoin wasn't merely digital cash, it was an alternative to banks.

" The Times 03/Jan/2009 Chancellor on brink of second bailout for banks"—Genesis Block

---

Planting Bitcoin — Species (1/4)

Sound Money (sanum pecuniam)

By Dan Held

Posted January 6, 2019

This is part 1 of a 4 part series

- Part 1: Planting Bitcoin - Species
- Part 2: Planting Bitcoin - Season
- Part 3: Planting Bitcoin - Soil
- Part 4: Planting Bitcoin - Gardening

Foreword

I wrote this series, "Planting Bitcoin", to paint the origin story of Bitcoin leading up to the 10 year anniversary (10/31/2018). I felt that this story hadn't been told in a comprehensive and easy to read manner. I'd like to thank Jill Carlson for incepting this idea on the road trip back from Tahoe in early 2018.

Introduction

Bitcoin's origin is akin to planting a tree. It wasn't just Satoshi's selection of the species (code), but the season (timing), soil (distribution), and gardening (community) that were essential to its success. It had to grow to be strong, mighty, and huge. It

had to survive droughts, storms, and predators. Its deep roots had to support the weight of becoming a new world reserve currency.

What is Money

Money is most easily defined as the medium in which value is transferred. But Money is not just paper in your hand; or numbers in your bank account, Money represents something much more fundamental:

- Money is a primitive form of memory or record-keeping. It is the collective memory of who has the ability to allocate wealth.
- Money, which is the representation of the work required to acquire goods and services, can also be viewed as stored energy.
- Money is the central information utility of the world economy. As a medium of exchange, store of value, and unit of account, money is the critical vessel of information about the conditions of markets.

The main functions of money are Store of Value (SoV), Medium of Exchange (MoE), and Unit of Account (UoA). No money starts by providing all three functions, each new species of money follows a distinct evolutionary path that we will cover later. Let's first start by identifying the newest species of money, Bitcoin.

Species

"These protocols can't be described comprehensively as static objective things. They're best thought of as live systems"—Ari Paul

Bitcoin is a new form of life, a new species of money called "cryptocurrency." More importantly, it is "sound money," or using proper taxonomy, "sanum pecuniam." Sound money is defined as money that has a purchasing power determined by markets, independent of governments and political parties which is essential for individual freedom.

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

The code of life is written into an organism at its inception. Satoshi carefully architected Bitcoin's DNA, or genetic code, to be the best sound money ever created. We can think of Bitcoin's genetic code as representing instructions that have been written to incentivize the organization and coordination of cellular function.

"I believe I've worked through all those little details over the last year and a half while coding it, and there were a lot of them"- Satoshi Nakamoto

Bitcoin's genetic code:

- Satoshi needed a way for the Bitcoin to spark itself into existence, so he coded in its DNA a fixed supply (21M Bitcoins). An increase in Bitcoin's price inevitably leads to a corresponding increase in participants (users), security (mining), and developers. This becomes a self-reinforcing feedback loop.
- Bitcoin's mining function, Proof of Work (PoW) is both its metabolism and defense mechanism. Bitcoin eats energy to generate new coins and build digital walls to protect the network. PoW also makes Bitcoin anti-fragile, or in other words, as it grows larger, it becomes more resistant to attack.
- A new Bitcoin block is found every 10 minutes, this genetic code enables Bitcoin's cells to effectively communicate and coordinate with each other despite enormous distances. It is the internal clock that sets the metabolic rate.

"It lives and breathes on the internet. It lives because it can pay people to keep it alive. It lives because it performs a useful service that people will pay it to perform. It lives because anyone, anywhere, can run a copy of its code. It lives because all the running copies are constantly talking to each other. It lives because it is radically transparent: anyone can see its code and see exactly what it does. It can't be changed. It can't be argued with. It can't be tampered with. It can't be corrupted. It can't be stopped. It can't even be interrupted. If nuclear war destroyed half of our planet, it would continue to live, uncorrupted."—Ralph Merkle

Bitcoin's genetic code manifests itself via traits (characteristics of an organism) that may or may not be visible.

Traits

In biology, a trait or character is a feature of an organism. According to Charles Darwin's theory of evolution by natural selection, organisms that possess heritable traits that enable them to better adapt to their environment compared with other members of their species will be more likely to survive, reproduce, and pass more of their genes on to the next generation.

Money is no different. Money has traits that enable it to survive and thrive as a Store of Value (SoV), Medium of Exchange (MoE), and Unit of Account (UoA). Bitcoin is a new species that has vastly superior traits to its predecessors. Below we dive deeper into those traits between different species of money.

Traits of Money	Bitcoin	Gold	Fiat
Verifiable	High	Moderate	Moderate
Fungible	High	High	High
Portable	High	Low	High
Durable	Moderate	High	Low
Divisible	High	Low	Moderate
Scarce	High	Moderate	Low
Established History	Low	High	Low
Censorship resistant	High	Moderate	Low
Unforgeable Costliness	High	High	Low
***Openly Programmable**	High	Low	Low
***Decentralized**	High	Moderate	Low

Bitcoin's birth introduced two new traits, "Openly programmable" and "Decentralized"

(The sections below, on the attributes that make for a sound money, are largely borrowed from Vijay Boyapati 's article " The Bullish Case for Bitcoin ")

Verifiable

Fiat currencies and gold are fairly easy to verify for authenticity. However, despite providing features on their banknotes to prevent counterfeiting, nation-states and their citizens still face the potential to be duped by counterfeit bills. Gold is also not immune from being counterfeited. Sophisticated criminals have used gold-plated tungsten as a way of fooling gold investors into paying for false gold. Bitcoins, on the other hand, can be verified with absolute mathematical certainty.

Fungible

Gold provides the standard for fungibility. When melted down, an ounce of gold is nearly indistinguishable from any other ounce. Fiat currencies, on the other hand, are only as fungible as the issuing institutions allow them to be. While it may be the case that a fiat banknote is usually treated like any other by merchants accepting them, there are instances where large-denomination notes have been treated differently to small ones. For instance, India's government, in an attempt to stamp out India's untaxed gray market, completely demonetized their 500 and 1000 rupee banknotes.

Bitcoins are fungible at the network level, meaning that every bitcoin, when transmitted, is treated the same on the Bitcoin network. However, because bitcoins are traceable on the blockchain, a particular bitcoin may become tainted by its use in illicit trade and merchants or exchanges may be compelled not to accept such tainted bitcoins. Despite this, there is no alternative pricing for "tainted Bitcoins" so it remains highly fungible.

Portable

Bitcoins are the most portable store of value ever used by man. A single USB stick can contain a billion dollars, easily carried anywhere, transmitted near instantly. Fiat currencies, being fundamentally digital, are also highly portable. However, governments can control the free flow of capital. Cash can be used to avoid capital controls, but then the risk of storage and cost of transportation become significant. Gold, being physical in form and incredibly dense, is by far the least portable. When bullion is transferred between a buyer and a seller it is typically only the title to the gold that is transferred, not the physical bullion itself (It cost Germany $9.1 million to repatriate their gold).

Durable

Gold is the king of durability—the vast majority of gold that has ever been mined or minted, including the gold of the Pharaohs, remains today and will for near eternity (it can only be destroyed through nuclear transmutation). While fiat currency exists both in physical and digital forms, we will only consider the durability of its digital form... the durability of the institution that issues them. Many fiat issuing governments have come and gone over the centuries, and their currencies disappeared with them. If history is a guide, it would be folly to consider fiat currencies durable in the long term—the US dollar and British Pound are relative anomalies in this regard. Bitcoins, having no issuing authority, may be considered durable so long as the network that secures them remains in place. Given that Bitcoin is still in its infancy, it is too early to draw strong conclusions about its durability. However, there are encouraging signs that the network displays a remarkable degree of "anti-fragility ."

Divisible

Bitcoins can be divided down to a hundred millionth of a bitcoin and transmitted at such infinitesimal amounts. Fiat currencies are typically divisible down to pocket change, which has little purchasing power, making fiat divisible enough in practice. Gold, while physically divisible, becomes difficult to use when divided into small enough quantities that it could be useful for lower-value day-to-day trade.

Scarce

The attribute that most clearly distinguishes Bitcoin from fiat currencies and gold is its predetermined absolute scarcity: only 21 million bitcoins can ever be created (the number of units is arbitrary, as Bitcoins can be subdivided into 210 quadrillion satoshis). This gives the owner of bitcoins a known percentage of the total possible supply. Gold, while remaining quite scarce through history, is not immune to increases in supply. If it were ever the case that a new method of mining or acquiring gold became economic, the supply of gold could rise dramatically (ex: sea-floor or asteroid mining). Finally, fiat currencies, while only a relatively recent invention of history, have proven to be prone to constant increases in supply. Nation-states have shown a persistent proclivity to inflate their money supply to solve short-term political problems.

Established history

No monetary good has a history as long and storied as gold, which has been valued for as long as human civilization has existed. Coins minted in the distant days of antiquity still maintain significant value today . The same cannot be said of fiat currencies, which are a relatively recent anomaly of history. From their inception, fiat currencies have had a near-universal tendency toward eventual worthlessness. The use of inflation as an insidious means of invisibly taxing a citizenry has been a temptation that no states in history have been able to resist. Bitcoin, despite its short existence, has weathered enough trials in the market that there is a high likelihood it will not vanish as a valued asset any time soon. Furthermore, the Lindy effect suggests that the longer Bitcoin remains in existence the greater society's confidence that it will continue to exist long into the future. The median age of a human is ~30 years old, which means Bitcoin has been around for nearly 33.3% of the average human life. If Bitcoin exists for 20 years, there will be near-universal confidence that it will be available forever, much as people believe the Internet is a permanent feature of the modern world.

Censorship resistant

One of the most significant sources of early demand for bitcoins was their use in the illicit drug trade. Silk Road was a testament to this resistance. The key attribute that makes Bitcoin valuable for proscribed activities is that it is "permissionless" at the network level. When bitcoins are transmitted on the Bitcoin network, there is no human intervention deciding whether the transaction should be allowed. As a distributed peer-to-peer network, Bitcoin is, by its very nature, designed to be censorship-resistant. This is in stark contrast to the fiat banking system, where states regulate banks and the other gatekeepers of money transmission to report and prevent outlawed uses of monetary goods. A classic example of regulated money

transmission is capital controls. A wealthy millionaire, for instance, may find it very hard to transfer their wealth to a new domicile if they wish to flee an oppressive regime (Russian assets in the UK being frozen). Although gold is not issued by states, its physical nature makes it difficult to transmit at distance, making it far more susceptible to state regulation than Bitcoin. India's Gold Control Act is an example of such regulation. If your mission is to disrupt central banks, you need to have sovereign level censorship resistance.

"Bitcoin's advantages lie not in its speed, convenience, or friendly user experience. Bitcoin's value comes from it having an immutable monetary policy precisely because nobody can easily change it"—Saifedean Ammous

Unforgeable Costliness

Money that is costly to create. Due either to its original cost (gold mining) or the improbability of its history (art)—and that it is difficult to fake this costliness. Bitcoin's PoW ensures the cost to mine a Bitcoin is near equivalent to how much it would cost to purchase one on an exchange. The unforgeable costliness pattern includes the following basic steps:

"(1) find or create a class of objects that is highly improbable, takes much effort to make, or both, *and* such that the measure of their costliness can be verified by other parties.

(2) use the objects to enable a protocol or institution to cross trust boundaries"

- Nick Szabo

Openly Programmable

Bitcoin is open-source; its design is public, it is usable by anyone/anywhere/anytime. Developers can freely program applications on top of the Bitcoin protocol without having to ask anyone for permission.

"It is dynamic, upgradable and extendable. It does not need throwing out and replacing with each new iteration, it will continuously improve."—Neil Woodfine

Decentralized

In it's simplest definition, decentralization means a lack of centralized control. Or the degree to which an entity within the system can resist coercion and still function as part of the system. Coercion doesn't necessarily mean force, it means negative incentives to align with an authority. Decentralization is an important trait for money

because any centralized control could threaten any one of the other traits (especially scarcity and censorship resistance)

Decentralization is also important because it enables greater social scalability . The challenge is that natural systems inherently evolve towards centralization (hierarchies). We see this emergent property in cryptocurrencies as well. Hierarchy is an emergent property of networks. When we consider more complex systems, we must contend with more complex relationships between the layers. Quantifying decentralization is an especially thorny issue.

Decentralization is such a misunderstood concept, because people apply it to a whole system, when really it needs to be applied to multiple layers within the system: The Protocol, The Politics and The Practical.—Sarah Lewis

Evolution

For a species of money to survive, it needs to be competitive on every attribute and be exceptionally better on a few of them. Attributes don't sum, they multiply.

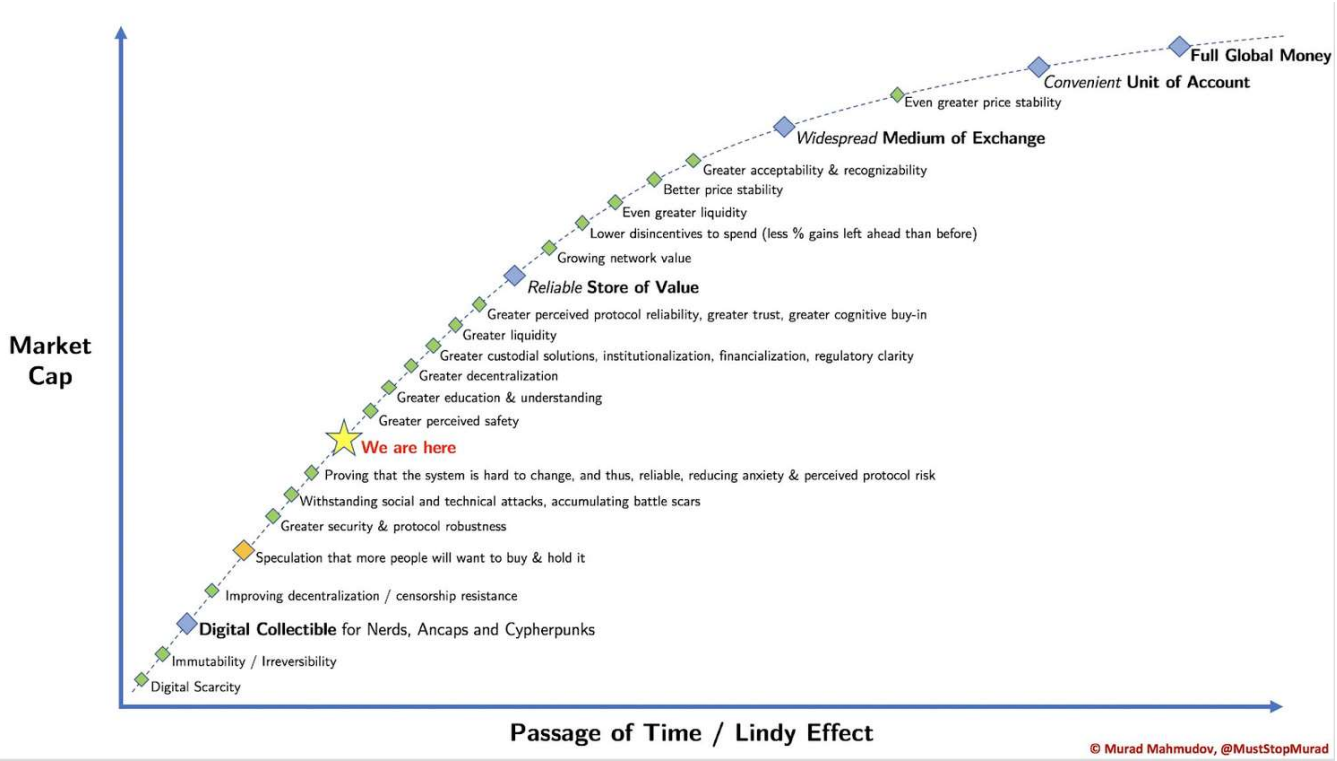
When Gold was first introduced, the bead makers (an example of a more primitive form of money) probably tried to convince the ignorant population that gold was no substitute for beads. But it turned out that gold had traits that were more advantageous. It did not matter what anyone thought. Gold was destined to be a more powerful currency than shells or beads.

The fact that gold has remained a valued commodity for thousands of years speaks to the importance of these specific traits. In fact, the combination of traits possessed by gold and other precious metals eventually provided the foundation for the next evolution in money, fiat currency. In money's next evolution of species, fiat currency fulfilled several critical traits to an even greater degree than gold. Paper was more portable and could be more easily transacted. That is not to say it was entirely superior. In many cases, fiat currencies lacked durability, and as we will see, would eventually become less and less scarce (due to inflation) The critical flaw: its supply was controlled by kings and governments and increasingly used as a tool to wield power and control. Upon every new iteration of species, they each evolve in the following four stages (taken from "The Bullish Case for Bitcoin"):

1. **Collectible**. In the very first stage of its evolution, money will be demanded solely based on its peculiar properties, usually becoming a whimsy of its possessor. Shells, beads and gold were all collectibles before later transitioning to the more familiar roles of money.
2. **Store of value**: Once it is demanded by enough people for its peculiarities, money will be recognized as a means of keeping and storing value over time.

As a good becomes more widely recognized as a suitable store of value, its purchasing power will rise as more people demand it for this purpose. The purchasing power of a store of value will eventually plateau when it is widely held and the influx of new people desiring it as a store of value dwindles.

3. **Medium of exchange**: When money is fully established as a store of value, its purchasing power will stabilize. Having stabilized in purchasing power, the opportunity cost of using money to complete trades will diminish to a level where it is suitable for use as a medium of exchange.
4. **Unit of account**. When money is widely used as a medium of exchange, goods will be priced in terms of it. I.e., the exchange ratio against money will be available for most goods.



Bitcoin's stage in the evolutionary process is shown below, provided by [Murad Mahmudov]

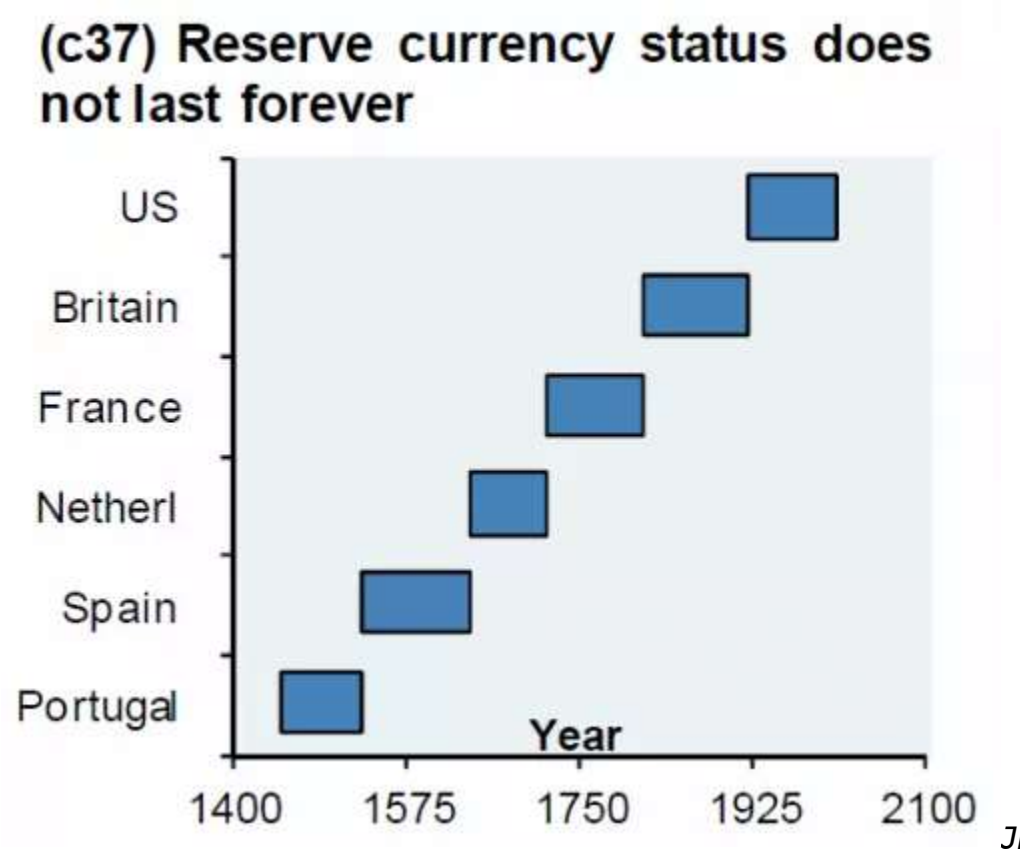
Bitcoin's stage in the evolutionary process is shown below, provided by Murad Mahmudov

Survival and Extinction

Extinction can most simply be described as the failure of a species to compete in an environment to such at a degree that it eventually ceases to exist. The inability to compete itself may be the result of two primary causes; increased competition from superior species or a dramatic change in environment.

"Charles Darwin's theory of natural selection originated to provide an evidence-based explanation of the past. We now leverage this theory to look forward and understand its implications on the future of currency. Given the ever-changing conditions of the future, will gold and fiat currencies continue to compete or go the way of the dinosaur?"—Ryan Walker "On the Origins of Money: Darwin and the Evolution of Cryptocurrency"

According to a study of 775 fiat currencies by DollarDaze.org the average life expectancy of a fiat currency is 27 years. The study also indicated the most common causes of any given currencies extinction are hyperinflation, monetary reform, war and independence. Looking towards the fittest of fiat currencies, those that become reserve currencies, we find that most last just under 100 years. (Note: US currency only starts from 1933 because USD was redeemable for gold prior to that)



JPM, Hong Kong Monetary Authority, December 2011

With fiat currencies being so susceptible to failure, gold has long served as an alternative as it is more scarce and durable. In terms of scarcity, fiat currencies can be printed and inflated at the will of their authorities.

"While Bitcoin is a new invention of the digital age, the problems it purports to solve—namely, providing a form of money that is under the full command of its

owner and likely to hold its value in the long run—are as old as human society itself"—Saifedean Ammous

The currencies are in a state of hyper-evolution as they continue to take on a varied array of distinctive traits that set them apart from one another within their own competitive ecosystem (fiat/crypto).

Equally as threatening to traditional forms of money, the conditions of the environment in which currencies compete is in a constant state of change. Undertones of growing distrust in centralized entities encourage populations to consider alternative stores of value.

Sovereignty, once a trait that was necessary for the survival of a currency, may now be falling out of favor. Centralized failures such as the US financial crisis of 2008 or hyper-inflated fiat currencies such as Zimbabwe dollars or Argentinian pesos compound these sentiments. The most profound of these conditions is the growing awareness throughout the world that decentralized trust is possible.

Instead of becoming anti-fragile, which is the property of growing stronger in a volatile and stressful environment, central banks have removed danger and mortality from failure, which causes competition to stagnate or degrade.

Sometimes stressors are so strong that they are fatal for a species of money. While this is devastating for the money itself, the population comprised of those that survive are fitter on average. This isn't because any of the survivors grew stronger from the stress, but simply because the weaker monies were removed.

"We humans regularly underestimate high-impact, long-tail events . Careful consideration of long tail events is especially important in the design of a protocol that has the potential to become the backbone of the global economy"—Hugo Nguyen

It is interesting to imagine what Charles Darwin would make of the current state of money. History would have us believe that the existence and survival of any entity, be it plant, animal, corporation, or money is subject to the laws of natural selection.

With this understanding, it is hard to imagine Darwin contesting the opinion that Bitcoin possesses the necessary traits to become the dominant species of money.

Bitcoin has been perfectly honed for its environment through its exceptional genetic code and the manifestation of that code in the form of superior traits.

Bitcoin is the apex predator of money and is constantly evolving. None of the previous monetary life forms stand a chance.

Bitcoin: Winner Takes Most or Winner Takes All?

Exploring market share capture in cryptocurrencies

By Misir Mahmudov and Yassine Elmandjra

Posted January 7, 2019

This series will explore how the winner-takes-all or winner-takes-most notion applies to the cryptocurrency market. In Part I, we will provide a high-level overview on the evolution of monetary systems up to the inception of cryptocurrencies, shedding light on the limitations of previous forms of money. In Part II, we will explain why the clear winner, likely Bitcoin, should capture most, if not all cryptocurrency market share. In Part III, we will apply this reasoning to the global economy and determine the extent to which the cryptocurrency market may capture a share of global base money.

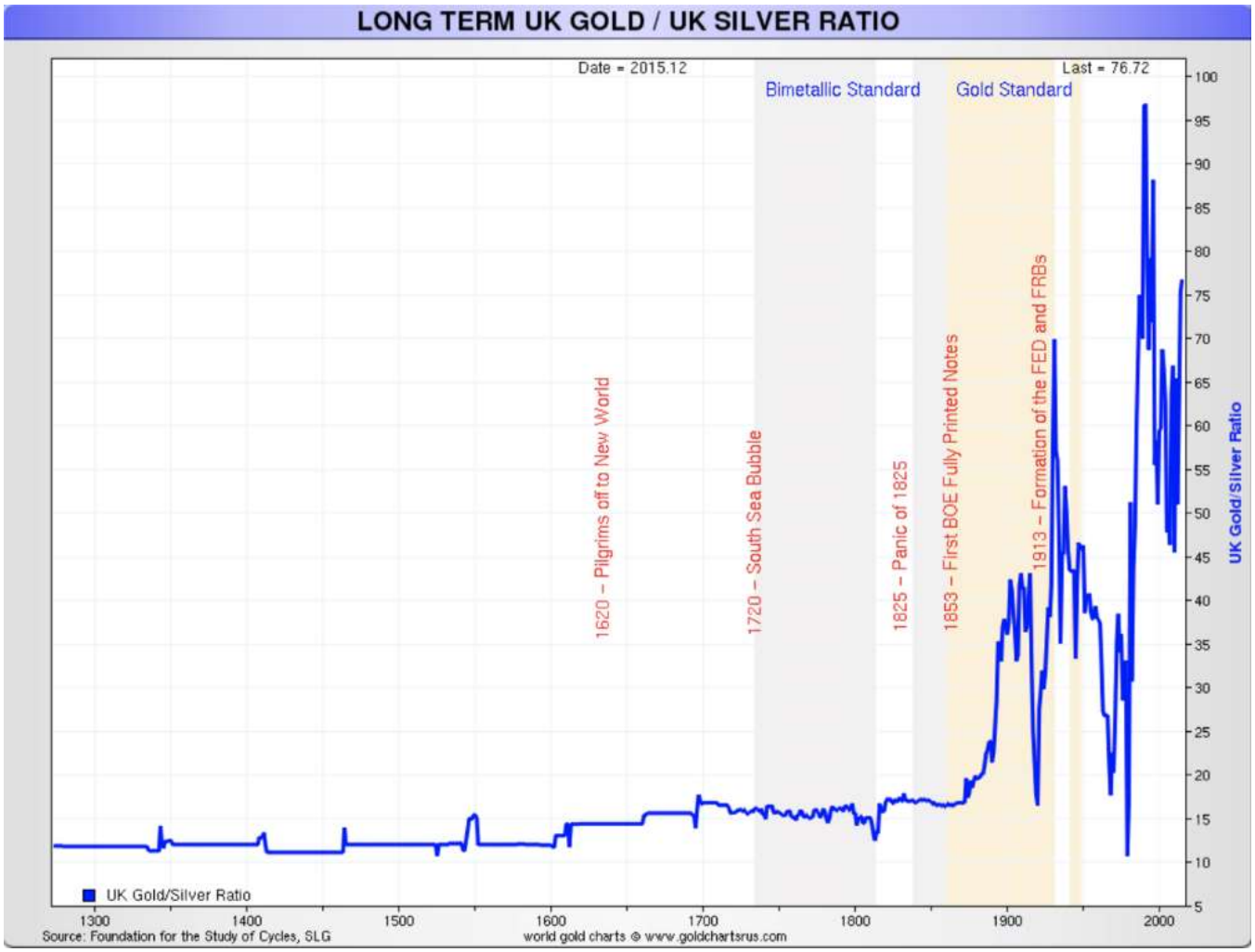
Part I: The Quest for a Global Money

Before the rise of any universal monetary standards, barter was a common means of direct exchange. Subject to the problem of coincidence of wants, civilization came to understand the impracticability of barter. In an attempt to provide a solution to this impracticality, indirect exchange emerged and was made possible with intermediary goods such as seashells, glass beads, and cattle. Over time, modern technologies (like mass utilization of hydrocarbon fuel energy and importation) considerably advanced manufacturing and transportation, making the world increasingly connected. Exploration and intercontinental trade became more prevalent, and the standard traits of money evolved to accommodate a more global context. This ultimately undermined existing media of exchange, as the lack of absolute scarcity and low costs of production could not provide money guarantees and were exploited by increasingly advanced technologies. Specifically, outside groups learned how to easily reproduce region-specific forms of money. Unaware of the absolute abundance of their money, nations suffered severe wealth dilution. [1]

As the limitations in existing forms of money began to manifest, specific properties of monetary goods emerged that better fulfilled money's store of value and medium of exchange functionalities, including scarcity, durability, portability, fungibility, verifiability, divisibility, and established history. Through a process of monetary natural selection, goods competed with each other based on these demanded

attributes and in the 19th century, the world converged to gold as the global monetary standard.

With the rise of gold, other forms of commodity money took form. Silver as a money was popularized because of the high costs associated with using gold in day-to-day trade. Silver's lower value per unit weight relative to gold made it easier to use for smaller transactions. [2] For centuries, the gold to silver ratio remained between 12 and 15 and was recognized as the bimetallic standard. But this bimetallic standard ended up as nothing but a temporary phenomenon adopted to overcome insufficient technology. With the introduction of paper money backed by gold, which gave people the ability to trade any amount of value represented in gold terms, silver's monetary role was subsequently reduced. The graph below shows how rapidly the gold to silver ratio soared after the popularization of paper money.

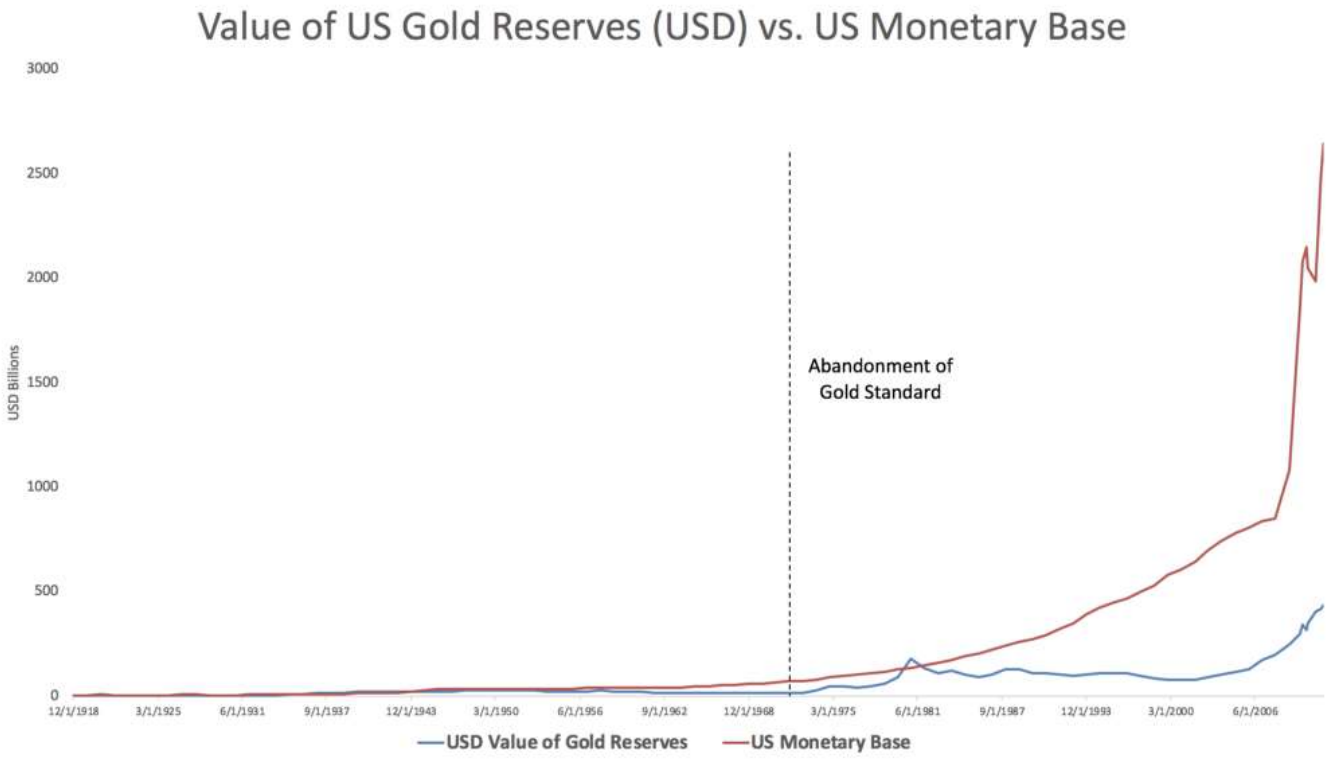


Gold / Silver Ratio https://www.goldbroker.com/news/gold-and-silver-correlation-988

Through financialization, gold's limitations to serve as a global money began to surface. In particular, gold's physical nature and high value per unit weight made it vulnerable to centralization and its detrimental effects. With gold's lack of portability and the high friction in using a scale to measure the amount of gold in every transaction, the state intervened to establish standardized units by minting (coining) gold coins. As citizens got acclimated with the conferred legitimacy and the infrastructure built around standardized units, the state felt comfortable engaging with what is known as 'coin clipping', a form of debasement whereby jurisdictions would reduce the content of gold in a coin and use the excess gold to finance expenditure at the cost of citizens.

Later, goldsmiths, who provided services for custodying precious metals, introduced promissory notes (IOUs) that were redeemable for metals. These notes (paper money) eventually became commonly used in exchange. The goldsmiths understood that they could lend out more notes than gold they had stored in their vaults because people were unlikely to simultaneously redeem their gold reserves. This practice became known as fractional reserve banking. Goldsmiths, which later became banks, issued receipts in excess of the represented metal and generated massive profits as a result.

The 18th and the 19th centuries saw the formalization of the Gold Standard as the proliferation of banknotes and the less sound nature of silver made itself known. The Gold Standard was a monetary system whereby a country's monetary supply was directly linked to the value of its gold reserves, putting a cap on a nation's ability to inflate supply. By the 20th century, states began exploiting the limitations of gold and abusing the practice of fractional reserve banking, ultimately removing its viability as a global money. The US was able to centralize gold reserves, often forcefully confiscating gold from its citizens, [3] and began printing money in excess of their underlying reserves. Instead of attempting to redeem themselves, the US under Richard Nixon cancelled the convertibility of the dollar into gold and officially abandoned the Gold Standard in 1971. Ties between gold and paper money were in turn severed, marking the beginnings of fully unbacked fiat currencies. Below is a chart of the US monetary base expansion relative to the value of US gold reserves.



Currencies... Currencies Everywhere.

Today, there exists over 180 currencies across 195 countries. The reason for such an anomaly is simple: there is no free market for currencies. Currency markets have been restricted by governments in order to maintain financial control. There are numerous laws and institutions set up for the exact purpose of inhibiting a free market monetary system. This includes enforced borders, legal tender laws, capital controls, state decrees, seigniorage privileges, local control, local monopolies on violence, debt extinguishing laws, capital gains taxes, implicit bailout guarantees for banks, central banks and dozens of other artificial barriers. This type of legislation forces people around the world to keep using inferior currencies under the threat of direct or indirect violence or repercussions. The centralized nature of the financial system and flows allows governments and institutions to impose these restrictions and greatly limit people's ability to express their true demand for superior, more competitive currencies. Fiat money's soundness is now dependent on an authority's ability to enforce legitimate monetary policy. People living in countries like Venezuela are unable to reliably store their wealth due to hyperinflation induced by irresponsible monetary policy and limited availability of more reliable currencies due to strict capital controls. In addition, as the only form of legal tender, citizens are obliged to pay taxes in and accept the inferior currency in exchange for goods and services. The more competitive currencies, like the dollar, that do make their way into countries like Venezuela, are sold at large premiums as the high demand is not met

by the controlled supply. Until recently, citizens of countries like Venezuela had no way to opt out of this system and were forced to adopt easy money.

The government's control of money has made it vulnerable to gross mismanagement. In an interview in 1984, Friedrich Hayek famously said: *"I don't believe we shall ever have a good money again before we take the thing out of the hands of government. 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."* And, in Free Market Monetary System , Friedrich Hayek notes that " *the monopoly of government of issuing money has not only deprived us of good money but has also deprived us of the only process by which we can find out what would be good money. We do not even quite know what exact qualities we want … because we have never been allowed to experiment with it. We have never been given a chance to find out what the best kind of money would be."*

Enter Bitcoin: The Experiment That Allows Us To Experiment

In 2008, Satoshi Nakamoto proposed Bitcoin, an alternative financial system free from top-down control. Bitcoin, "a system for electronic transactions without relying on trust", was not created to fit existing governments and financial systems.

Bitcoin is the experiment that allows us to experiment. Unlike any money of the past, Bitcoin is borderless, permissionless, censorship-resistant, and easily verifiable. As such, Bitcoin may precisely be this "sly roundabout way" that bypasses prohibitive mechanisms and legacy financial institutions that restrict people's access to a free market for money. Bitcoin is often referred to as digital gold because it maintains and improves upon most of gold's properties, including scarcity and unforgeable costliness. Given its digital nature, bitcoins are easily divisible, portable and unseizable, which enables it to be much better protected from the threats of centralization and the fate experienced by gold. First introduced by Vijay Boyapati and then further expanded upon by Dan Held, below is a table assessing Bitcoin, gold and fiat's ability to fulfill the traits of money.

Traits of Money	Bitcoin	Gold	Fiat
Verifiable	High	Moderate	Moderate
Fungible	High	High	High
Portable	High	Low	High
Durable	Moderate	High	Low
Divisible	High	Low	Moderate
Scarce	High	Moderate	Low
Established History	Low	High	Low
Censorship resistant	High	Moderate	Low
Unforgeable Costliness	High	High	Low
***Openly Programmable**	High	Low	Low
***Decentralized**	High	Moderate	Low

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

The Rise of Cryptocurrencies

Cryptocurrencies are first and foremost money . With the exception of a few, 'crypto-tokens' are either clearly intended to be money or are intended to be money but are obfuscated by technological jargon. As Bitcoin's community grew and its prices rose, other cryptocurrencies (often referred to as altcoins) began to hit the market. Many of these cryptocurrencies were built in an attempt to iterate and improve upon Bitcoin's "fundamental design flaws" and "limited functionality". In 2018, ten years after Bitcoin's inception, there are now over 2,000 cryptocurrencies .

Contrary to the 20th century's locally nationalized market for money, the cryptocurrency market much better resembles a competitive private market where no coercive monopolies distort price signals by preventing competitors from entering. Given the open source nature of cryptocurrencies, anyone is free to create their own or modify existing ones, which is as simple as copying the publicly available code of an existing cryptocurrency. This in turn encourages open and inexpensive experimentation.

The open source nature of cryptocurrencies is a promising mechanism to determine what the natural money of society might be. As Jörg Guido Hülsmann highlights in

the Ethics of Money Production, *"the only way to find out the natural money of society is to let people freely associate and choose the best means of exchange out of the available alternatives."*

Assuming operation under a free market, the question then becomes to what extent the natural money captures market share. While today's world has manifested itself differently, a glimpse of a winner take most, if not all, reality was seen with gold. Assuming a long-term time horizon, this same glimpse of reality may play out with cryptocurrencies, this time as more than just a temporary phenomenon.

In Part II, we explore in depth the validity of a winner-takes-all narrative. By defining market size to be the total monetary premium of all cryptocurrencies and deriving what drives a good's monetary premium, we shed light on the merits of such a narrative.

(1) Rai stones in Yap and glass beads in West Africa (2) Using gold was impractical for daily purchases as it required measuring and dividing it into small quantities. (3) In 1933, Roosevelt's Executive Order 6102 forbade the hoarding of gold coin and bullion

---

Economic Teachings of Bitcoin

What I've Learned From Bitcoin: Part II

Gigi

Posted January 11, 2019

This is part 2 of a 3 part series

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

Money doesn't grow on trees. To believe that it does is foolish, and our parents make sure that we know about that by repeating this saying like a mantra. We are encouraged to use money wisely, to not spend it frivolously, and to save it in good times to help us through the bad. Money, after all, does not grow on trees.

Bitcoin taught me more about money than I ever thought I would need to know. Through it, I was forced to explore the history of money, banking, various schools of economic thought, and many other things. The quest to understand Bitcoin lead me down a plethora of paths, some of which I try to explore in this series. This is the second of three parts:

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

In Part I of this series, some of the philosophical questions Bitcoin touches on were discussed. Part II will take a closer look at money and economics. Again, I will only be able to scratch the surface. Bitcoin is not only ambitious, but also broad and deep in scope, making it impossible to cover all relevant topics in a single essay, article, or book. I am starting to doubt if it is even possible at all.

Bitcoin is a child of many disciplines. Being a new form of money, learning about economics is paramount in understanding it. Dealing with the nature of human action and the interactions of economic agents, economics is probably one of the largest and fuzziest pieces of the Bitcoin puzzle.

Blind monks examining Bitcoin

Like the first part, this essay is an exploration of the various things I have learned from Bitcoin. And just like the first part, it is a personal reflection of my journey down the rabbit hole. Having no background in economics, I am definitely out of my comfort zone and aware that any understanding I might have is incomplete. Like blind monks examining an elephant, everyone who approaches this novel technology does so from a different angle and will come to different conclusions. Blindfolded as I am, I will try to outline what I have learned, even at the risk of making a fool out of myself. After all, I am still trying to answer the question:

"What have you learned from Bitcoin?"

After seven lessons examined through the lens of philosophy, let's use the lens of economics to look at seven more. I hope that you will find the world of Bitcoin as educational, fascinating and entertaining as I did and still do. In any case, hop on and enjoy the ride. Economy class is all I can offer this time. Final destination: sound money.

Find lessons 1-7 here.

Lesson 8: Financial Ignorance

One of the most surprising things, to me, was the amount of finance, economics, and psychology required to get a grasp of what at first glance seems to be a purely *technical* system—a computer network. To paraphrase a little guy with hairy feet: "It's a dangerous business, Frodo, stepping into Bitcoin. You read the whitepaper, and if you don't keep your feet, there's no knowing where you might be swept off to."

To understand a new monetary system, you have to get acquainted with the old one. I began to realize very soon that the amount of financial education I enjoyed in the educational system was essentially *zero*.

Like a five-year-old, I began to ask myself a lot of questions: How does the banking system work? How does the stock market work? What is fiat money? What is *regular* money? Why is there so much debt? How much money is actually printed, and who decides that?

After a mild panic about the sheer scope of my ignorance, I found reassurance in realizing that I was in good company.

"Isn't it ironic that Bitcoin has taught me more about money than all these years I've spent working for financial institutions? ...including starting my career at a central bank"—aarontaycc "I've learned more about finance, economics, technology, cryptography, human psychology, politics, game theory, legislation, and myself in the last three months of crypto than the last three and a half years of college"—bitcoindunny

These are just two of the many confessions all over twitter. Bitcoin, as was explored in part one, is a living thing. Mises argued that economics also is a living thing. And as we all know from personal experience, living things are inherently difficult to understand.

"A scientific system is but one station in an endlessly progressing search for knowledge. It is necessarily affected by the insufficiency inherent in every human effort. But to acknowledge these facts does not mean that present-day economics is backward. It merely means that economics is a living thing—and to live implies both imperfection and change." —Ludwig von Mises

We all read about various financial crises in the news, wonder about how these big bailouts work and are puzzled over the fact that no one ever seems to be held accountable for damages which are in the trillions. I am still puzzled, but at least I am starting to get a glimpse of what is going on in the world of finance.

Some people even go as far as to attribute the general ignorance on these topics to systemic, willful ignorance. While history, physics, biology, math, and languages are all part of our education, the world of money and finance surprisingly is only explored superficially, if at all. I wonder if people would still be willing to accrue as much debt as they currently do if everyone would be educated in personal finance and the workings of money and debt. Then I wonder how many layers of aluminum make an effective tinfoil hat. Probably three.

"Those crashes, these bailouts, are not accidents. And neither is it an accident that there is no financial education in school. [...] It's premeditated. Just as prior to the Civil War it was illegal to educate a slave, we are not allowed to learn about money in school." —Robert Kiyosaki

Like in The Wizard of Oz, we are told to pay no attention to the man behind the curtain. Unlike in The Wizard of Oz, we now have real wizardry: a censorship-resistant, open, borderless network of value-transfer. There is no curtain, and the magic is visible to anyone.

Bitcoin taught me to look behind the curtain and face my financial ignorance.

Lesson 9: Inflation

Trying to understand monetary inflation, and how a non-inflationary system like Bitcoin might change how we do things, was the starting point of my venture into economics. I knew that inflation was the rate at which new money was created, but I didn't know too much beyond that.

While some economists argue that inflation is a good thing, others argue that "hard" money which can't be inflated easily —as we had in the days of the gold standard—is essential for a healthy economy. Bitcoin, having a fixed supply of 21 million, agrees with the latter camp.

Usually, the effects of inflation are not immediately obvious. Depending on the inflation rate (as well as other factors) the time between cause and effect can be several years. Not only that, but inflation affects different groups of people more than others. As Henry Hazlitt points out in *Economics in One Lesson*: "The art of economics consists in looking not merely at the immediate but at the longer effects of any act or policy; it consists in tracing the consequences of that policy not merely for one group but for all groups."

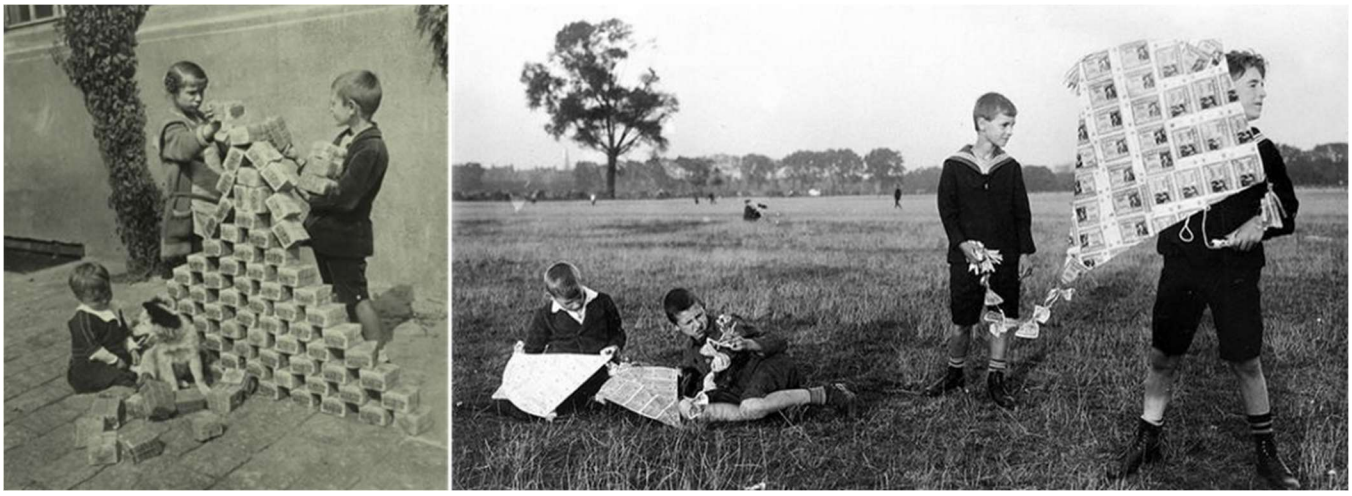
One of my personal lightbulb moments was the realization that issuing new currency—printing more money—is a *completely* different economic activity than all the other economic activities. While real goods and real services produce real value

for real people, printing money effectively does the opposite: it takes away value from everyone who holds the currency which is being inflated.

“Mere inflation—that is, the mere issuance of more money, with the consequence of higher wages and prices—may look like the creation of more demand. But in terms of the actual production and exchange of real things it is not.” —Henry Hazlitt

The destructive force of inflation becomes obvious as soon as a little inflation turns into *a lot*. If money hyperinflates, things get ugly real quick. As the inflating currency falls apart, it will fail to store value over time and people will rush to get their hands on any goods which might do.

Another consequence of hyperinflation is that all the money which people have saved over the course of their life will effectively vanish. The paper money in your wallet will still be there, of course. But it will be exactly that: worthless paper.



Hyperinflation in the Weimar Republic (1921-1923)

Money declines in value with so-called “mild “ inflation as well. It just happens slowly enough that most people don’t notice the diminishing of their purchasing power. And once the printing presses are running, currency can be easily inflated, and what used to be mild inflation might turn into a strong cup of inflation by the push of a button. As Friedrich Hayek pointed out in one of his essays, mild inflation usually leads to outright inflation.

""Mild” steady inflation cannot help—it can lead only to outright inflation.”

—Friedrich Hayek

Inflation is particularly devious since it favors those who are closer to the printing presses. It takes time for the newly created money to circulate and prices to adjust, so if you are able to get your hands on more money before everyone else’s devaluates you are ahead of the inflationary curve. This is also why inflation can be seen as a

hidden tax because in the end governments profit from it while everyone else ends up paying the price.

“I do not think it is an exaggeration to say history is largely a history of inflation, and usually of inflations engineered by governments for the gain of governments.”

—Friedrich Hayek

So far, all government-controlled currencies have eventually been replaced or have collapsed completely. No matter how small the rate of inflation, “steady” growth is just another way of saying exponential growth. In nature as in economics, all systems which grow exponentially will eventually have to level off or suffer from catastrophic collapse.

“It can’t happen in my country,” is what you’re probably thinking. You don’t think that if you are from Venezuela, which is currently suffering from hyperinflation. With an inflation rate of over 1 million percent, money is basically worthless.

It might not happen in the next couple of years, or to the particular currency used in your country. But a glance at the list of historical currencies shows that it will inevitably happen over a long enough period of time. I remember and used plenty of those listed: the Austrian schilling, the German mark, the Italian lira, the French franc, the Irish pound, the Croatian dinar, etc. My grandma even used the Austro-Hungarian Krone. As time moves on, the currencies currently in use will slowly but surely move to their respective graveyards. They will hyperinflate or be replaced. They will soon be historical currencies. We will make them obsolete.

“History has shown that governments will inevitably succumb to the temptation of inflating the money supply.” —Saifedean Ammous

Why is Bitcoin different? In contrast to currencies mandated by the government, monetary goods which are not regulated by governments, but by the laws of physics, tend to survive and even hold their respective value over time. The best example of this so far is gold, which, as the aptly-named *Gold-to-Decent-Suit Ratio* shows, is holding its value over hundreds and even thousands of years. It might not be perfectly “stable”— a questionable concept in the first place—but the value it holds will at least be in the same order of magnitude.

If a monetary good or currency holds its value well over time and space, it is considered to be *hard*. If it can’t hold its value, because it easily deteriorates or inflates, it is considered a *soft* currency. The concept of hardness is essential to understand Bitcoin and is worthy of a more thorough examination. We will return to it in the last economic lesson: sound money.

As more and more countries suffer from hyperinflation, more and more people will have to face the reality of hard and soft money. If we are lucky, maybe even some central bankers will be forced to re-evaluate their monetary policies. Whatever might happen, the insights I have gained thanks to Bitcoin will probably be invaluable, no matter the outcome.

Bitcoin taught me about the hidden tax of inflation and the catastrophe of hyperinflation.

Lesson 10: Value

Value is somewhat paradoxical, and there are multiple theories which try to explain why we value certain things over other things. People have been aware of this paradox for thousands of years. As Plato wrote in his dialogue with Euthydemus, we value some things because they are rare, and not merely based on their necessity for our survival.

"And if you are prudent you will give this same counsel to your pupils also—that they are never to converse with anybody except you and each other. For it is the rare, Euthydemus, that is precious, while water is cheapest, though best, as Pindar said."

—Plato

This paradox of value shows something interesting about us humans: we seem to value things on a subjective basis, but do so with certain non-arbitrary criteria. Something might be *precious* to us for a variety of reasons, but things we value do share certain characteristics. If we can copy something very easily, or if it is naturally abundant, we do not value it.

It seems that we value something because it is scarce (gold, diamonds, time), difficult or labor-intensive to produce, can't be replaced (an old photograph of a loved one), is useful in a way in which it enables us to do things which we otherwise couldn't, or a combination of those, such as great works of art.

Bitcoin is all of the above: it is extremely rare (21 million), increasingly hard to produce (reward halvening), can't be replaced (a lost private key is lost forever), and enables us to do some quite useful things. It is arguably the best tool for value transfer across borders, virtually resistant to censorship and confiscation in the process, plus, it is a self-sovereign store of value, allowing individuals to store their wealth independent of banks and governments, just to name two.

Bitcoin taught me that value is subjective but not arbitrary.

Lesson 11: Money

What is money? We use it every day, yet this question is surprisingly difficult to answer. We are dependent on it in ways big and small, and if we have too little of it our lives become very difficult. Yet, we seldom think about the thing which supposedly makes the world go round. Bitcoin forced me to answer this question over and over again: What the hell is money?

In our "modern" world, most people will probably think of pieces of paper when they talk about money, even though most of our money is just a number in a bank account. We are already using zeros and ones as our money, so how is Bitcoin different? Bitcoin is different because at its core it is a very different *type* of money than the money we currently use. To understand this, we will have to take a closer look at what money is, how it came to be, and why gold and silver was used for most of commercial history.

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

—Satoshi Nakamoto

Seashells, gold, silver, paper, bitcoin. In the end, **money is whatever people use as money**, no matter its shape and form, or lack thereof.

Money, as an invention, is ingenious. A world without money is insanely complicated: How many fish will buy me new shoes? How many cows will buy me a house? What if I don't need anything right now but I need to get rid of my soon-to-be rotten apples? You don't need a lot of imagination to realize that a barter economy is maddeningly inefficient.

The great thing about money is that it can be exchanged for *anything else*—that's quite the invention! As Nick Szabo brilliantly summarizes in *Shelling Out: The Origins of Money*, we humans have used all kinds of things as money: beads made of rare materials like ivory, shells, or special bones, various kinds of jewelry, and later on rare metals like silver and gold.

Being the lazy creatures we are, we don't think too much about things which just work. Money, for most of us, works just fine. Like with our cars or our computers, most of us are only forced to think about the inner workings of these things if they break down. People who saw their life-savings vanish because of hyperinflation know the value of hard money, just like people who saw their friends and family vanish because of the atrocities of Nazi Germany or Soviet Russia know the value of privacy.

The thing about money is that it is all-encompassing. Money is half of every transaction, which imbues the ones who are in charge with creating money with enormous power.

“Given that money is one half of every commercial transaction and that whole civilizations literally rise and fall based on the quality of their money, we are talking about an awesome power, one that flies under the cover of night. It is the power to weave illusions that appear real as long as they last. That is the very core of the Fed’s power.”

—Ron Paul

Bitcoin peacefully removes this power, since it does away with money creation and it does so without the use of force.

Money went through multiple iterations. Most iterations were good. They improved our money in one way or another. Very recently, however, the inner workings of our money got corrupted. Today, almost all of our money is simply created *out of thin air* by the powers that be. To understand how this came to be I had to learn about the history and subsequent downfall of money.

If it will take a series of catastrophes or simply a monumental educational effort to correct this corruption remains to be seen. I pray to the gods of sound money that it will be the latter.

Bitcoin taught me what money is.

Lesson 12: The history and downfall of money

Many people think that money is backed by gold, which is locked away in big vaults, protected by thick walls. This ceased to be true many decades ago. I am not sure what I thought, since I was in much deeper trouble, having virtually no understanding of gold, paper money, or why it would need to be backed by something in the first place.

One part of learning about Bitcoin is learning about fiat money: what it means, how it came to be, and why it might not be the best idea we ever had. So, what exactly is fiat money? And how did we end up using it?

If something is imposed by *fiat*, it simply means that it is imposed by formal authorization or proposition. Thus, fiat money is money simply because *someone* says that it is money. Since all governments use fiat currency today, this someone is *your* government. Unfortunately, you are not *free* to disagree with this value proposition. You will quickly feel that this proposition is everything but non-violent. If you refuse to use this paper currency to do business and pay taxes the only people you will be able to discuss economics with will be your cellmates.

The value of fiat money does not stem from its inherent properties. How good a certain type of fiat money is, is only correlated to the political and fiscal (in)stability of those who dream it into existence. Its value is imposed by decree, arbitrarily.

fi·at /ˈfēˌät,ˈfēət/ — "Let it be done"

Until recently, two types of money were used: **commodity money**, made out of precious *things*, and **representative money**, which simply *represents* the precious thing, mostly in writing.

We already touched on commodity money above. People used special bones, seashells, and precious metals as money. Later on, mainly coins made out of precious metals like gold and silver were used as money. The oldest coin found so far is made of a natural gold-and-silver mix and was made more than 2700 years ago. If something is new in Bitcoin, the concept of a coin is not it.

Lydian electrum coin

Turns out that hoarding coins, or hodling, to use today's parlance, is almost as old as coins. The earliest coin hodler was someone who put almost a hundred of these coins in a pot and buried it in the foundations of a temple, only to be found 2500 years later. Pretty good cold storage if you ask me.

One of the downsides of using precious metal coins is that they can be clipped, effectively debasing the value of the coin. New coins can be minted from the clippings, inflating the money supply over time, devaluing every individual coin in the

process. People were literally shaving off as much as they could get away with of their silver dollars. I wonder what kind of *Dollar Shave Club* advertisements they had back in the day.

Since governments are only cool with inflation if they are the ones doing it, efforts were made to stop this guerrilla debasement. In classic cops-and-robbers fashion, coin clippers got ever more creative with their techniques, forcing the 'masters of the mint' to get even more creative with their countermeasures. Isaac Newton, the world-renowned physicist of *Principia Mathematica* fame, used to be one of these masters. He is attributed with adding the small stripes at the side of coins which are still present today. Gone were the days of easy coin shaving.

Example of shaved coins

Even with these methods of coin debasement kept in check, coins still suffer from other issues. They are bulky and not very convenient to transport, especially when large transfers of value need to happen. Showing up with a huge bag of silver dollars every time you want to buy a Mercedes isn't very practical.

Speaking of German things: How the United States *dollar_got its name is another interesting story. The word "dollar" is derived from the German word _Thaler_, short for a _Joachimsthaler.* A Joachimsthaler was a coin minted in the town of *Sankt Joachimsthal*. Thaler is simply a shorthand for someone (or something) coming from the valley, and because Joachimsthal was *the* valley for silver coin production, people simply referred to these silver coins as *Thaler*. Thaler (German) morphed into daalders (Dutch), and finally dollars (English).

The original "dollar". Saint Joachim is pictured with his robe and wizard hat. Picture cc-by-sa Berlin-George

The introduction of representative money heralded the downfall of hard money. Gold certificates were introduced in 1863, and about fifteen years later, the silver dollar was also slowly but surely being replaced by a paper proxy: the silver certificate.

It took about 50 years from the introduction of the first silver certificates until these pieces of paper morphed into something that we would today recognize as one U.S. dollar.

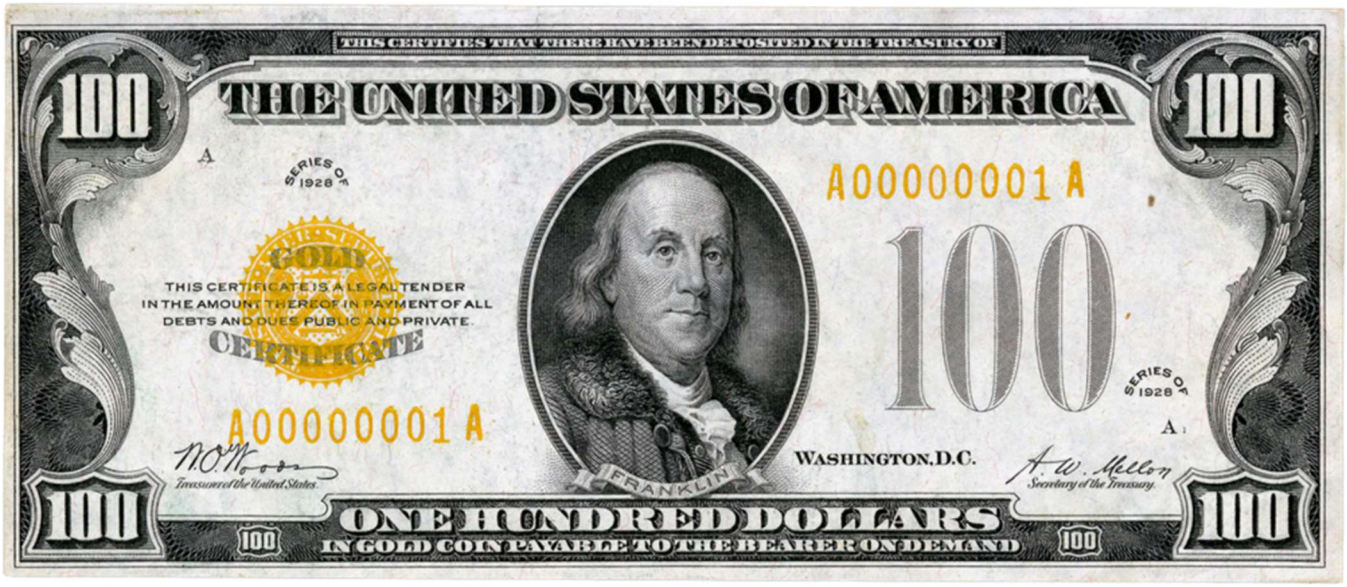
A 1928 U.S. silver dollar. "Payable to the bearer on demand." Picture credit to the National Numismatic Collection at the Smithsonian Institution

Note that the 1928 U.S. silver dollar above still goes by the name of *silver certificate*, indicating that this is indeed simply a document stating that the bearer of this piece of paper is owed a piece of silver. It is interesting to see that the text which indicates this got smaller over time. The trace of "certificate" vanished completely after a while, being replaced by the reassuring statement that these are federal reserve notes.

As mentioned above, the same thing happened to gold. Most of the world was on a bimetallic standard, meaning coins were made primarily of gold and silver. Having certificates for gold, redeemable in gold coins, was arguably a technological improvement. Paper is more convenient, lighter, and since it can be divided arbitrarily by simply printing a smaller number on it, it is easier to break into smaller units.

To remind the bearers (users) that these certificates were representative for actual gold and silver, they were colored accordingly and stated this clearly on the certificate itself. You can fluently read the writing from top to bottom:

"This certifies that there have been deposited in the treasury of the United States of America one hundred dollars in gold coin payable to the bearer on demand."



Picture credit to National Numismatic Collection, National Museum of American History.

In 1963, the words “PAYABLE TO THE BEARER ON DEMAND” were removed from all newly issued notes. Five years later, the redemption of paper notes for gold and silver ended.

The words hinting on the origins and the idea behind paper money were removed. The golden color disappeared. All that was left was the paper and with it the ability of the government to print as much of it as it wishes.

With the abolishment of the gold standard in 1971, this century-long sleight-of-hand was complete. Money became the illusion we all share to this day: fiat money. It is worth something because someone commanding an army and operating jails says it is worth something. As can be clearly read on every dollar note in circulation today, “THIS NOTE IS LEGAL TENDER”. In other words: It is valuable because the note says so.

A 2004 series U.S. twenty dollar note used today. "THIS NOTE IS LEGAL TENDER"

By the way, there is another interesting lesson on today's bank notes, hidden in plain sight. The second line reads that this is legal tender "FOR ALL DEBTS, PUBLIC AND PRIVATE". What might be obvious to economists was surprising to me: All money is debt. My head is still hurting because of it, and I will leave the exploration of the relation of money and debt as an exercise to the reader.

As we have seen, gold and silver were used as money for millennia. Over time, coins made from gold and silver were replaced by paper. Paper slowly became accepted as payment. This acceptance created an illusion—the illusion that the paper itself has value. The final move was to completely sever the link between the representation and the actual: abolishing the gold standard and convincing everyone that the paper in itself is precious.

Bitcoin taught me about the history of money and the greatest sleight of hand in the history of economics: fiat currency.

Lesson 13: Fractional Reserve Insanity

Value and money aren't trivial topics, especially in today's times. The process of money creation in our banking system is equally non-trivial, and I can't shake the feeling that this is deliberately so. What I have previously only encountered in academia and legal texts seems to be common practice in the financial world as well: nothing is explained in simple terms, not because it is truly complex, but because the truth is hidden behind layers and layers of jargon and *apparent* complexity. "Expansionary monetary policy, quantitative easing, fiscal stimulus to the economy." The audience nods along in agreement, hypnotized by the fancy words.

Fractional reserve banking and quantitative easing are two of those fancy words, obfuscating what is really happening by masking it as complex and difficult to understand. If you would explain them to a five-year-old, the insanity of both will become apparent quickly.

Godfrey Bloom, addressing the European Parliament during a joint debate, said it way better than I ever could:

"[...] you do not really understand the concept of banking. All the banks are broke. Bank Santander, Deutsche Bank, Royal Bank of Scotland—they're all broke! And why are they broke? It isn't an act of God. It isn't some sort of tsunami. They're broke because we have a system called 'fractional reserve banking' which means that banks can lend money that they don't actually have! It's a criminal scandal and it's been going on for too long. [...]

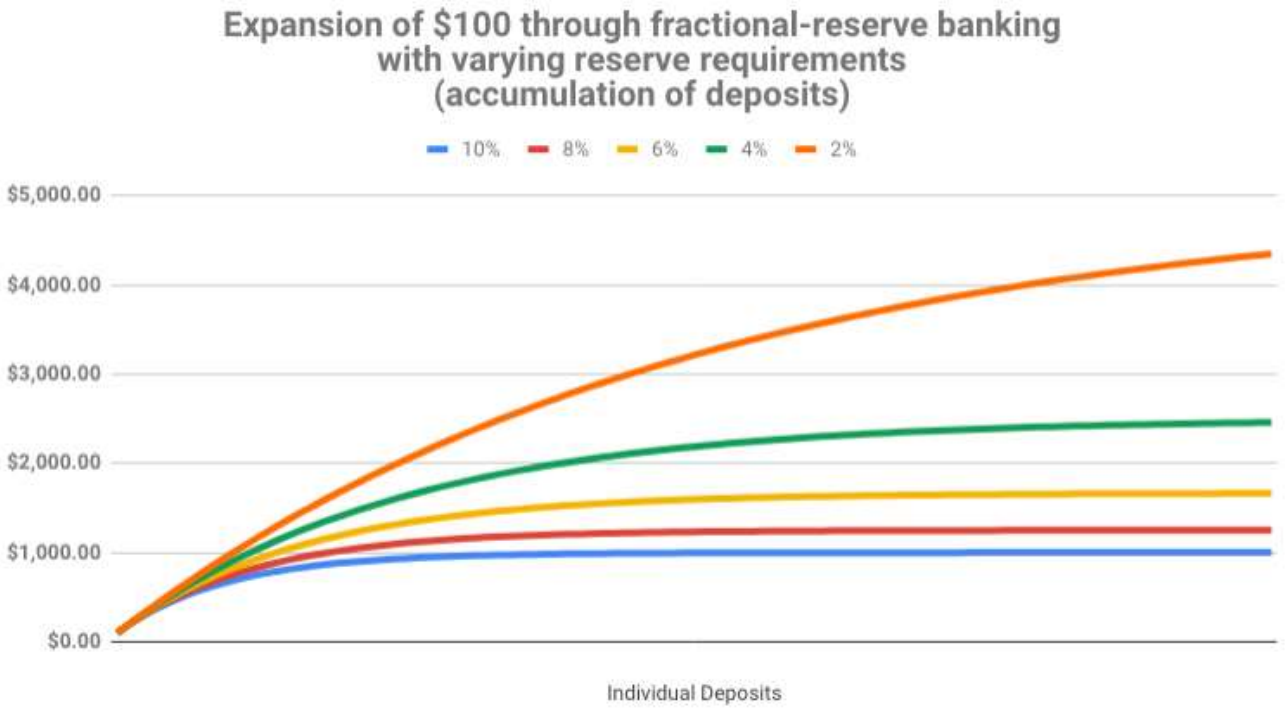
We have counterfeiting—sometimes called quantitative easing—but counterfeiting by any other name. The artificial printing of money which, if any ordinary person did, they'd go to prison for a very long time [...] and until we start sending bankers—and I include central bankers and politicians—to prison for this outrage it will continue."

Let me repeat the most important part: banks can lend money that they don't actually have.

Thanks to fractional reserve banking, a bank only has to keep a small *fraction* of every dollar it gets. It's somewhere between 0 and 10%, usually at the lower end, which makes things even worse.

Let's use a concrete example to better understand this crazy idea: A fraction of 10% will do the trick and we should be able to do all the calculations in our head. Win-win. So, if you take $100 to a bank—because you don't want to store it under your mattress—they only have to keep the agreed upon *fraction* of it. In our example that would be $10, because 10% of $100 is $10. Easy, right?

So what do banks do with the rest of the money? What happens to your $90? They do what banks do, they lend it to other people. The result is a money multiplier effect, which increases the money supply in the economy enormously. Your initial deposit of $100 will soon turn into $190. By lending a 90% fraction of the newly created $90, there will soon be $271 in the economy. And $343.90 after that. The money supply is recursively increasing, since banks are literally lending money they don't have. Without a single Abracadabra, banks magically transform $100 into one thousand dollars or more. Turns out 10x is easy. It only takes a couple of lending rounds.



Don't get me wrong: There is nothing wrong with lending. There is nothing wrong with interest. There isn't even anything wrong with good old regular banks to store your wealth somewhere more secure than in your sock drawer.

Central banks, however, are a different beast. Abominations of financial regulation, half public half private, playing god with something which affects everyone who is part of our global civilization, without a conscience, only interested in the immediate future, and seemingly without any accountability or auditability.

While Bitcoin is still inflationary, it will cease to be so rather soon. The strictly limited supply of 21 million bitcoins will eventually do away with inflation completely. We now have two monetary worlds: an inflationary one where money is printed arbitrarily, and the world of Bitcoin, where final supply is fixed and easily auditable for everyone. One is forced upon us by violence, the other can be joined by anyone who wishes to do so. No barriers to entry, no one to ask for permission. Voluntary participation. That is the beauty of Bitcoin.

I would argue that the argument between Keynesian and Austrian economists is no longer purely academical. Satoshi managed to build a system for value transfer on steroids, creating the soundest money which ever existed in the process. One way or another, more and more people will learn about the scam which is fractional reserve banking. If they come to similar conclusions as most Austrians and Bitcoiners, they

might join the ever-growing internet of money. Nobody can stop them if they choose to do so.

Bitcoin taught me that fractional reserve banking is pure insanity.

Lesson 14: Sound money

The most important lesson I have learned from Bitcoin is that in the long run, hard money is superior to soft money. Hard money, also referred to as *sound money*, is any globally traded currency that serves as a reliable store of value.

Granted, Bitcoin is still young and volatile. Critics will say that it does not store value reliably. The volatility argument is missing the point. Volatility is to be expected. The market will take a while to figure out the just price of this new money. Also, as is often jokingly pointed out, it is grounded in an error of measurement. If you think in dollars you will fail to see that one bitcoin will always be worth one bitcoin.

"A fixed money supply, or a supply altered only in accord with objective and calculable criteria, is a necessary condition to a meaningful just price of money."

—Fr. Bernard W. Dempsey, S.J.

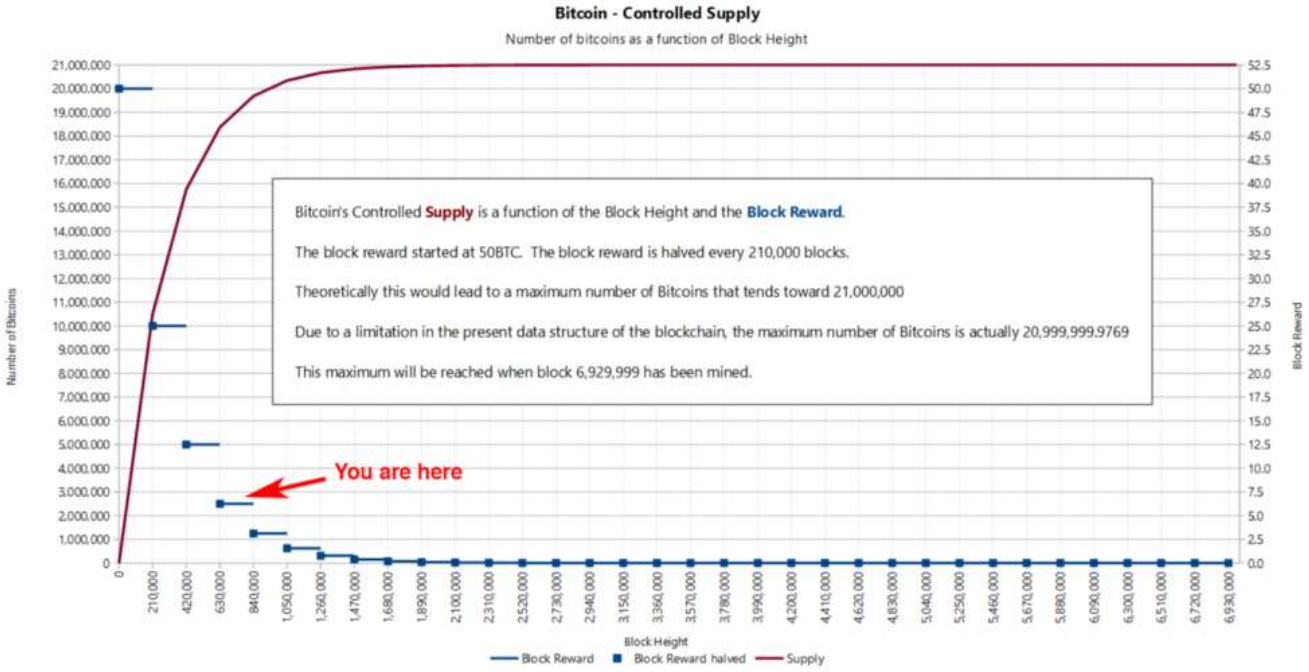
As a quick stroll through the graveyard of forgotten currencies has shown, money which can be printed will be printed. So far, no human in history was able to resist this temptation.

Bitcoin does away with the temptation to print money in an ingenious way. Satoshi was aware of our greed and fallibility—this is why he chose something more reliable than human restraint: mathematics.

$$\frac{\sum_{i=0}^{32} 210000 \left\lfloor \frac{50*10^8}{2^i} \right\rfloor}{10^8}$$

Bitcoin's "supply formula"

While this formula is useful to describe Bitcoin's supply, it is actually nowhere to be found in the code. Issuance of new bitcoin is done in an algorithmically controlled fashion, by reducing the reward which is paid to miners every four years. The formula above is used to quickly sum up what is happening under the hood. What really happens can be best seen by looking at the change in block reward, the reward paid out to whoever finds a valid block, which roughly happens every 10 minutes.



Formulas, logarithmic functions and exponentials are not exactly intuitive to understand. The concept of *soundness* might be easier to understand if looked at in another way. Once we know how much there is of something, and once we know how hard this something is to produce or get our hands on, we immediately understand its value. What is true for Picasso's paintings, Elvis Presley's guitars, and Stradivarius violins is also true for fiat currency, gold, and bitcoins.

The hardness of fiat currency depends on who is in charge of the respective printing presses. Some governments might be more willing to print large amounts of currency than others, resulting in a weaker currency. Other governments might be more restrictive in their money printing, resulting in harder currency.

Before we had fiat currencies, the soundness of money was determined by the natural properties of the stuff which we used as money. The amount of gold on earth is limited by the laws of physics. Gold is rare because supernovae and neutron star collisions are rare. The "flow" of gold is limited because extracting it is quite an effort. Being a heavy element it is mostly buried deep underground.

The abolishment of the gold standard gave way to a new reality: adding new money requires just a drop of ink. In our modern world adding a couple of zeros to the balance of a bank account requires even less effort: flipping a few bits in a bank computer is enough.

"One important aspect of this new reality is that institutions like the Fed cannot go bankrupt. They can print any amount of money that they might need for themselves at virtually zero cost." —Jörg Guido Hülsmann

The principle outlined above can be expressed more generally as the ratio of "stock" to "flow". Simply put, the *stock* is how much of something is currently there. For our purposes, the stock is a measure of the current money supply. The *flow* is how much there is produced over a period of time (e.g. per year). The key to understanding sound money is in understanding this stock-to-flow ratio.

Calculating the stock-to-flow ratio for fiat currency is difficult, because how much money there is depends on how you look at it. You could count only banknotes and coins (M0), add traveler checks and check deposits (M1), add saving accounts and mutual funds and some other things (M2), and even add certificates of deposit to all of that (M3). Further, how all of this is defined and measured varies from country to country and since the US Federal Reserve stopped publishing numbers for M3, we will have to make do with the M2 monetary supply. I would love to verify these numbers, but I guess we have to trust the fed for now.

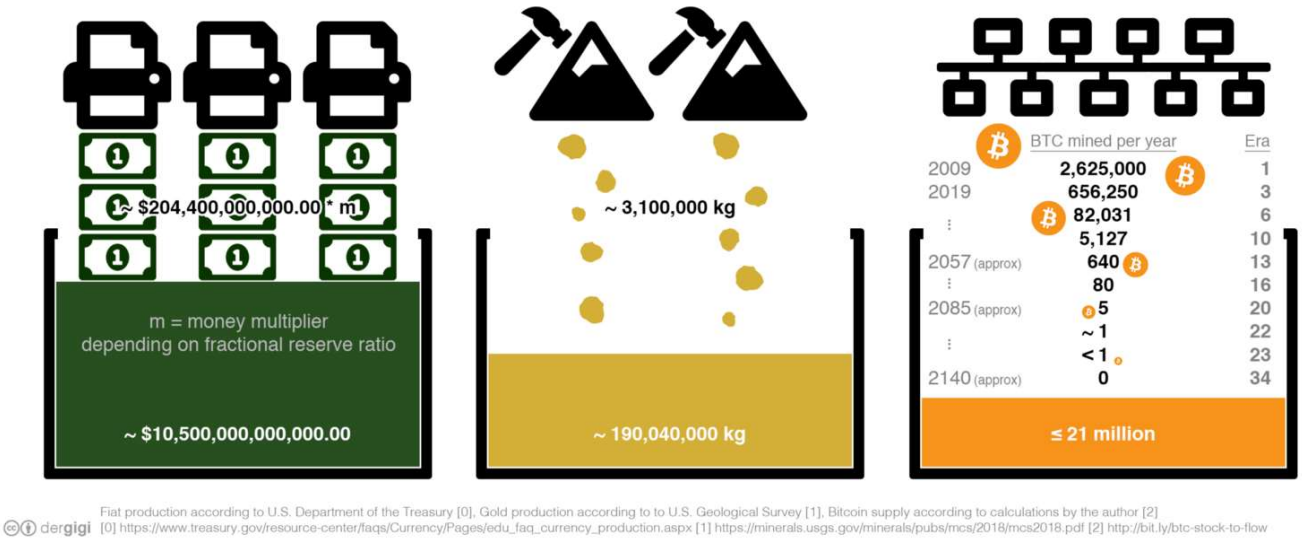
Gold, one of the rarest metals on earth, has the highest stock-to-flow ratio. According to the US Geological Survey, a little more than 190,000 tons have been mined. In the last few years, around 3100 tons of gold have been mined per year.

Using these numbers, we can easily calculate the stock-to-flow ratio for gold: 190,000 tons / 3,100 tons = ~61.

Nothing has a higher stock-to-flow ratio than gold. This is why gold, up to now, was the hardest, soundest money in existence. It is often said that all the gold mined so far would fit in two olympic-sized swimming pools. According to my calculations, we would need four. So maybe this needs updating, or Olympic-sized swimming pools got smaller.

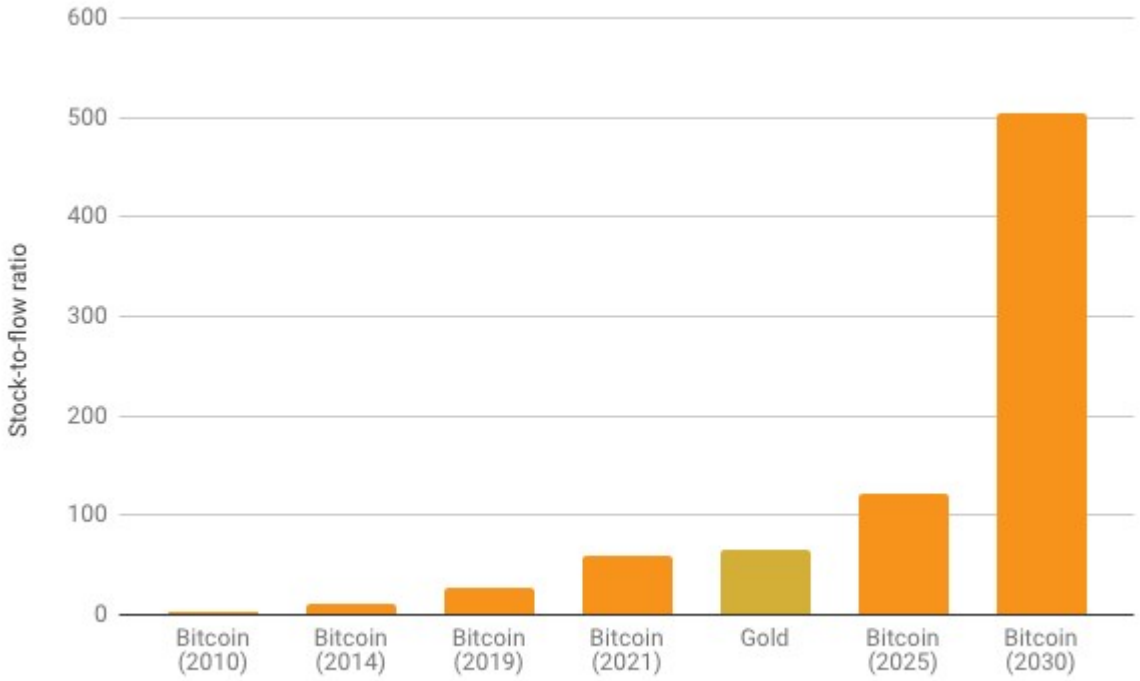
Enter Bitcoin. As you probably know, bitcoin mining was all the rage in the last couple of years. This is because we are still in the early phases of what is called the *reward era*, where mining nodes are rewarded with *a lot* of bitcoin for their computational effort. We are currently in reward era number 3, which began in 2018 and will end in early 2020, probably in May. While the bitcoin supply is predetermined, the inner workings of Bitcoin only allow for approximate dates. Nevertheless, we can predict with certainty how high Bitcoin's stock-to-flow ratio will be. Spoiler alert: it will be high.

How high? Well, it turns out that Bitcoin will get infinitely hard.



Visualization of stock and flow for USD, gold, and Bitcoin

Due to an exponential decrease of the mining reward, the flow of new bitcoin will diminish resulting in a sky-rocketing stock-to-flow ratio. It will catch up to gold in 2020, only to surpass it four years later by doubling its soundness again. Such a doubling will occur 64 times in total. Thanks to the power of exponentials, the number of bitcoin mined per year will drop below 100 bitcoin in 50 years and below 1 bitcoin in 75 years. The global faucet which is the block reward will dry up somewhere around the year 2140, effectively stopping the production of bitcoin. This is a long game. If you are reading this, you are still early.



Rising stock-to-flow ratio of bitcoin as compared to gold

As bitcoin approaches infinite stock to flow ratio it will be the soundest money in existence. Infinite soundness is hard to beat.

Viewed through the lens of economics, Bitcoin's *difficulty adjustment* is probably its most important component. How hard it is to mine bitcoin depends on how quickly new bitcoins are mined. It is the dynamic adjustment of the network's mining difficulty which enables us to predict its future supply.

(It actually depends on how quickly valid blocks are found, but for our purposes, this is the same thing as "mining bitcoins" and will be so for the next 120 years.)

The simplicity of the difficulty adjustment algorithm might distract from its profundity, but the difficulty adjustment truly is a revolution of Einsteinian proportions. It ensures that, no matter how much or how little effort is spent on mining, Bitcoin's controlled supply won't be disrupted. As opposed to every other resource, no matter how much energy someone will put into mining bitcoin, the total reward will not increase.

Just like $E=mc^2$ dictates the universal speed limit in our universe, Bitcoin's difficulty adjustment dictates the **universal money limit** in Bitcoin.

If it weren't for this difficulty adjustment, all bitcoins would have been mined already. If it weren't for this difficulty adjustment, Bitcoin probably wouldn't have survived in its infancy. It is what secures the network in its reward era. It is what ensures a steady

and fair distribution of new bitcoin. It is the thermostat which regulates Bitcoin's monetary policy.

Einstein showed us something novel: no matter how hard you push an object, at a certain point you won't be able to get more speed out of it. Satoshi also showed us something novel: no matter how hard you dig for this digital gold, at a certain point you won't be able to get more bitcoin out of it. For the first time in human history, we have a monetary good which, no matter how hard you try, you won't be able to produce more of.

Bitcoin taught me that me that sound money is essential.

Conclusion

As we leave the "blockchain not bitcoin" days behind us, most people start to realize that there is not a *single* invention which encapsulates the genius of Bitcoin. It is the combination of multiple, previously unrelated pieces, glued together by game theoretical incentives, which make up the revolution that is Bitcoin.

For me, the economic teachings of Bitcoin are as fascinating as the philosophical ones examined in part one. Being a technophile, I can't wait to tell you what Bitcoin taught me about technology in the third and final part of this series.

As mentioned before, I think that any answer to the question *"What have you learned from Bitcoin?"* will always be incomplete. The symbiosis of the two living systems examined here—Bitcoin and economics—is too intertwined and evolving too fast to ever be fully understood by a single person.

"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." —Friedrich Hayek

Learning these lessons enabled me to finally understand what Hayek meant by the above. I believe that Bitcoin is the sly, roundabout way to re-introduce sound money to the world. Thanks to the economic teachings of Bitcoin I learned what good money is and that having it is possible.

What have you learned from Bitcoin?

Acknowledgments

- Again, thanks to Arjun Balaji for the tweet which gave birth to this series.
- Thanks to Saifedean Ammous for his convictions, savage tweets, and writing *The Bitcoin Standard*

- Thanks to Dhruv Bansal for taking the time to discuss some of these ideas with me.
- Thanks to Matt Odell for his candor and also for taking the time to discuss some of these ideas with me, even if he doesn't remember all of it.
- Thanks to Michael Goldstein and Pierre Rochard for curating and providing relevant literature via the Nakamoto Institute
- Thanks to Jannik,Camilo, and Matt for providing feedback to early drafts of this article

Further Reading

There exists an almost endless list of books and essays on the topics discussed above and economic thought in general. The books and articles listed below are but a small selection which were particularly influential in my thinking. I am grateful for all the people who shared their insights, past and present.

- *The Bitcoin Standard: The Decentralized Alternative to Central Banking* by Saifedean Ammous
- *Economics in One Lesson* by Henry Hazlitt
- *Human Action* by Ludwig von Mises
- *The Ethics of Money Production* by Jörg Guido Hülsmann
- *The Denationalization of Money* by Friedrich Hayek
- *The Machinery of Freedom* by David D. Friedman
- *The Case Against The Fed* by Murray N. Rothbard
- *End the Fed* by Ron Paul
- *Shelling Out: The Origins of Money* by Nick Szabo
- *The Bitcoin Halving and Monetary Competition* by Saifedean Ammous
- *The Bullish Case For Bitcoin* by Vijay Boyapati
- *Bitcoin's distribution was fair* by Dan Held

Unpacking Bitcoin's Assurances

Dis-aggregating the system's guarantees

By Nic Carter

Posted Jan 13, 2019

It has rightfully been pointed out that Bitcoin's decentralization is but a means to an end—censorship resistance. This is in response to the decentralization fetishism that

has characterized Bitcoin competitors and the blockchain industry in general. This is an appropriate response: cosmetic network decentralization is probably not sufficient if you plan on breaking any serious rules, and irrelevant if the industry you are seeking to disrupt is dentistry.

Bitcoin's fault-tolerant architecture was designed to survive extreme duress, and its multi-variate decentralization was created (or more accurately: emerged) to promote this. However, censorship resistance—the ability to broadcast information without restriction—does not fully cover the guarantees that Bitcoin provides to users, although it is perhaps the most significant.

In this post I will try and define the various guarantees that Bitcoin users can expect by taking advantage of the system's features over the entire usage lifecycle—from acquisition to exit. Censorship resistance is central to these but not sufficiently comprehensive. I call these 'assurances,' although they aren't perfectly assured, since things go wrong in the real world. (I've been a fan of 'assurances' in this context since reading this post.) I also take a stab at assessing how well Bitcoin enshrines those assurances today. This framework can apply to other cryptocurrencies, but I've tailored the content to Bitcoin specifically as it is the best understood today.

Touted assurance	*Open access**	*Seizure resistance*	*Censorship resistance*	*Counterfeit resistance*	*Free exit**
Bitcoin user phase	**Acquisition**	**Static state**	**Broadcast**	**Receipt**	**Divestment**
Enabling technologies	p2p exchanges, voucher systems, Bitcoin ATMs conventional exchanges, mobile wallets, bearer wallets, multisig	Elliptic curve cryptography, hardware wallets, multisig, paper wallets, brainwallets	P2p gossip broadcast protocol, Sybil-resistant networking, cheap verification and full node proliferation, redundant broadcast (satellite, SMS, radio, mesh)	Cryptographic auditability guarantees, Proof of Work minting, low bandwidth & storage fully validating nodes, hardware full nodes, node service providers, bandwidth reduction techniques	Tumblers, CoinJoin, other privacy enhancements, p2p exchanges, trust-minimized direct sales intermediation
Threats to those assurances	Exchange concentration, capital controls, extension of US banking rules to cryptocurrency exchanges globally	Hardware wallet supply chain attacks, imprisonment / extortion, bank vault raids, quantum computing (long term)	Costly full nodes (leading to a reduction in node count), network DOS attacks, very high fees (for small transactions), loss of internet connectivity	Concentration in node providers, costly full nodes, complexity in validating transactions, deviations from the PoW minting schedule	Taint analysis, shared user blacklists, chain analysis, collusion among exchanges, regulatory action against unregulated exchanges
Strength of assurance	Weak. Exchanges are tightly regulated and fragile to government action. P2p exchanges not yet widespread	Extraordinarily strong. Bitcoin's property rights are some of the strongest ever conceived, and robust to many forms of attack	Currently strong but at risk. Internet closure is a realistic way to prevent broadcast in authoritarian states	Currently strong but at risk. Large/costly full nodes make trust-minimized validation more difficult	Weak. Chain analysis and risk-averse exchanges degrade the saleability of grey or suspected black market coins

* proposed name

Bitcoin's assurances by usage phase

Open access

This is the shorthand for "the right to freely acquire Bitcoin." No amount of decentralization in Bitcoin's architecture itself can guarantee this. As many Bitcoiners

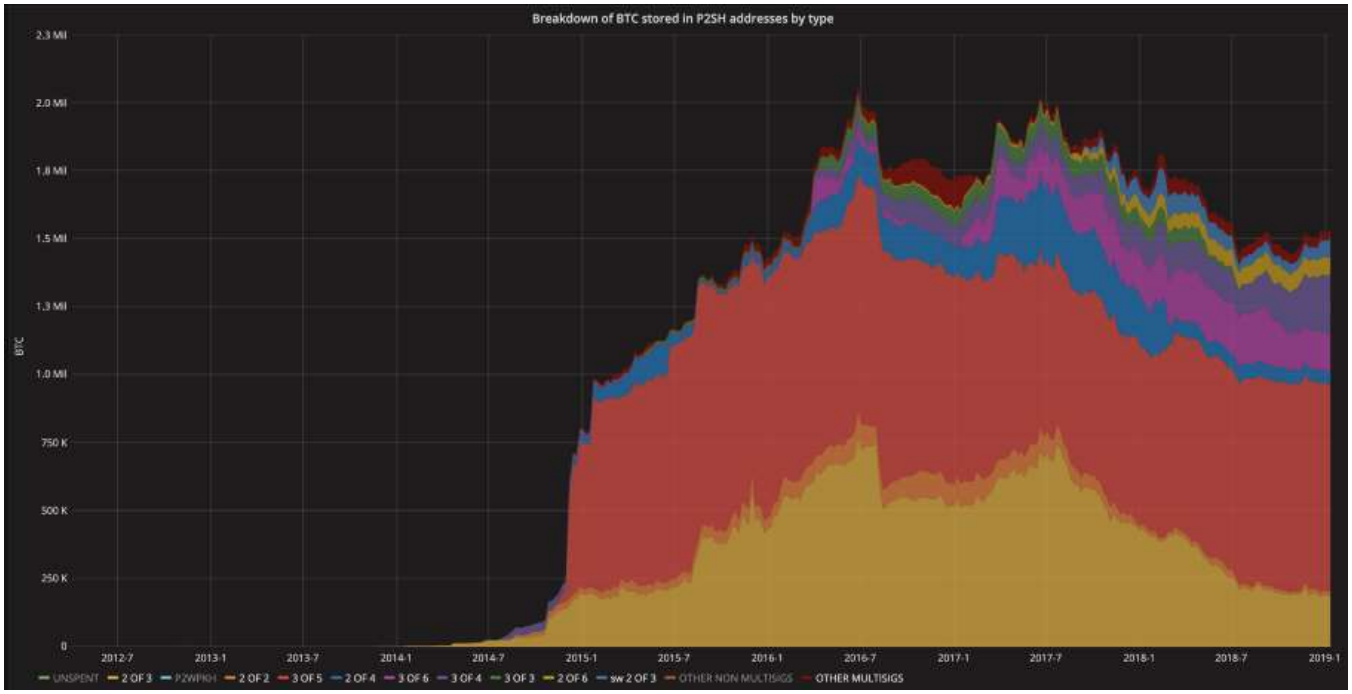
will point out, free access to the asset requires a vibrant and competitive industry of fiat onramps. The existence of quasi monopolists attempting to build regulatory moats in order to raise barriers to entry threatens this. If acquisition of the asset can only occur in a couple large venues, they are not only susceptible to state action, but also liable to collusively deplatform individuals at will. Imagine what happens to the Venezuelan equivalent of Coinbase during a currency crisis: the government trivially shuts it down to preserve its monetary monopoly.

Thus, while large, regulator-friendly, conventional exchanges are good onramps in the developed world, where cryptocurrencies are not (yet) a threat to local sovereign currencies, they aren't a good fit for states experiencing demonetization or high inflation, which is where access is most impactful. Centralized exchanges must be supplemented by peer to peer exchanges like LocalBitcoins, Hodl Hodl, Paxful—and indeed, they are the venues where trading seems to occur (Venezuelan traders are doing $300m annualized on LocalBitcoins, Nigeria ~$170m, Russia close to a billion USD). Wallets which allow for trust-minimized trading like Opendimes are vital here—receiving an Opendime where you can be sure your counterparty doesn't know the private key beats waiting an hour for six confirmations.

Lastly, paper voucher systems enabling users to acquire smaller quantities of Bitcoin at street kiosks or from corner shops are an important piece of the puzzle. Vouchers work by exchanging fiat for a receipt with a code on it; settlement can be done later. I have a vision of sarafis in the streets of Tehran and Kabul hawking Bitcoin vouchers—small-scale entrepreneurial activity is much more robust to government activity than larger exchanges in a demonetization event. Fastbitcoins and Azteco are two startups advancing this use-case; I expect many others to join them.

Peer to peer exchanges like Hodl Hodl rely on a crucial and unheralded technology: Bitcoin's native multi-signature (multisig) capability. A simple, well-understood, trusted, and widely-used multisig implementation enables massive secondary benefits. In the case of Hodl Hodl, it allows buyers and sellers to transact with a high degree of confidence that they will not be cheated. In 2-of-3 multisig contract, the seller and buyer must both sign the release transaction; and if one disagrees, it is referred to the arbitrator for a decision. In practice, the vast majority of transactions settle without arbitration—the threat of mediation itself enforces good behavior.

Multisig is popular in Bitcoin today: about 1.65m BTC (about $6b) are held in known multisig wallets. This figure climbs to 3.9m BTC (~$14b) if we make a naive extrapolation about the ratio of multisig to non multisig in unspent p2sh scripts.



Source: p2sh.info

To sum up, open access to Bitcoin is a core component of the system—what use is the asset if you can't easily obtain it?—yet it is somewhat overlooked. It's important to be realistic about this. Bitcoin suffers from a paradox whereby individuals in countries with relatively less need for Bitcoin have frictionless access to it, while individuals dealing with hyperinflation have to reckon with a less developed onramp infrastructure. There is much work to be done here.

Seizure resistance

One of the chief motivations for this article was to differentiate the unencumbered broadcast rights that Bitcoin grants users from the strong guarantees it grants to users when it is at rest. As mentioned above, censorship occurs at the time of broadcast, so 'censorship resistance' doesn't quite describe Bitcoin's unique properties when idle.

Thus the inclusion of **seizure resistance**(this is also sometimes referred to as 'tamper resistance' or 'judgment resistance'). By this I mean the ability of users to retain access to their Bitcoin under duress, during times of upheaval or displacement, all in a peaceful and covert way.

As Hasu and Su Zhu have eloquently written, Bitcoin can be understood as an independent institution which provides users property rights which are untethered from the state or the legal system. As virtually all property rights trace back to the state, the legal system, or some local monopoly on violence, Bitcoin's cryptography-based property rights are a genuinely new paradigm.

This has been covered at length, but the fact that individuals can store their wealth in a 12 or 16-word passphrase held in their memory is quite astounding. While that's not the most failure-resistant way to operate, it makes one's wealth extremely portable and concealable.

Multisig also comes into play here. Innovative custody companies like Casa (disclaimer: Castle Island is an investor) rely on a 3-of-5 multisignature setup whereby the user controls four keys physically dispersed, and Casa holds one for disaster recovery. This makes physical attacks on Bitcoin holders much more difficult and expensive, while preserving convenience and resilience to faults (seedless recovery is possible if a hardware wallet is lost). The secure key sharding that Bitcoin offers fundamentally reinvents what it means to be a custodian, and opens the door for all kinds of innovative hybrid models which offer various resilience/autonomy tradeoffs.

Censorship resistance

This is the most celebrated assurance attributed to Bitcoin, so I'll be brief. At its core, Bitcoin allows permissionless broadcast through the p2p gossip protocol and the miner fee incentive. Anyone can make a transaction, although they have to sufficiently compensate a miner to include it in a block. If there is a lot of traffic, this could entail a delay or a higher fee. The other required component here is a well-connected network of nodes available to route transactions. If full nodes were to become very expensive and difficult to run, full node counts might decline, making broadcast more difficult. That said, node counts would have to drop precipitously to impair network performance, so this isn't an immediate concern.

One realistic impairment to censorship resistance is the simple approach of simply shutting off local access to the internet. While Bitcoin's global infrastructure cannot be realistically held back by even by the most motivated state actor, a state under severe monetary duress—experiencing a demonetization event, for instance—might take the extreme step of temporarily restricting access to Bitcoin by shutting off the internet. In recent memory, governments in Iran, Turkey, and Russia have shown themselves willing to exert massive collateral damage on local internet access to target services like Telegram and Wikipedia. Places like China where the internet and Bitcoin usage are already tightly regulated would be well-positioned to impose such restrictions. It's not inconceivable that a state could attempt to target Bitcoin in such a manner.

Touted mitigations to state censorship of Bitcoin's broadcast layer include Nick Szabo's long-range radio proposal as well as Samourai/Gotenna's SMS and short-range radio mesh proofs of concept. These initiatives, however, are still either in the R&D phase or the very earliest phases of deployment. At present, individuals in internet-restricted locations have little recourse when faced with such an attack,

aside from physically getting their funds out of the country in a hardware or paper wallet. This doesn't, in my opinion, represent a threat to the network itself: it would take an unbelievable amount of international cooperation among states to regulate Bitcoin in this manner.

Network DOS attacks through fee spam are also an effective if costly way to make it more difficult for everyday users to broadcast transactions. There are few mitigations for this aside from waiting out the attacker or outbidding them.

Counterfeit resistance

This is a crucial quality of the system, and yet it doesn't get quite the rhetorical exposure that censorship resistance does. **Counterfeit resistance** is simply the idea that individuals who use Bitcoin have very cheap access to the tools required to verify that payments they are receiving are legitimate, that their savings have not been debased through inflation, and that their counterparties aren't cheating them in some way.

Comparing Bitcoin to gold, the ability to run a full node is akin to owning a professional-grade XRF spectrometer to check the integrity of your bullion. Compared to the expensive and tricky tests to verify gold's authenticity, verifying the integrity of one's Bitcoin is a breeze. Running a node costs a few dollars a year and can be done on consumer hardware and bandwidth with little difficulty. This very accessible counterfeit resistance only persists as long as running a node is relatively cheap—a significant increase in the bandwidth, computation, or memory required to run a fully validating node would hinder it significantly. Right now, Bitcoin is growing at a stable rate, and physical plug-n-play node hardware has made full nodes more accessible than ever, so this assurance seems safe for now. For individuals and enterprises that don't want to run nodes directly, a good diversity of managed node software exists.

The other side of counterfeit resistance is the ability to determine that all units that exist were created according to a predefined, predictable schedule. The proof of work minting function, plus the difficulty adjustment, takes care of this. Well—close enough. Naively assuming that blocks were meant to arrive every 10 minutes on average, Bitcoin is actually slightly ahead of schedule by 30,000 blocks or so. This is because hash power has generally increased over time, and this caused block arrival to outpace the defined schedule due the coarse granularity in the difficulty adjustment. Aside from this interesting emergent property, Bitcoin's PoW has never been compromised, nor has the hash function been broken (and this doesn't seem eminently likely in the foreseeable future). Verifying that the correct number of units exist is as simple as running the *gettxoutsetinfo* command in your Bitcoin Core node.

The inherent auditability of Bitcoin and all of its derivatives is what makes deceptions like the Bitcoin Private covert inflation scandal easy to spot.

At present, Bitcoin's counterfeit resistance is made possible by a deliberate design philosophy from the core developers that prides accessibility and user self-sovereignty at all costs. It is augmented by a network of Bitcoin businesses that provide hardware nodes or managed access to node software. However, if the chain's growth were to radically accelerate, consumer-grade counterfeit resistance would be significantly impaired.

Free exit

Free exit—the ability to sell Bitcoin unencumbered—is another aspect of the system that is sometimes overlooked. It's not strictly a Bitcoin guarantee, but Bitcoin's usefulness is significantly downgraded in its absence. The real world consequences of overzealous chain analysis companies (whose heuristics implicate innocent users through false positives) make themselves felt when those users attempt to sell their Bitcoin for fiat. Since fiat offramps are the most easily regulated and are run by risk-averse institutions, they are a natural target for entities that create blacklists and ascribe taint to individual UTXOs.

There are a few strategies to reckon with this. One is to obfuscate the origin of funds through collaborative tumblers like the Wasabi wallet . Another approach is to reverse-engineer the heuristics that chain analysis firms use and develop mixing strategies that implicate everyone in taint (thus rendering those heuristics incoherent) or that avoid detection altogether through specialized transaction types. This is the general approach of the folks behind the Samourai wallet. Routing around the centralized, highly-regulated exchanges is another option, either on the p2p marketplaces or by exchanging BTC for goods and services, rather than fiat.

Ultimately, I expect that a tranche of grey or black-market Bitcoins will emerge, with coins available at a discount in exchange for their reduced access to capital markets. This will not be a death knell—there will likely be more than enough demand globally for slightly cheaper Bitcoins, even if they cannot be traded on Coinbase. The world is a big place, with a variety of regulatory regimes, and individuals fleeing hyperinflation may not be too bothered by the fact that the Bitcoins they acquired cannot be deposited on US-regulated exchanges.

The objective for this piece was to present a framework of the major assurances that Bitcoin provides to users, and make it clear that censorship resistance is only one of them. Additionally, I wanted to make the point that Bitcoin the software is only one part of a much vaster system—a collaborative social and industrial project aiming to provide unencumbered financial tools to individuals the world over. Entrepreneurs that have created hardware wallets, merchant services, novel exchanges, voucher

systems, Bitcoin contract structuring, and hybrid custody models have all done their bit to advance user sovereignty and discretion when it comes to their personal wealth. They deserve to be recognized, as does the broader struggle to make these touted assurances a reality.

Tweetstorm: Bitcoin as SoV

By Dan Held

Posted January 14, 2019

1) Satoshi's Vision™ is a silly endeavor, as it doesn't matter what it was, we are where we are now. However, those pushing the "Bitcoin was first made for payments" narrative insist on cherry-picking sentences from the white paper and forum posts to champion their perspective.

2) The following tweetstorm is a categorical repudiation of this tired narrative. Bitcoin was purpose-built to first be a Store of Value (SoV), a thread:

3) How do we determine Satoshi's intention? We need to look at his ideology, description of functionality/architecture, timing, and audience. Let's start with how Satoshi describes the problem Bitcoin solves. In his first public comms after the whitepaper, in the first paragraph:

4) "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

5) He later expands on that Libertarian thought in his other writings: "[with Bitcoin] we can win a major battle in the arms race and gain a new territory of freedom for several years."—Satoshi Nakamoto

6) How does Satoshi describe Bitcoin? His forum posts provide insight through his consistent gold/metal analogy: "Bitcoin [is] more like a collectible or commodity." - Satoshi

7) "In this sense, it's more typical of a precious metal. Instead of the supply changing to keep the value the same, the supply is predetermined and the value changes. As the number of users grows, the value per coin increases" - Satoshi

8) “As a thought experiment, imagine there was a base metal as scarce as gold but with the following properties: [not useful/no utility]. And one special, magical property: can be transported over a communications channel” - Satoshi

9) “If there were nothing in the world with intrinsic value that could be used as money, only scarce but no intrinsic value, I think people would still take up something. (I’m using the word scarce here to only mean limited potential supply)” - Satoshi

10) “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 Satoshi here clearly highlights that Bitcoin’s scarcity gives it value… as a SoV. Limited supply is meaningless for VISA

11) So we now have an idea of Satoshi’s motivations, and how he describes Bitcoin, but what does his timing tell us? Bitcoin’s launch during the 08’ financial crisis was not coincidental. Satoshi had been coding Bitcoin for the last 2 years. Let’s look at the sequence of events

12) Jan - July: Fed tries to stop the housing bust: Fed bails out Bear Sterns. Paulson explains the need to bail out Fannie Mae, Freddie Mac the two agencies that held or guarantee 50% of the $12T in US mortgages.

13) Aug 18: Satoshi registers org Sept 15: Lehman Brothers files for bankruptcy, the largest in U.S. history ($600B) Sept 17: Investors withdrew a record $144B from their money market accounts. During a typical week, only about $7B is withdrawn

14) Oct 3: Bitcoin whitepaper PDF likely created Oct 13: Treasury Secretary Paulson talks with 9 major bank CEOs. The total bailout package ~$2.25T Oct 21: Fed lends $540B to bail out money market funds Oct 31: Satoshi publishes the Bitcoin whitepaper

15) With the 2008 financial crisis, trust had been lost in a world that ran on trust. Bitcoin was launched in a time of absolute necessity, Satoshi planted the seed at precisely the right moment. The world didn’t need a new VISA, they needed an alternative to banks.

16) So we now have an idea of Satoshi’s motivations, how he describes Bitcoin, and his timing, what about this initial audience for the whitepaper? How did he market his message?

17) Satoshi crafted the whitepaper as a call to arms for his target audience: the Cypherpunks on the cryptography mailing list. Key components of their ideology are privacy and finality. His message needed to resonate with them as they would have to help him build it.

18) "Therefore, privacy in an open society requires anonymous transaction systems. An anonymous system empowers individuals to reveal their identity when desired and only when desired; this is the essence of privacy." - A Cypherpunk's Manifesto

19) Many point to this in the whitepaper "peer-to-peer version of electronic cash would allow online payments" as proof that Satoshi meant for Bitcoin's main purpose is to disrupt VISA. However, "cash" represents a pseudonymous push payment in contrast to a credit-based system

20) Cash is a bearer asset. Let's look at the whitepaper with that in mind: *"A purely peer-to-peer version of electronic [bearer assets] that would allow online payments to be sent directly from one party to another without going through a financial institution."*

21) Note that the origin of the word "cash" is "caisse" (French) meaning money-box. So cash is by definition store-of-value. Other Cypherpunks had used the word cash in their whitepapers to reflect that functionality, like "HashCASH", "eCASH", etc"

22) In the other part of the whitepaper sentence the phrase "peer-to-peer" has been used as well against the SoV narrative. Charlie Lee has a great tweet storm that addresses this point of contention:

23) "Bitcoin isn't "peer-to-peer." Payments are sent from sender to miners, who record it on a distributed ledger. The recipient receives the payment when it's recorded. BUT, this is facilitated by a p2p network where transactions are broadcasted."@SatoshiLite

24) "Lightning network payments, on the other hand, are p2p payments. They are sometimes direct p2p, sometimes indirect p2p. LN payments have to be sent from p2p to get from the sender to the recipient. Both have to be online, just like other p2p networks like BitTorrent"

25) "Bitcoin with Lightning Network more closely fits the Bitcoin whitepaper's title: "A Peer-to-Peer Electronic Cash System." This is Satoshi's Vision." -@SatoshiLite

26) He wrote the paper to fit his target audience, but the source code implementation were his product specs. "If the Bitcoin Whitepaper is the Declaration of Independence, the Source Code is the Constitution" -@pierre_rochard

27) "The functional details are not covered in the paper, but the sourcecode is coming soon."—Satoshi Nakamoto

Aka the whitepaper was marketing, the important details are coming. **28)** In true Cypherpunk fashion, Satoshi's whitepaper was quickly followed by code release in January 2009. The notion that good ideas need to be implemented, not just discussed, is very much part of the culture of the mailing list.

29) Just focusing on the whitepaper is a gross misinterpretation, here are the things not described in the whitepaper, but included in the source code or later defined by Satoshi: 21M hard cap, 10 minute blocks, 1 mb block caps.

30) If Satoshi wanted Bitcoin to first be used as a medium of exchange to purchase goods and services, he would have made it inflationary. People don't spend deflationary currencies when they can make the same purchase in infl. curr. There's even a name for It, Gresham's Law

31) Which is entirely intuitive. Why would any average consumer spend their Bitcoin with the perception that it will be worth more in the future when they can spend their fiat that they KNOW will be worth less?

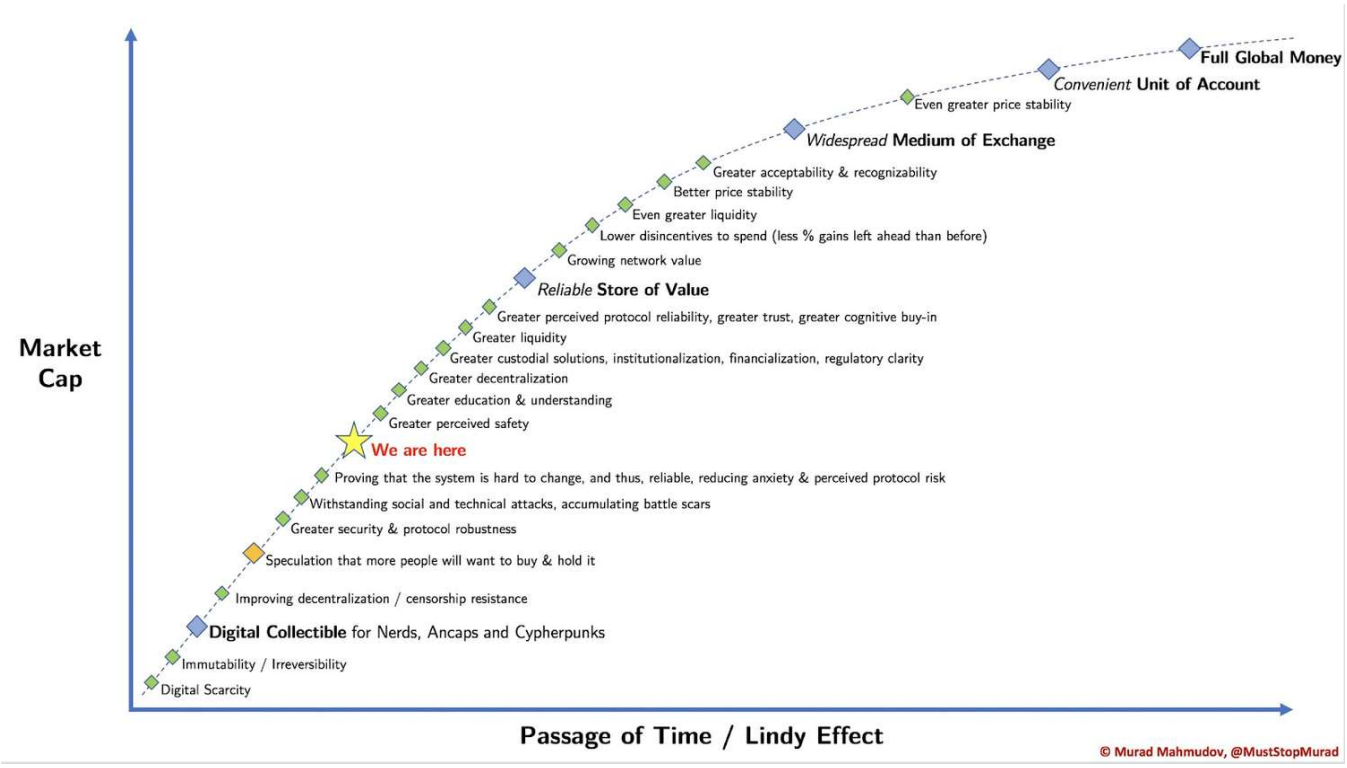
32) So far that doesn't sound like he's trying to disrupt VISA now does it? And if that wasn't made perfectly clear, he permanently etched this message into the Genesis Block: *"The Times 03/Jan/2009 Chancellor on brink of second bailout for banks"*

33) To take it a step further, as a subtle jab to central banks, he chose his birthday as the date the US made gold ownership illegal through EO 6102 April 5th. He chose 1975 as his year of birth which is the year when the US citizens were allowed to own gold again

34) And finally, why did Satoshi choose to be anonymous if he were just disrupting payments?

What he was trying to accomplish was clear, he wanted to build a new backbone for the financial system. Bitcoin isn't merely digital cash, but an alternative to banks.

35) And how does a new money get created? A new money comes into existence through stages: Collectible, SoV, MoE, and UoA. SoV and MoE aren't mutually exclusive. It's about where in the cycle of appreciation we're in. At maturity, the payment use case finally makes sense.



Bitcoin evolution over time

36) Some may balk at the SoV terminology for Bitcoin since the price fluctuates. However, nothing in this life has a "stable" value, the longest running fiat currency, GBP, has lost 99% of its value since inception. Bitcoin has all the traits of a good SoV

37) Bitcoin is stable. The protocol has a 99.99989% uptime which is higher than USD. The "fluctuation" you see is the volatility of the world flowing into the stability of Bitcoin in ebbs and flows.

38) When applying "The Szaboian Theory of Money Origins" to Bitcoin, it is reasonable to conclude we just barely left the "collectible phase" and are now witnessing it's first steps into "Proto-money"@Willem_VdBergh @NickSzabo4

39) This phase, which is characterized by its primordial exploration of the SoV properties of the commodity, can easily take a decades to properly mature. Volatility is part of this maturing process.

40) People pushing the MoE narrative at this moment in time are counterproductive to adoption. By creating these expectations, which are unattainable at the moment, many people will get burned or disillusioned. This is a big loss for adoption and for

the affected individuals

41) "Only by informing people correctly about the use case Bitcoin has *at this moment* can we maximize it's adoption and prevent a lot of people from making the biggest financial mistake of their life."@Willem_VdBergh

42) So how did the payments narrative become a thing? A/ Satoshi used it to attract the cypherpunks B/ HODLing isn't good for business. In order to command higher valuations, startups latched onto narratives that VCs would fund. And in 2013-2016 that was "merchant processing."

43) Background on me: I was the first PM @Blockchain and @ChangeTip, both attempted to get people to use Bitcoin for payments. Consumers couldn't care less, which is entirely intuitive: right now it's not faster, cheaper, or easier to use for 99.99% of use cases.

44) After all of this do you really think Bitcoin was primarily built for payments at this stage in its lifecycle?

45) If you enjoyed this tweet storm, please sign up for an e-mail newsletter which will include more of my thoughts like these. (at a date far in the future when I have time)

46) Special thanks for the insight and inspiration:

@real_vijay, @nwoodfine, @saifedean, @NickSzabo4, @MustStopMurad, @pierre_rochard, @nic__carter, @hugohanoi, @MartyBent, @francispouliot_, @TuurDemeester, @arjunblj, @jimmysong, @hasufl, @prestwich, @CremeDeLaCrypto, @SatoshiLite, @MrHodl

---

Money, Bitcoin and Time: 1 of 3

By Robert Breedlove

Posted January 20, 2019

This is part 1 of a 3 part series

- Money, Bitcoin and Time: 1 of 3
- Money, Bitcoin and Time: 2 of 3
- Money, Bitcoin and Time: 3 of 3

A synthesis of perspectives from many prolific thinkers, this 3-part essay will cover the following topics in sequence:

- Money—its properties, story and evolutionary history
- Bitcoin—its nature and significance in the story of money (see PART 2)
- Time—perspectives on its value and how the story of money might play out (see PART 3)

This essay is guided, inspired and adapted from the literary works of many. Each section header will include a number [n] referencing relevant synthesized works at the end of each part. For those seeking further elucidation on any of the topics discussed herein, I highly encourage you to read these original works.

This essay is also available in .pdf form at: https://www.parallaxdigital.io/blog

Please feel free to send any questions or feedback to info@parallaxdigital.io

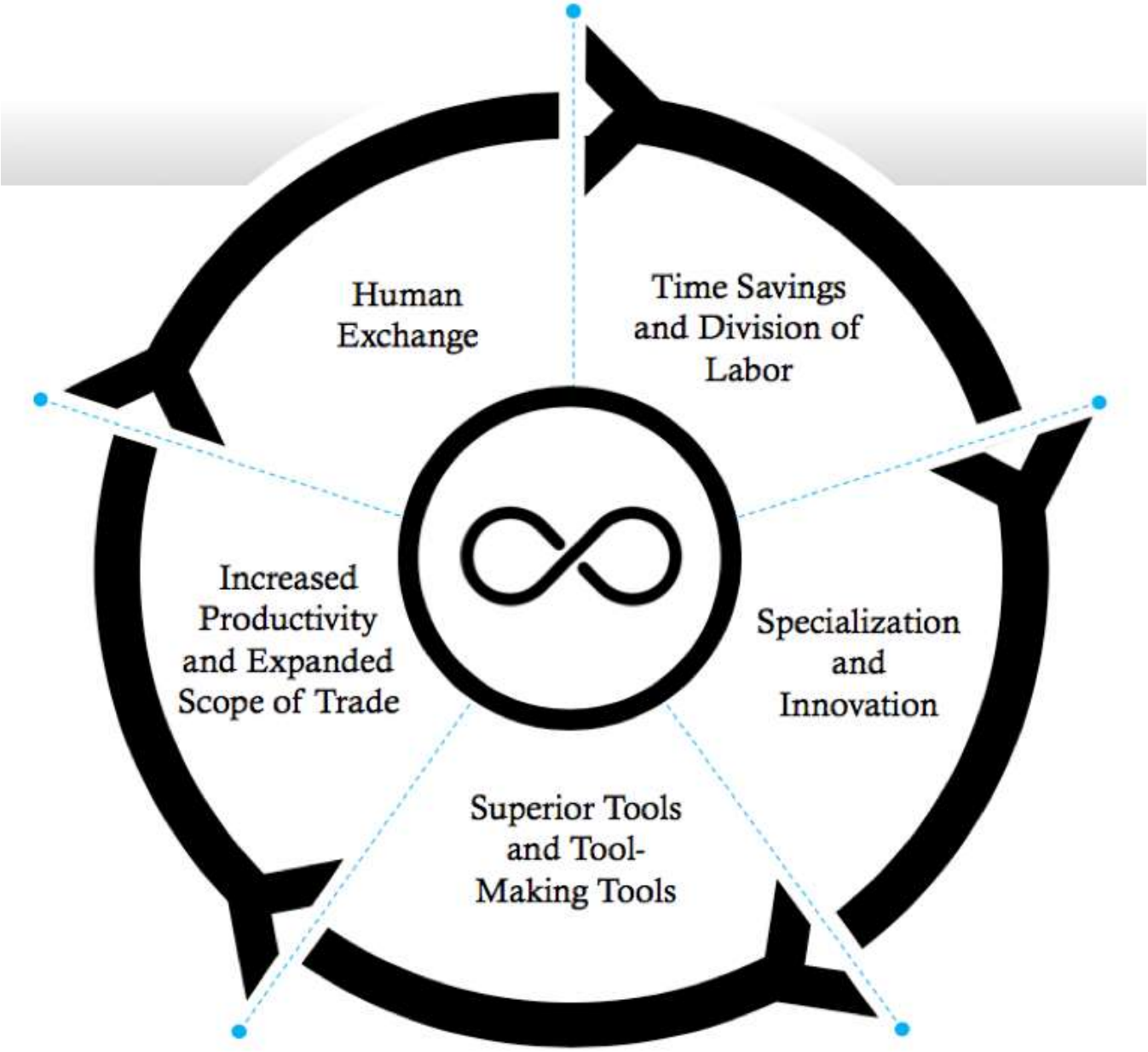
The Simple Truth about Money: Money is the most successful story ever told by humans. It is a reflexive narrative: meaning it has value only because everyone believes it, and everyone believes it because it has value. Money is a story that continues to be written...

Human Exchange [2,6]

Human beings are the networked species. Initially, these were small bands of hunters and gatherers numbering no more than 150 persons strong (Dunbar's number). When humans began to exchange with one another, they intuitively discovered the *division of labor* which allows people to focus on their relative advantages and concentrate on their chosen craft. The division of labor enables the *specialization* of productive efforts for mutual gain. If John makes axes faster than Steve, and Steve makes bows faster than John, then they both are better off by specializing and trading. Interestingly, this holds true even if John is faster than Steve at making axes and bows (up to a point) and, amazingly, this effect compounds.

Tools, or technologies, are mechanisms that increase *productivity* by amplifying the returns on human time directed at production. You can chop more wood per man hour using an axe than you can with your bare hands. As people made and exchanged more tools, time savings increased and specialization deepened. Specialization sparked innovation, because it encouraged the investment of time in tool-making tools, such as whetstones used for making sharper axes. This enabled people to create superior tools, which increased productivity even further. That saved more time, which people used to specialize even further and expand their *scope of trade* by exchanging with an even greater number and variety of people, which

increased the division of labor even further, and so on. This recursive dynamic persists to this day as a virtuous cycle with no known natural limit—modern markets in goods, services and ideas allow human beings to exchange and specialize honestly for the betterment of all. In this way, the act of exchange is the incipient force driving all human progress and *prosperity* . Prosperity is simply time saved, which is proportional to the division of labor:



Human exchange is the incipient force driving all human progress and _prosperity_ . Prosperity is simply time saved, which is proportional to the division of labor. This recursive dynamic persists to this day as a virtuous cycle with no known natural

limit — modern markets in goods, services and ideas allow human beings to exchange and specialize honestly for the betterment of all.

Human exchange is to cultural evolution what sex is to biological evolution. By exchanging and specializing, innovations come into existence and spread. At some point, human intelligence became collective and cumulative in a way that happened to no other animal. Language, and later writing, allowed us to pass our collective learnings to each successive generation. Written language allowed us to manifest and share our belief systems. As the only animal that can tell and believe stories, we learned to organize ourselves using abstractions such as money, mathematics, nations and corporations. Our unique ability to tell and believe stories—as free market capitalists, human rights activists, national citizens or whatever story we accord with—enables us to cooperate flexibly in large numbers and across genetic boundaries. This scale of collaboration, never attained by any other animal before or since, is the reason mankind came to dominate the Earth. We are the networked species, fully interconnected by our acts of exchange. A spontaneous emergent property of these complex human interactions is money, which solved problems inherent to trade and accelerated the rate of human exchange and the division of labor. Money, as the vital lubricant for human exchange, was among the first stories we used to collectively organize ourselves.

Story of Money [1]

Let's begin with first principles and follow logic from there. The simplest form of human exchange is the direct trading of actual goods, say guns for boats, in a process known as *direct exchange* or barter. Direct exchange is only practical when few people are trading few goods. In larger groups of people, there are more opportunities for individuals to specialize in production and trade with more people, which increases the aggregate wealth for everyone. This simple fact, that exchange enables us to produce more goods per hour of human effort is the foundation of economics itself:

Economics is the social science of increasing production per unit of contribution.

Larger groups of people exchanging goods mean larger markets, but also creates a problem of *non-coincidence of wants* — what you are seeking to acquire by trade is produced by someone who doesn't want what you have to offer. This problem has three distinct dimensions:

- Non-coincidence in Scales—imagine trying to trade pencils for a house, you cannot acquire fractions of a house and the owner of the house may not need such a large amount of pencils
- Non-coincidence of Locations—imagine trying to trade a coal mine in one place for a factory in another location, unless by coincidence you are seeking a

factory in that exact location and the counterparty you are dealing with is seeking a coal mine in that precise place, the deal will not be completed since factories and coal mines are not movable
- Non-coincidence in Time Frames—imagine trying to accumulate enough oranges to trade for a truck, since the oranges are perishable they would likely rot before the deal could be completed

The only way to resolve this three-dimensional problem is with *indirect exchange,* where you seek to find another person with a good desired by the counterparty and exchange your good for theirs only to, in turn, exchange it for the counterparty's good to complete the deal. The intermediary good used to complete the deal with the counterparty is called a *medium of exchange* – the first function of money. Over time, people tend to gradually converge on a single medium of exchange (or, at most, a few media of exchange) as it simplifies trade. A good that becomes widely accepted as a medium of exchange is commonly called money.

Money offers its users pure optionality, as it can be readily exchanged for any good available in the marketplace. In other words, money is the most liquid asset within a trade network. In this sense, money is said to have the highest *salability*, meaning the ease with which it can be sold on the market at any time with the least loss in price. Salability of a good is relatively determinable by how well it addresses the three dimensions of the non-coincidence of wants problem:

- Salability across Scales—a good that is easily subdivided into smaller units or grouped together in larger units, which allows the user to trade it in whatever quantity desired
- Salability across Space—a good that is easily transported or transmitted over distances
- Salability across Time—a good that can reliably hold its value into the future by being resistant to rot, corrosion, counterfeit, unpredictable increases in supply and other debasements of value

It is the third element, salability across time, that determines a good's utility as a *store of value*—the second function of money. Since the production of each new unit of a monetary good makes every other unit relatively less scarce, it dilutes the value of the existing units in a process known as *inflation* . Protecting value from confiscation via inflation is a critical feature of money, and money is critical to the existence of flourishing trade networks.

Hard Money [1]

Hard money is more trustworthy as a store of value precisely because it resists intentional debasements of its value by others and therefore maintains salability across time. The hardness of a monetary good, also known as its soundness, is

determined by the stock of its existing supply and the flow of its new supply. The ratio which quantifies the hardness of money is called the *stock-to-flow* ratio:

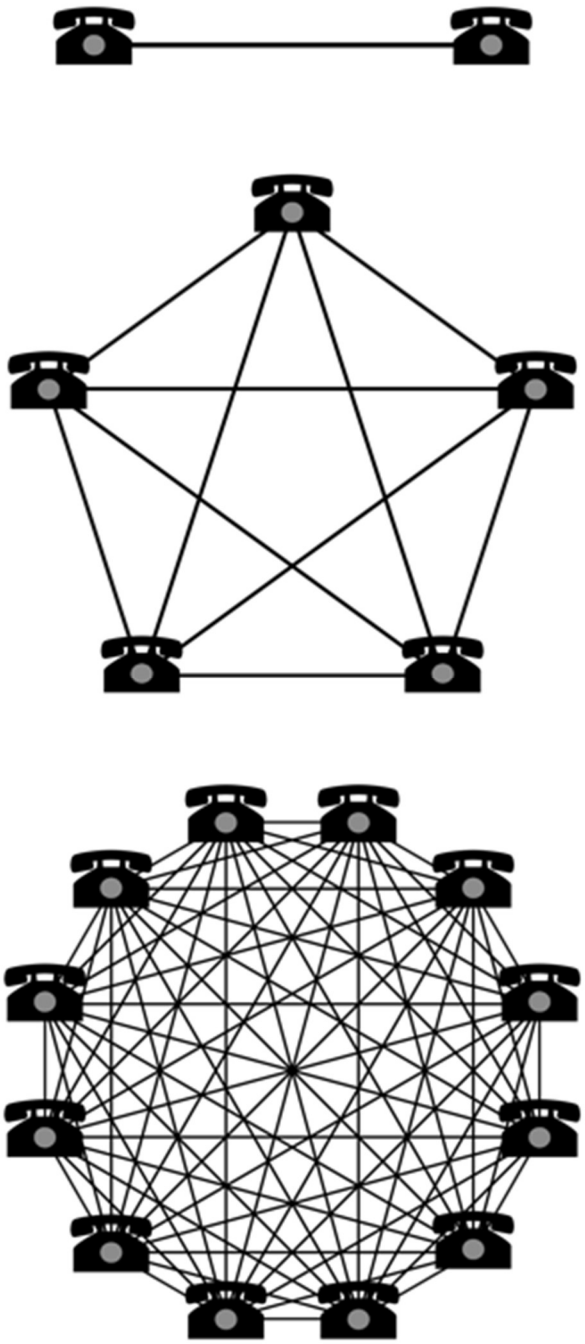
- 'Stock' is the existing supply of monetary units
- 'Flow' is the newly created supply over a specified time period, usually one year
- Dividing the stock of a monetary good by its flow equals its stock-to-flow ratio
- The higher the stock-to-flow ratio, the greater the hardness (or soundness) of money

The higher the stock-to-flow ratio, the more resistant the money is to having its value compromised by inflation. There are no correct choices as to forms of money, however there are consequences to what form a market naturally selects. If people choose to store their wealth in a monetary good which exhibits less hardness, then the producers of this monetary good are incentivized to produce more monetary units, which expropriates the wealth of existing unit holders and destroys the monetary good's salability across time. This is the fatal flaw of *soft money*: anything used as a store of value that can have its supply increased will have its supply increased, as producers seek to steal the value stored within the soft monetary units and store it in a harder form of money. As many historical examples in this essay will demonstrate, any monetary good which can have its supply cheaply and easily increased will rapidly destroy the wealth of those using it as a store of value.

For a good to assume a dominant monetary role within an economy, it must exhibit superior hardness with a higher stock-to-flow ratio than competing monetary goods. Otherwise, excessive unit production will destroy the wealth of savers and the incentives to use it as a store of value. Particular goods achieve monetary roles based on the interplay of people's decisions. It is from the chaos of complex human interactions that monetary orders emerge. Therefore, it is important to consider the social aspects of the spontaneous emergence of monetary orders.

Money is a Social Network [1,4]

Money, as a value system which connects people across space and time, is the original and largest social network. The value of a network is a reflection of the total number of possible connections it allows. Similar to the telephone and modern social media platforms, a monetary network becomes exponentially more valuable as more people join it because the number of possible connections it allows is proportional to the square of the number of its total network participants, a relationship defined by *Metcalfe's Law*:



Network values are based on the number of possible connections they allow. Such values grow exponentially with the addition of each new constituent — a property commonly known as network effects.

In a monetary network, more possible connections mean more salability and a broader scope of trade. Participants in a monetary network are connected by their use of a common form of money to express and store value. *Network effects*, defined as the incremental benefit attained by adding a new member to a network for all existing members in that same network, encourage people to adopt a single form of

money. Intuitively, a monetary good that holds value across time (hard money) is always preferable to one that loses value (soft money). This causes people to naturally gravitate to the hardest form of money available to them. Further, since human exchange is a singular communal phenomenon suffering from a three-dimensional non-coincidence of wants problem, any monetary good that can solve all three dimensions of this problem will win the entire (or vast majority) of the market. For these reasons, a free market for money exhibits a *winner take all* (or, at least, a winner take most) *dynamic* . Network effects accelerate people's natural coalescence around a single monetary technology since larger monetary networks support higher salability of the monetary good involved. However, the selection of a monetary good is limited by the technological realities of the markets selecting. This can impede the winner take all dynamic, since particular monetary goods each satisfy the desirable traits of money to greater or lesser extents.

Monetary Traits [1,4]

As we will see, markets have naturally and spontaneously selected for the monetary good which best satisfies a variety of desirable traits that determine how useful a particular monetary good is as a form of money:

- Hardness—resistance to unpredictable supply increases and debasements of value
- Fungibility—units are interchangeable and indistinguishable from one another
- Portability—ease of transporting or transmitting monetary units across distances
- Durability—resistance of monetary units to rot, corrosion or deterioration of value
- Divisibility—ease of subdividing or grouping monetary units
- Security—resistance to counterfeiting or forgery
- Sovereignty—the source of its value, trust factors and permissions necessary to transact with it (natural social consensus or artificial government decree)
- Government Issued—authorized as legal tender by a government

As discussed, hardness is the singular trait that takes primacy over all others in determining a good's suitability for playing a monetary role. Money, as an expression of value, has remained conceptually constant but has evolved to inhabit many different goods over time. Like language, which was first spoken, then written and now typed, the meaning expressed by money remains the same while its modality continually evolves. As the monetary technologies we use to express value change, so too do our preferences.

Prospects of Prosperity [1]

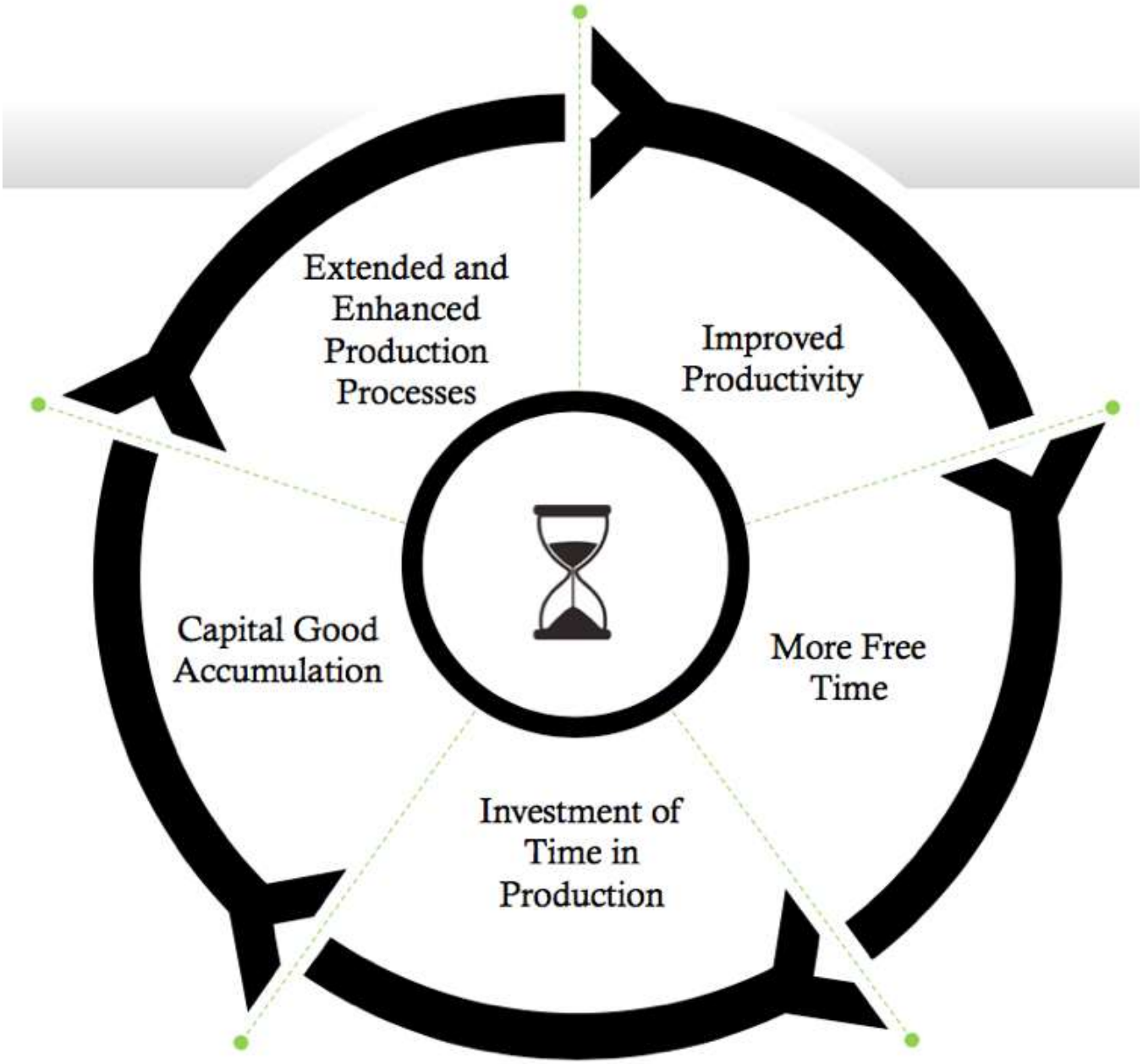
In economics, a critical aspect of human decision making is called *time preference*, which refers to the ratio at which an individual values the present relative to the future. Time preference is positive for all humans, as the future is uncertain, and the end could always be near. Therefore, all else being equal, we naturally prefer to receive value sooner rather than later. People who prefer to defer current consumption and instead invest for the future are said to have a lower time preference. The lowering of time preference is closely related to the hardness of money and is also exactly what enables human civilization to advance and become more prosperous. In regard to time preference, hard money is important in three critical aspects:

- By providing a reliable way to protect value across time, hard money incentivizes people to think longer term and thus lowers their time preferences
- As a stable unit of measurement, hard money enables markets to grow ever-larger by reducing the costs and risks of free trade, which increases the incentives for long-term cooperation and lowers time preferences
- Self-sovereign money (like gold and Bitcoin) that cannot be manipulated by any single party reduces governmental intervention which encourages the growth of free markets, which increases their long-term stability and lowers time preferences

A lower time preference is an important part of what separates humans from other animals. By considering what is better for the future, we can curb our animalistic impulses and choose to act rationally and cooperate for the betterment of everyone involved. As humans lower their time preference, they develop a scope for carrying out tasks over longer time horizons. Instead of spending all our time producing goods for immediate consumption, we can choose to spend time creating superior goods that take longer to complete but benefit us more in the long run. Only by lowering time preference can humans produce goods that are not meant to be consumed themselves but are instead used in the production of other goods. Goods used exclusively for the production of other goods are called *capital goods* .

Only humans with a lower time preference can decide to forgo a few hours of fishing and opt to build a superior fishing pole, which cannot be eaten itself, but in the future will enable better results per hour of human effort spent fishing. This is the essence of *investment*: humans defer immediate gratification and invest their time producing capital goods which will, in turn, make the production process itself more sophisticated, extend it over a longer time horizon and yield superior results per hour of human effort. In this way, investment increases capital good stocks which increases productivity. Amazingly, this effect also transforms into a *positive feedback*

loop . Also known as a virtuous cycle or the flywheel effect, a positive feedback loop is a process that is recursively energized (its outputs also serve as its inputs) and therefore creates compounding effects. Positive feedback loops play an important role in biology, chemistry, psychology, sociology, economics and cybernetics. In respect to investment, as more capital goods are accumulated, levels of productivity are increased even more and the time horizon of production is extended even further:



As people exhibit lower time preferences and spend their time wisely, they increase their capacity for investment and create more free time for themselves.

To understand this preference clearly, let's consider two hypothetical fishermen, Harold and Louis, who start out with nothing other than their bare hands. Harold has a higher time preference than Louis and chooses to spend his time catching fish with using just his bare hands. Using this approach, Harold spends about 8 hours per day to catch enough fish to feed himself for one day. Louis, on the other hand, spends just 6 hours per day catching fish, makes do with the smaller amount of fish and chooses to spend the other 2 hours building a fishing pole. Two weeks later, Louis has succeeded in building a fishing pole, which he can now use to catch twice as many fish per hour as Harold. Louis's investment in the fishing pole could allow him to only fish for 4 hours each day, eat the same amount of fish as Harold and spend his other 4 hours in leisure. However, since Louis has a lower time preference, he instead chooses to fish for 4 hours per day and spend the other 4 hours building a fishing boat.

One month later, Louis has succeeded in building a fishing boat, which he can now use to go further out to sea and catch fish that Harold has never even seen. Not only has Louis increased his productivity (fish caught per man hour) but he has also increased the quality of his production (a greater variety of fish from the deep sea). By using his fishing pole and boat, Louis now needs only 1 hour per day to catch a day's worth of food and spends his other 7 hours engaged in further capital accumulation—building better fishing poles, boats, nets, lures, etc.—which, in turn, further increases his productivity and quality of life.

Should Louis and his descendants continue to exhibit a lower time preference, the results will compound over time and across generations. As they accumulate more capital, their work efforts will be ever-further amplified by productivity gains and enable them to engage in ever-larger projects that take ever-longer to complete. These gains are amplified even further when Louis and his descendants begin trading with others that specialize in crafts in which they themselves do not—such as housing, wine making or farming. Successive layers of learning, productivity gains and flourishing trade networks are the foundational sediment upon which all human advancement in terms of knowledge, technology and culture is built. Human advancement is noticeable in the tools we make and the way we relate with one another.

From this perspective, it becomes clear that the most important economic decisions any individual faces are related to the trade-offs they face with their future self. Eat less fish today, build a fishing boat tomorrow. Eat clean today, be healthy tomorrow. Exercise today, be fit tomorrow. Read books today, be knowledgeable tomorrow. Invest money today, be wealthy tomorrow. We can all take solace that this compounding force of nature is always available to each and every one of us. No matter how bad the circumstances are for a man with a low time preference, he will

likely find a way to keep compounding his present efforts and prioritizing his future self until he achieves his objectives. Contrarily, no matter how much fortune and wealth favors the man with a high time preference, he will likely find a way to continue squandering his wealth and shortchanging his future self. These individual relationships with our future selves is the microcosm of the societal macrocosm. As society develops a lower time preference, its prospects of prosperity improve in tandem.

Foundation of Economic Growth [1,4]

There are many factors beyond the scope of this essay which influence time preference. Most relevant to our discussion is the expected future value of money. As we have seen, hard money is superior at holding its value across time. Since its purchasing power tends to remain constant or grow over time, hard money incentivizes people to delay consumption and invest for the future, thereby lowering their time preference. On the other hand, soft money is subject to having its supply increased unexpectedly. Increasing the money supply is the same as lowering the *interest rate*, which is effectively the price of borrowing money and the incentive to save. By reducing the interest rate, the incentive to save and invest is diminished whereas the incentive to borrow is increased. So, soft money disincentivizes a favorable orientation towards the future. In other words, soft money systems raise society's time preference. For this reason, soft money, once it is sufficiently debased, tends to precede societal collapse (more on this later).

An ideal hard money would be one whose supply is absolutely scarce, meaning no one could produce more of it. The only noncriminal way to acquire money in such a society would be to produce something of value and exchange it for money. As everyone seeks to acquire more money, everyone would become ever-more productive which would encourage capital accumulation, productivity gains and a lowering of time preference. Since the money supply is fixed, economic growth would cause the prices of real goods and services to drop over time, as a fixed quantity of monetary units chases an increasing quantity of goods. Since people could expect to be able to purchase more with the same amount of money in the future, such a world would discourage immediate consumption and encourage saving and investment for the future. Paradoxically, a world that consistently defers consumption will actually end up consuming more in the long run as its increased savings would increase investment and productivity, thus making its citizens wealthier in the future. This dynamic would spark a positive feedback loop—with present needs met and an ever-greater focus on the future, people naturally begin concentrating other aspects of life such as social, cultural and spiritual endeavors. This is the essence of free market capitalism: people choosing to lower their time preference, defer immediate gratification and invest in the future.

The foundation of all economic growth is delayed gratification, which leads to savings, which leads to investment, which extends the duration of the production cycle and increases productivity in a self-sustaining, virtuous cycle with no known natural limit.

Debt is the opposite of saving. As saving creates the possibility for capital accumulation and its associated benefits, debt is what can reverse it by reducing capital stocks, productivity and living standards across generations. As we will show later, when the gold standard was forcibly ended by governments, money not only became much softer, but it also fell under the command of politicians who are incentivized to operate with high time preferences as they strive for reelection every few years. This explains why politicians continue to mandate the use of soft government money, despite the long-term harm it causes to an economy, ensuring that it remains the dominant form of money in the world (we will cover soft government money's unnatural ascent to world domination later).

When a form of money becomes globally dominant, it finally serves the third function of money—*unit of account* . History shows us that this function is the final evolutionary stage in the natural ascendancy of monetary goods that achieve a dominant role—which are first a store of value, then a medium of exchange and finally a unit of account. As economist William Stanley Jevons explained:

"Historically speaking, gold seems to have served, firstly, as a commodity valuable for ornamental purposes; secondly, as stored wealth; thirdly, as a medium of exchange; and, lastly, as a measure of value."

Today, the US Dollar is dominant and serves as the global unit of account as prices are most commonly expressed in its terms. This consistency of expression simplifies trade and enables a (somewhat) stable pricing structure for the global economy.

The Economic Nervous System [1]

Market prices are an essential communicative force in economics. As economic production moves from a primitive scale, it becomes harder for individuals to make production, consumption and trade decisions without having a fixed frame of reference (unit of account) which to compare the value of different objects to one another.

In his paper 'The Use of Knowledge in Society' Friedrich Hayek elucidated the economic problem as not merely a matter of allocating human effort. More accurately, the economic problem is one of allocating human effort according to knowledge that is distributed in the minds of people that are each primarily concerned with their respective area in the broader economy. This distributed knowledge includes the:

- Conditions of production
- Availability of the factors of production
- Preferences of individuals

Knowledge, due to its dynamic and fluid nature, cannot be fully known by a single entity as it is constantly in flux and widely distributed within many minds. In a free market economic system prices capture this distributed knowledge, convert it into impartial information and disseminate it widely. *Price signals* are the coordinating force of free market systems. Each individual decision maker can faithfully rely on the prices of goods relevant to their production process, as the prices themselves are a distillation of all known market realities into a single, actionable variable. Each individual's buy and sell decisions, in turn, further shape prices which carry this altered information back out into the market. Price signals are to market participants what light is to the eye.

To understand this point, consider the 2010 earthquake which badly damaged an area in Chile responsible for a great deal of the world's copper production. This earthquake severely damaged copper mines and export infrastructure, which immediately reduced the flow of new supply to the world copper market and resulted in a 6.2% increase in its price. Anyone in the world whose business interfaces with the copper market will be affected by this, but they do not need any specific knowledge about the earthquake in Chile or market conditions to decide how to respond. All the relevant information they need to make effective decisions is contained within the price of copper itself. Immediately, all firms that demand copper are incentivized to demand less, delay purchases or find substitutes. On the other side of the market, all firms that produce copper are incentivized to produce more of it. With a natural shift in price, everyone in the world involved in the copper industry is incentivized to act in a way that alleviates the negative consequences of the earthquake. This is the power of a free market with accurate price signals.

The wisdom of the crowd is always superior to the wisdom of the board room. There is simply no way to recreate the adaptivity and collective intelligence of markets by installing a centralized planning authority. How would they decide who should increase production and by how much? How would they decide who should reduce consumption and by how much? How would they coordinate and enforce their decisions in real time on a global scale? In this sense, prices are the economic nervous system that disseminate knowledge across the world and help coordinate complex production processes by:

- Incentivizing supply and demand changes to match economic reality and restore market equilibriums quickly
- Efficiently matching buyers and sellers in the marketplace

- Compensating producers for their work efforts

Without accurate price signals, humans could not benefit from the division of labor and specialization beyond a small scale. Trade allows producers of goods to mutually increase their living standards by specializing in goods in which they have a relative or *comparative advantage*—goods they can produce relatively faster, cheaper or better. Accurate prices expressed in a common, stable medium of exchange help people identify their comparative advantage and specialize in it. Specialization, guided by reliable price signals, enables producers to improve their efficiency of production and accumulate capital specific to their craft. This is why the most productive allocation of human efforts is only determinable by an accurate pricing system within a free market. Also (as we will see later), this is exactly why capitalism prevailed over socialism, because socialism lacked an economic nervous system. But before diving into the economic aspects which underpinned this historic ideological struggle and seeing how it is still relevant today, we first need to understand the evolutionary forces that have shaped money throughout history.

Monetary Evolution [1]

Throughout history, money has taken many forms—seashells, salt, cattle, beads, stones, precious metals and government paper have all functioned as money at one or more points in history. Monetary roles are naturally determined by the technological realities of the societies shaping the salability of goods. Even today, forms of money still spontaneously emerge with things like prepaid mobile phone minutes in Africa or cigarettes in prisons being used as localized currencies. Different monetary technologies are in constant competition, like animals competing within an ecosystem. Although instead of competing for food and mates like animals, monetary goods compete for the belief and trust of people. Believability and trustworthiness form the basis of *social consensus*—the source of a particular monetary good's sovereignty from which it derives its market value along with the trust factors and permissions necessary to transact with it.

As these competitions continue to unfold in a free market, goods attain and lose monetary roles according to the traits which determine how believable or trustworthy they are and are expected to remain over time. As we will show, free market competition is ruthlessly effective at promulgating hard money as it only allows those who choose the hardest form available to maintain wealth over time. This *market-driven natural selection* causes new forms of money to come into existence and older forms to fade into extinction. Like biologically-driven natural selection, in which nature continuously favors the organisms which are best suited for success in their respective ecologies, this market-driven natural selection is a process in which people naturally and rationally favor the most believable and

trustworthy monetary technologies available in their respective trade networks. Unlike ecological competition which can favor many dominant organisms, the marketplace for money is driven by network effects and favors a winner take all (or, at least, a winner take most) dynamic as the non-coincidence of wants problem is universal and if a single hard money is capable of solving all three of its dimensions than it will become dominant (as discussed earlier in the social network aspects of money).

An example of this market-driven natural selection of money comes from the ancient Rai Stones system of Yap Island, located in what is today Micronesia. Rai Stones were large disks of various sizes with a hole in the middle that weighed up to eight thousand pounds each. These stones were mined in neighboring Palau or Guam and were not native to Yap. Acquiring these stones involved a labor-intensive process of quarrying and shipping. Procuring the largest Rai Stones required workforces numbering in the hundreds. Once the stones arrived in Yap, they were placed in a prominent location where everyone could see them. Owners of the stones could then use them as payment by announcing to the townsfolk the transfer of ownership to a new recipient. Everybody in the town would then record the transaction in their individual ledger, noting the new owner of the stone. There was no way to steal the stone because its ownership was recorded by everyone. In this way, the Rai Stones solved the three dimensions of the non-coincidence of wants problem for the Yapese by providing:

- Salability across scales as the stones were various in size and payments could be made in fractions of a stone
- Salability across space as the stones were accepted for payment everywhere on the island and did not have to be moved physically, just recorded by the townsfolks' individual ledgers (remarkably similar to Bitcoin's distributed ledger model, as we will see later)
- Salability across time due to the durability of stones and the difficulty of procuring new stones which meant that the existing supply of stones was always large relative to any new supply that could be created within a given time period (a high stock-to-flow ratio)

This monetary system worked well until 1871, when an Irish-American captain named David O'Keefe was found shipwrecked on the shores of Yap by the local islanders. Soon, O'Keefe identified a profit opportunity in buying coconuts from the Yapese and selling them to coconut oil producers. However, he could not transact with the locals because he was not a Rai Stone owner and the locals had no use for his foreign forms of money. Undeterred, O'Keefe sailed to Hong Kong and acquired some tools, a large boat and explosives to procure Rai Stones from neighboring Palau. Although he met resistance from them initially, he was eventually able to use his Rai Stones to

purchase coconuts from the Yapese. Other opportunists followed O'Keefe's lead and soon the flow of Rai Stones increased dramatically. This sparked conflict on the island and disrupted economic activity. By using modern technologies to acquire Rai Stones more cheaply, foreigners were able to compromise the hardness of this ancient monetary good. The market naturally selected against Rai Stones because, as their stock-to-flow ratio declined, they became less reliable as a store of value and thus lost their salability across time, which ultimately led to the extinction of this ancient monetary system.

A similar story played out in western Africa which for centuries used aggry beads as money. These small glass beads were used in a region where glassmaking was an expensive craft, which gave them a high stock-to-flow ratio and made them salable across time. Since aggry beads were small and light they could easily be combined into necklaces or bracelets and transported easily, thus giving them salability across scales and space. In the 16th century, European explorers discovered the high value ascribed to these beads by the west Africans and began importing them in mass quantities; as European glassmaking technology made them extremely cheap to produce. Slowly but surely, the Europeans used these cheaply produced beads to acquire most of the precious resources of Africa. The net effect of this incursion into Africa was the transference its vast natural resource wealth to Europeans and the conversion of aggry beads from hard money to soft money. Again, the market naturally selected against a monetary good once its stock-to-flow ratio began to decline, as its store of value functionality and, therefore, its salability across time were compromised as a result. Although the details vary, this underlying dynamic of a declining stock-to-flow ratio presaging a good's loss of its monetary role has been the same for every form of money throughout history. Today, we are seeing a similar pattern cause the collapse of the Venezuelan bolivar, (where some Venezuelans are using Bitcoin to protect their wealth as the currency collapses).

As societies continued to evolve, they began to move away from artifact money like stones and glass beads and towards monetary metals. It was initially difficult to produce most metals which kept their supply flows low, thus giving them good salability across time. Gold in particular, with its extreme rarity in the Earth's crust and its virtual indestructibility, made it an extremely hard monetary technology. Gold mining was difficult, limiting supply increases relative to its existing supply, which itself could not be destroyed. Gold gave humans a way to store value across generations and develop a longer-term perspective on their actions (a lower time preference), which led to the proliferation of ancient civilizations:

The earliest coins are found mainly in the parts of modern Turkey that formed the ancient kingdom of Lydia. They are made from a naturally occurring mixture of gold and silver called electrum.

Monetary Metals [1]

The last dictator of the Roman Republic, Julius Caesar, issued a gold coin called the aureus coin which contained a standard 8 grams of gold. The aureus was traded widely across Europe and the Mediterranean, alongside a silver coin called the denarius, which was used for its superior salability across scales. Used together, these coins provided a hard money system that increased the scope of trade and specialization in the Old World. The republic became more economically stable and integrated for 75 years until the infamous emperor Nero came into power.

Nero was the first to engage in the act of *coin clipping* in which he would periodically collect the coins of his citizenry, melt them down and mint them into newer versions with the same face value but less precious metal content, keeping the residual content to enrich himself. Similar to modern day inflation, this was a way of surreptitiously taxing the population by debasing its currency. Nero and successive emperors would continue the practice of coin clipping for several hundred years to finance government expenditures:

Isaac Newton is attributed with adding the small stripes along the edges of coins as a security measure against coin clipping. These stripes are still present on most coins today.

Citizens gradually wised up to this deceit and began hoarding the coins with higher precious metal content and spending the debased coins, as they were legally required to be accepted at face value in settlement of debts, one of the earliest instances of *legal tender* laws being implemented. This had the effect of driving up the price of coins with higher precious metal content and driving down the price of those with less—a dynamic that came to be known as *Gresham's Law*: bad money (soft money) drives good money (hard money) out of circulation. This is an important law to recall when we look at how modern-day hoarding of Bitcoin impacts its price.

Eventually, a new coin called the solidus was introduced which contained only 4.5 grams of gold, almost half the content of the original aureus coin. Pursuant to this decline in monetary value, a cycle familiar to many modern economies running on government money began to take hold—coin clipping reduced the money's real value, increased the money supply, gave the emperor the means to continue imprudent spending and eventually ended with rampant inflation and economic crisis. Analogous to central bank practices today, Swiss banker Ferdinand Lips summarized this era well:

"Although the emperors of Rome frantically tried to 'manage' their economies, they only succeeded in making matters worse. Price and wage controls and legal tender laws were passed, but it was like trying to hold back the tides. Rioting, corruption, lawlessness and a mindless mania for speculation and gambling engulfed the empire like a plague."

Amid the chaos of the crumbling Roman Republic, Constantine the Great took power. Intent on restoring the once great empire, Constantine began adopting responsible economic policies. He first committed to maintaining the solidus at 4.5 grams of gold, ended the practice of coin clipping and began minting massive quantities of these standardized gold coins. Constantine then moved east and established Constantinople in modern day Istanbul. This became the birthplace of the Eastern Roman Empire, which adopted the solidus as its monetary system.

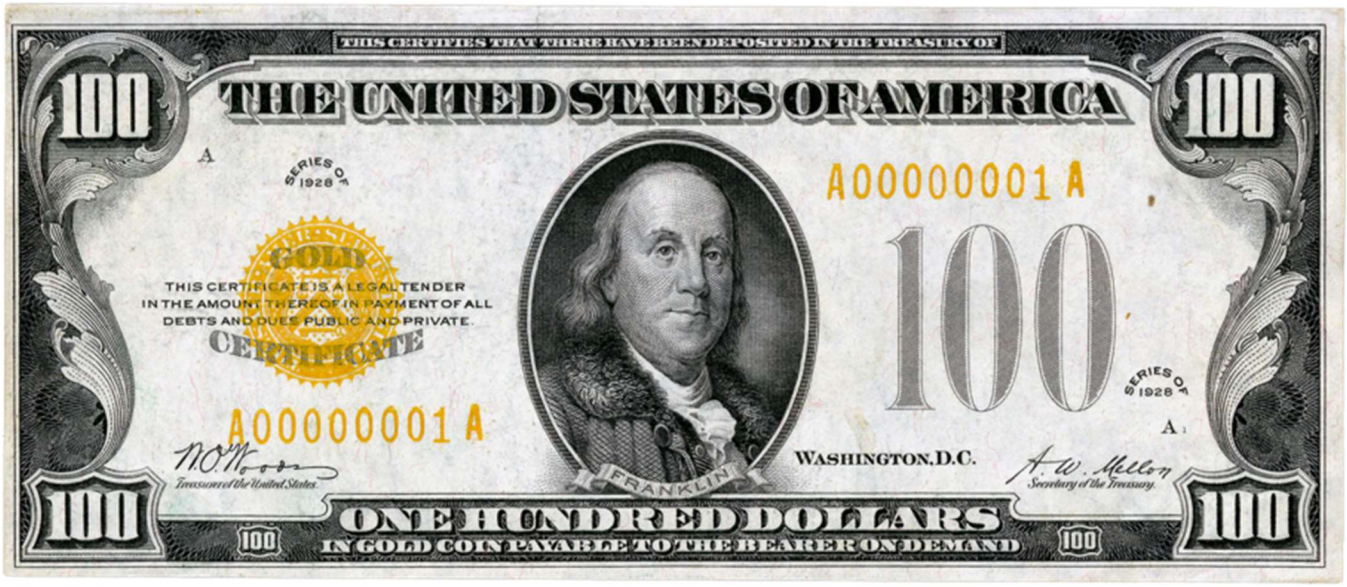
Rome continued its soft money-induced cultural deterioration until it finally collapsed in 476 AD. Meanwhile, Constantinople flourished. The solidus, which eventually became known as the bezant, provided a hard money system with which Constantinople would remain prosperous and free for centuries to come. As with Rome before it, the fall of Constantinople happened only when its rulers began the debasing its currency around 1050 AD. As with Rome before it, the move away from hard money led to the fiscal and cultural decline of the Eastern Roman Empire. After suffering many successive crises, Constantinople was ultimately overtaken by the Ottomans in 1453. However, the bezant inspired another form of hard money that still circulates to this day, the Islamic dinar. People all over the world have used this coin for over seventeen centuries—which began as the solidus before changing its name to the bezant and finally becoming the Islamic dinar—for transactions, thus highlighting the superior salability of a hard money such as gold across time.

Following the collapse of the Roman Empire, Europe fell into the dark ages. It was the rise of the city-state (a new story mankind would begin organizing itself around) and its use of hard money systems that would pull Europe out of the Dark Ages and into the Renaissance. Beginning in Florence in 1252, the city minted the florin which was the first major European coinage issued since Julius Caesar's aureus. By the end of the 14th century more than 150 European cities and states had minted coins to the same specifications as the florin. By giving its citizenry the ability to accumulate wealth in a reliable store of value which could be traded freely across scales, space and time, this hard money system unlocked scientific, intellectual and cultural capital within the Italian city-states and eventually spread to the rest of Europe. Of course, the situation was far from perfect, as there were still many periods marked by various rulers choosing to debase their currencies to finance war or lavish expenditure.

Global Gold Standard [1,4]

When they were being used as physical means of settlement, gold and silver coins served complementary roles. Silver, having a stock-to-flow ratio second only to that of gold, had the advantage of being a more salable metal across scales, since its lower value per weight than gold made it ideal as a medium of exchange for smaller transactions. In this way, gold and silver were complementary as gold could be used

for large settlements and silver could be used for smaller payments. However, by the 19th century, with the development of modern custodial banking and advanced telecommunications, people were increasingly able to transact seamlessly across scales using bank notes or checks backed by gold:



The US Dollar was once redeemable for gold on demand.

With all of the critical salability characteristics gathered under a gold standard monetary system facilitated by paper bank notes, the superior salability across scales of physical silver lost relevance, setting it up to become demonetized (due to the winner take all dynamic discussed earlier). Ironically, the same banking industry that enabled a global gold standard would in later years see to its elimination (more on this later).

A brief aside on silver: This demonetization dynamic also explains why the silver bubble popped many times throughout history when facing off with gold and will pop again if it ever reflates. Since silver is not the hardest form of monetary good available, should any significant investment flow into silver, its producers will be incentivized to increase the flow of silver, and store any value expropriated from its increased production in the hardest form of money available to them (which, before Bitcoin, was only gold). This, of course, will bring the price of silver crashing back down, taking the wealth from the investment inflows with it. As a more recent historical example of this dynamic in action: In the 1970s, the affluent Hunt brothers attempted to remonetize silver by buying vast quantities of it in the market. This drove up the price initially, and the Hunt brothers believed they could continue driving up its price until they cornered the market. Their intent was to induce others to chase its appreciation and recreate a monetary demand for silver. As they kept buying and the price kept rising, silver holders and producers kept selling into the

market. No matter how much the Hunt brothers purchased, the selling and flow of silver continued to outpace their buying, which decreased its stock-to-flow ratio and eventually led to a dramatic crash in the price of silver. The Hunt brothers lost over $1B (due to rampant inflation of government money since then, their losses equal $6.5B in 2019 dollars) in the ordeal, which is likely the highest price ever paid for learning the importance of hard money and its defining metric, the stock-to-flow ratio.

Driven by expanding telecommunication and trade networks, and with custodial banks enhancing its salability across scales by issuing gold-backed bank notes and checks, the gold standard spread quickly. More nations began switching to paper based monetary systems fully backed by and redeemable in gold. Network effects took hold as more nations moved onto the gold standard, giving gold deeper liquidity, more marketability and creating larger incentives for other nations to join.

Those nations which remained on a silver standard the longest before converting, like China and India, witnessed tremendous devaluations of their currencies in the intervening period. The demonetization of silver for China and India was an effect similar to the west Africans holding aggry beads when Europeans arrived. Foreigners who adopted the gold standard were able to gain control over vast quantities of the capital and resources in China and India. This drives home a key point: every time hard money encounters a softer form of money in a trade network, the softer money is ultimately outcompeted into extinction.

This dynamic has significant consequences for the holders of soft money and is an important lesson for anyone who believes their refusal of Bitcoin means they are protected from its economic impact. History shows us repeatedly that it is not possible to protect yourself from the consequences of others holding money that is harder than yours.

Finally, for the first time in history, the majority of the world economy began operating on a gold-based, hard money standard that was naturally selected for by the free-market.

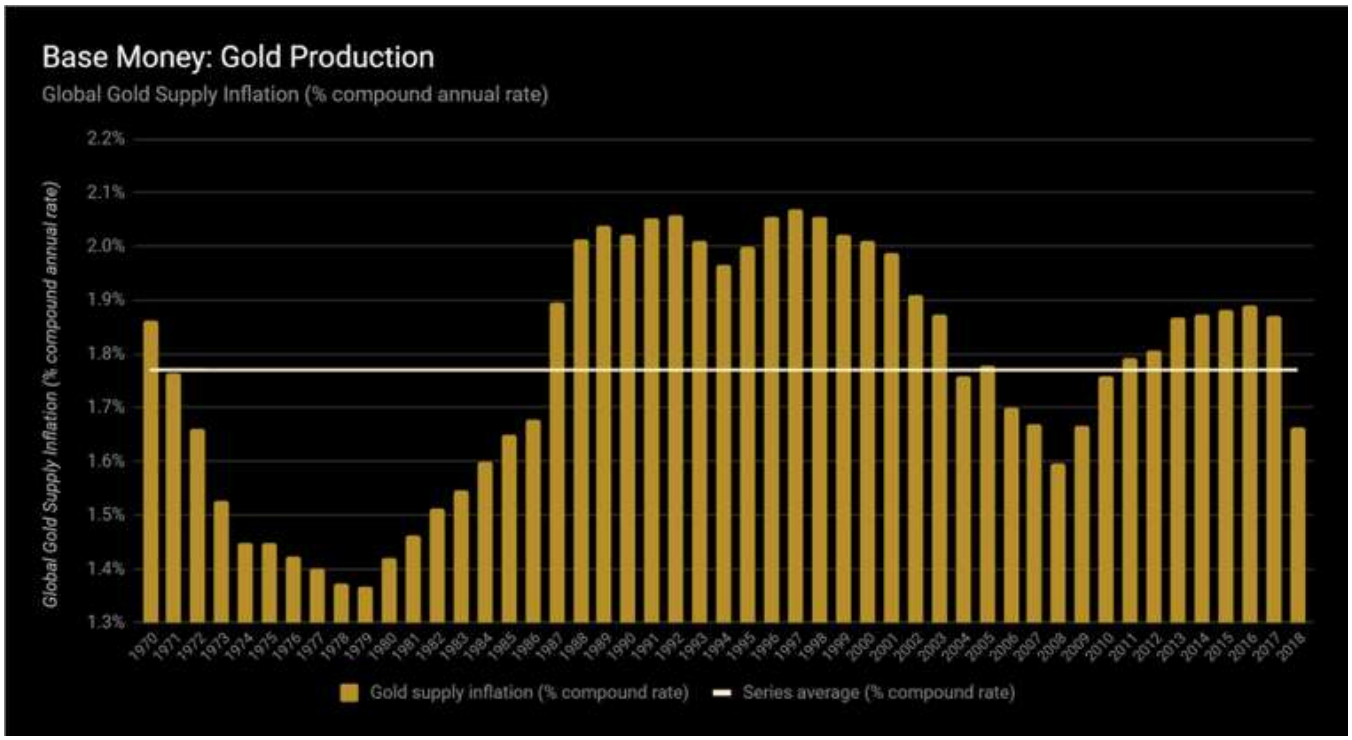
Hardness of Gold [1,3]

By this point in history, virtually everyone had come to fully trust gold's superior stock-to-flow ratio and therefore believed they could use it to reliably store value across time. After thousands of years of mining this chemically stable element, virtually all the gold ever procured by humans is still a part of its extant supply. The stock of all the gold in the world fits into an Olympic-sized swimming pool today and is valued at almost $8T USD. Gold is rare in the Earth's crust and extraction is costly in terms of time and energy, which keeps its flow predictably low. It is impossible to

synthesize gold by chemical means (as alchemy never panned out) and the only way to increase its supply is through mining.

The costliness of gold mining is the *skin in the game* necessary to increase its flow—the risk necessary to procure the reward. Skin in the game is a concept based on symmetry, a balance of incentives and disincentives: in addition to upside exposure, people should also be penalized if something for which they are responsible for goes wrong or hurts others. Skin in the game is the central pillar for properly functioning systems and is at the heart of hard money. For gold, its mining costs and risks form the disincentives which are balanced against the incentives of its market price. Unless consequential decisions are made by people who are exposed to the results of their decisions, the system is vulnerable to total collapse (an important consideration when we discuss soft government money later).

Every market-driven evolutionary step for money has naturally selected the form with the highest stock-to-flow ratio available to its population but stopped when the form lost this key property. With the highest stock-to-flow ratio of all the monetary metals, gold is the hardest physical form of money that has ever existed, which explains its success as hard money throughout history. Even with advances in mining techniques, gold still has a relatively low and predictable flow, as evidenced by its annual supply growth since 1970:



The rarity of gold in the Earth's crust ensures that its new supply flows are relatively low and predictable. Since gold is virtually indestructible, nearly every ounce that has ever been mined throughout history is still part of current supply stocks. The

combination of these factors gives gold the highest stock-to-flow ratio of any monetary metal and is precisely the reason gold became a global hard money standard.

Gold mining, of course, only makes economic sense if the cost of producing an additional ounce of gold is less than gold's market price per ounce. Relatedly, when the price of gold increases, its mining becomes more profitable and draws new miners into the market and makes new methods of gold mining economically feasible. This, in turn, increases the flow of gold until supply and demand forces again reach equilibrium. So, although gold is the hardest form of physical money, it doesn't have perfect hardness as changes in demand for it elicit both a supply and price response, meaning:

- An increase in the demand for gold increases its price,
- An increase in the price of gold incentivizes gold miners to increase its flow,
- An increase in the flow of gold increases its supply
- An increase in the supply of gold puts downward pressure on its price

In this way, changes in demand for gold are expressed partially in its price and partially in its supply flow. This *price elasticity of supply* is true for all physical commodities. For all practical purposes, as we will see later, the Earth always has more natural resources to yield assuming the right amount of time and effort are directed towards their production (this will support an important point later when we look at the impact of changes in demand on Bitcoin's price).

Final Settlement [1]

Gold also has the advantage of being an instrument of *final settlement* . Whereas the use of government money requires trust in the monetary policy and creditworthiness of the issuing authority or payment intermediaries, known as *counterparty risk*, the act of physically possessing gold comprises all of the trust factors and permissions necessary to use it as money. This makes gold a self-sovereign form of money. This is best understood as an identity of the universal accounting equation: Assets = Liabilities + Owner's Equity

When you own gold free and clear, it is your asset and no one else's liability, meaning that your personal balance sheet includes a 100% gold asset matched by 0% liabilities and 100% owner's equity (since no one else has a claim on your gold asset). This makes gold a *bearer instrument*, meaning that any individual in physical possession of the asset is presumed to be its rightful owner. This timeless and trustless nature of gold is the reason why it still serves as the base money and final settlement system of central banks worldwide.

In the 19th century, the term *cash* referred to central bank gold reserves, which was the dominant self-sovereign monetary good at the time. Cash settlement referred the transfer of physical gold between central banks to execute final settlement. Central banks can only settle with finality in physical gold, and still do so periodically in the modern era, since it is the only form of money that requires no trust in any counterparty, is politically neutral and gives its holders full sovereignty over their money. This is why gold maintains its monetary role even today as only the delivery of a bearer instrument can truly be the final extinguisher of debt. In this original sense of the word cash, gold is the only form of dominant cash money that has ever existed (although Bitcoin is well-suited to serve a similar role in the digital age, more on this later). Unfortunately, the combination of gold's self-sovereignty and physicality would lead to the demise of the gold standard.

Centralization of Gold [1,4]

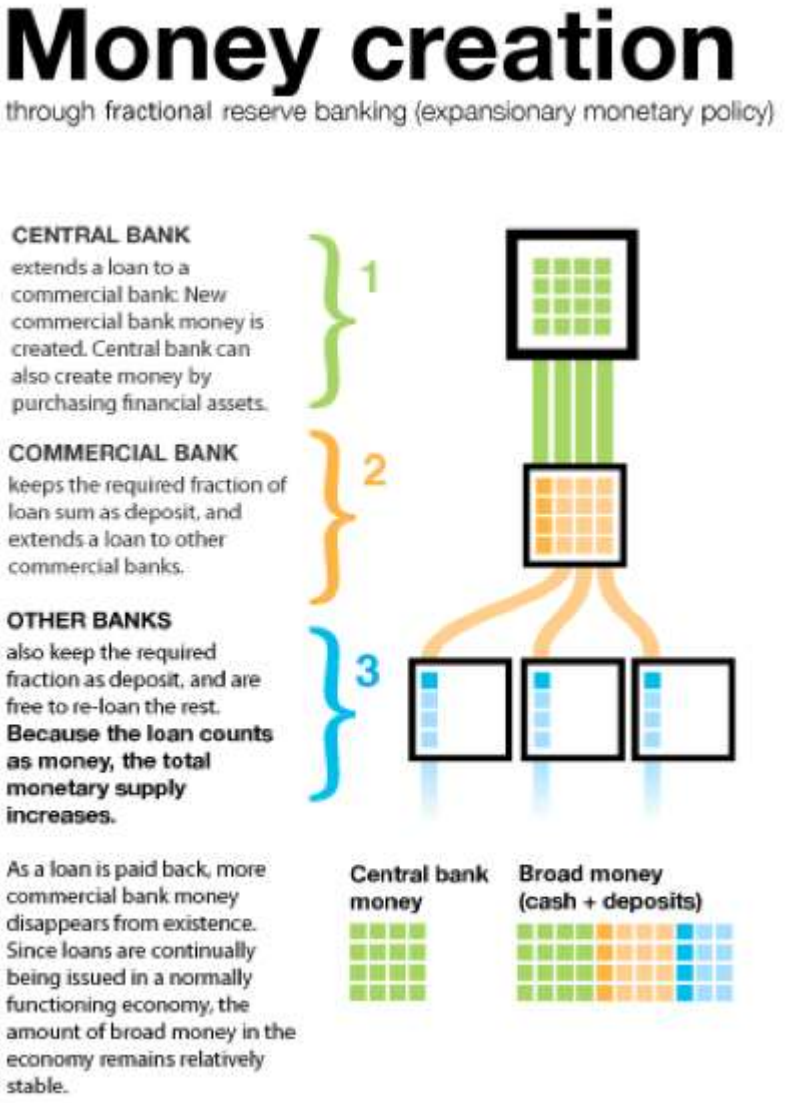
By the end of the 19th century, all the industrialized nations of the world were officially on the gold standard. By virtue of operating on a hard money basis, most of the world witnessed unprecedented levels of capital accumulation, free global trade, restrained government and improving living standards. Some of the most important achievements and inventions in human history were made during this era, which came to be known as *la belle époque* across Europe and *the Gilded Age* within the United States. This golden era enabled by the gold standard remains one of the greatest periods in human history:

"La Belle Époque was a period characterized by optimism, regional peace, economic prosperity, an apex of colonial empires, and technological, scientific, and cultural innovations. In the climate of the period, the arts flourished. Many masterpieces of literature, music, theater, and visual art gained recognition."

As multiple societies had now converged on gold as their universal store of value, they experienced significant decreases in trade costs and an attendant increase in free trade and capital accumulation. La Belle Époque was an era of unprecedented global prosperity. However, the hard money gold standard which catalyzed it suffered from a major flaw: settlement in physical gold cumbersome, expensive and insecure. This flaw is associated with the physical properties of gold, as it is dense, not deeply divisible and not easily transactable. Gold is expensive to store, protect and transport. It is also heavy per unit of volume which makes it difficult to use for day to day transactions. As discussed earlier, banks built their business model around solving these problems by providing secure custody for people's gold hoards. Soon after, banks began issuing paper bank notes that were fully redeemable in gold. Carrying and transacting with paper bank notes backed by gold was much easier than using actual gold. Offering superior utility and convenience, the use of bank notes flourished. This, along with government programs to confiscate gold from

citizens (such as Executive Order 6102 in the United States), encouraged the centralization of gold supplies within bank vaults all over the world.

Incapable of resisting the temptation of wealth expropriation by tampering with the money supply, banks soon began issuing more notes than their gold reserves could justify, thus initiating the practice of *fractional reserve banking* . This banking model facilitated the creation of money without any skin in the game. Governments took notice and began to gradually take over the banking sector by forming central banks, as this model enabled them to engage in *seigniorage*, a method of profiting directly from the *money creation process*:



In fractional reserve banking artificial money and credit is created. For instance, assuming a reserve

ratio of 10% and an initial deposit of $100 will soon turn into $190. By lending a 90% fraction of the newly created $90, there will soon be $271 in the economy. Then $343.90. The money supply is recursively increasing, since banks are literally lending money they don't have. In this way, banks magically transform $100 into over $1,000.

The ability to control this process was too tempting for governments to resist. Total control of over the money supply gave those in charge a mechanism to continually extract wealth from its citizenry. The virtually unlimited financial wealth the printing press provided gave those in power the means to silence dissent, finance propaganda and wage perpetual warfare. It is a fundamental economic reality that wealth cannot be generated by tampering with the money supply, it can only be manipulated and redistributed. Civilization itself relies on the integrity of the money supply to provide a solid economic foundation for free trade and capital accumulation. With a firm grip on the prevailing monetary order established, the next logical step for central banks was to begin moving away from the gold standard altogether.

Abolishing the Gold Standard [1]

By 1914, most of the major economies had begun printing money is excess of their gold reserves at the onset of World War I. Unsurprisingly, this had many negative consequences, some of which were immediate while others came on more slowly. Eliminating the gold standard immediately destabilized the unit of account by which all economic activity was assessed. Government currency exchange rates would now float against one another and become a source of economic imbalance and confusion. This distorted price signals, which would now be denominated in various government currencies with rapidly fluctuating exchange rates. This made the task of economic planning as difficult as trying to build a house with an elastic measuring tape.

For a world that was becoming increasingly globalized and technologically sophisticated, freely floating currency exchange rates represented a significant step backwards and gave rise to what is commonly called a 'a system of partial barter'. For people to buy goods from other people who lived on the other side of any number of imaginary lines called national borders, they would now be required to use more than one medium of exchange (their own currency and the foreign currency) to complete the transaction. To an extent, this reignited the non-coincidence of wants problem which money was meant to solve in the first place. Today, over $5T ($5,000,000,000,000) of foreign currencies are exchanged daily, forming an annual market valued at over 12 times global GDP. This industry is purely parasitic—it enriches bankers and sucks real value out of society in the form of global trade frictions, market distortions and transaction fees. For this reason, it is excluded from

GDP calculations and exist solely because of the inefficiencies caused by centrally controlled capital markets and the absence of a global, politically neutral hard money system. The resultant frictions to global trade fanned the flames of warfare.

Governments Take Control [1,3]

As 20th century wars raged, so did the printing presses. Governments and their central banks continued to grow more powerful with each new bank note printed as their citizens became poorer. The death stroke came when most governments, due to a unilateral decision of President Nixon in United States, finally severed the peg to gold entirely in the 1971. Which brings us to the modern form of dominant money: *government fiat money* . Fiat is a Latin word meaning decree, order or authorization. This is why government money is commonly referred to as fiat money, since its value exists solely because of government decree:

Today, the US Dollar is not redeemable for anything and its value is derived solely from government decree. Paradoxically, people were coerced into adopting soft government fiat money only because of their shared belief in gold as a hard monetary good.

This is an imperative point: it was possession of gold (self-sovereign, hard money) that gave governments the power to decree the value of their fiat money (soft money) in the first place. National governments were only able to achieve “sovereignty” because they drew this power from their possession of gold. Paradoxically, people were coerced into discarding the gold standard and adopting soft government fiat money only because of their belief in gold as a hard monetary good. This is proof that it is possible to create an artificial asset and endow it with monetary properties, whether by decree or by market-driven natural selection. Governments did so by stealing gold from citizens, which gave them the power to create fiat money and decree its value

by force. As we will later see, Satoshi Nakamoto did so by creating Bitcoin and releasing it into the marketplace as a self-sovereign money free to compete for the trust and belief of the people based on its own merits.

Central banks also began engaging in propaganda campaigns declaring the end of gold's monetary role. However, their actions rang louder than their words as they continued to accumulate and hold gold, a practice they continue to this day. Gold remains the exclusive instrument of final settlement between central banks. Strategically, holding large gold reserves also makes sense for central banks since they can opt to sell reserves into the market should gold start to appreciate too quickly and threaten the value of fiat money. With their monopoly position protected and reinforced by legal tender laws, propagandists and sufficient control of the gold market central banks were free to print money at will. This exorbitant privilege gives central banks extraordinary power and made them extremely dangerous entities. In the words of former US President Andrew Jackson spoken at the Constitutional Convention in 1787:

"I believe that banking institutions are more dangerous to our liberties than standing armies. If the American people ever allow private banks to control the issue of their currency, first by inflation, then by deflation, the banks and corporations that will grow up around them will deprive the people of all property until their children wake up homeless on the continent their fathers conquered. The issuing power should be taken from the banks and restored to the people, to whom it properly belongs."

Unlike to the flow restrictions associated with gold mining, there are practically no economic restraints preventing a government from printing more fiat money. Since there is virtually no cost associated with producing additional units (no skin in the game), government fiat money is the softest form of money in the history of the world. Predictably, money supplies grew quickly, especially in the heat of warfare. In the past, for societies operating with hard money systems, once the tide of war had shifted in favor of one belligerent over the other, treaties were quick to be negotiated as war is an extraordinarily expensive endeavor. The fiat money printing press, on the other hand, gave governments the ability to tap the aggregate wealth of entire populations to finance military operations by implicitly taxing them via inflation. This provided a more secretive, implicit method of funding warfare than explicit taxation or selling government wartime bonds. Wars began lasting much longer and became more violent. It is no coincidence that the century of total war coincided with the century of central banking:

Table 5.1	Conflicts steadily cost more in human lives		
Period	Conflict-related deaths (millions)	World population, mid-century (millions)	Conflict-related deaths as share of world population (%)
Sixteenth century	1.6	493.3	0.32
Seventeenth century	6.1	579.1	1.05
Eighteenth century	7.0	757.4	0.92
Nineteenth century	19.4	1,172.9	1.65
Twentieth century	109.7	2,519.5	4.35

The ability to print unlimited quantities of money gives governments a means to finance military operations by implicitly taxing their citizens via inflation. This provides a more secretive method of funding warfare then explicit taxation or selling government wartime bonds. Resultantly, wars have grown in duration and violence.

As is to be expected, soft government money has an abysmal track record as a store of value. This becomes abundantly clear when we look at its inflationary effects on the price of gold. An ounce of gold in 1971 was worth $35 USD, and today is worth over $1,200 USD (a decrease of over 97% in the value of each dollar due entirely to inflation). Based on these figures, it is easy to see that gold continues to appreciate as its supply is increased less quickly than the supply of $USD (government fiat money). The constantly increasing supply of government money means its currency depreciates continuously, as wealth is stolen from the holders of the currency (or assets denominated in it) and transferred to those who print the currency or receive it earliest. This transfer of wealth is known as the *Cantillon Effect*: the primary beneficiaries from expansionary monetary policy are the first recipients of the new money, who are able to spend it before it has entered wider circulation and caused prices to rise. Generally, this is why inflation hurts the poorest and helps the bankers, who are closest to the spigot of liquidity (the government fiat money printing press) in the modern economy. A centrally planned market for money like this completely contradicts the principles of free market capitalism.

Free Market Capitalism versus Socialism [1]

In a socialist system, the government owns and controls all means of production. This ultimately makes the government the sole buyer and seller of all capital goods in its economy. Such centralization stifles market functions, like price signals, and makes decision making highly ineffective. Without accurate pricing of capital goods to signal their relative supply, demand and relevant market conditions, there is no

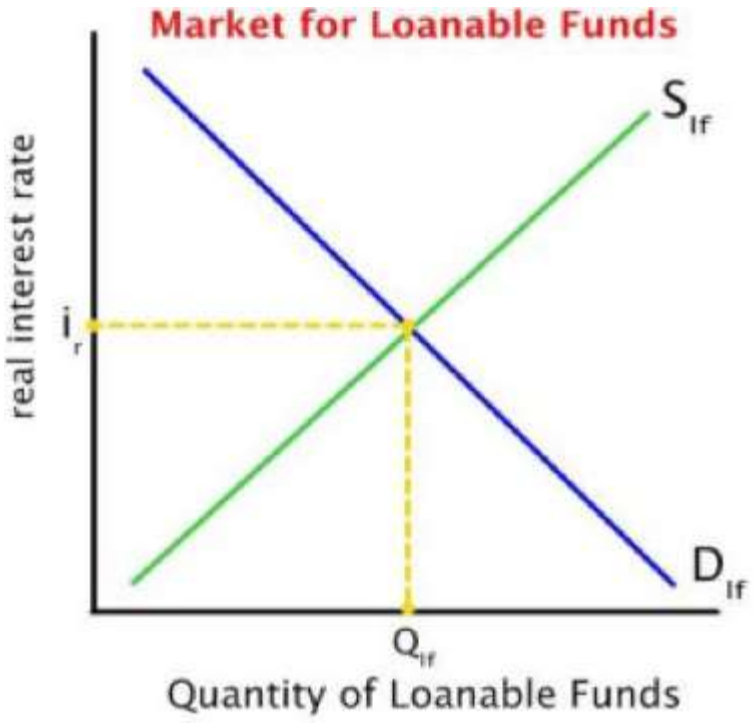
rational way to determine the most productive allocation of capital. Further, there is no rational way to determine how much to produce of each capital good. Scarcity is the starting point of all economics and people's choices are meaningless without skin in the game in the form of price or trade-offs. A survey without a price would find that everyone wants to own a private island but when price is included, very few can afford to own a private island. The point here is not to trumpet free market capitalism over socialism, but rather to clearly explicate the difference between the two ways of allocating resources and making production decisions:

- Free Market Capitalism places trust in Price Signals
- Socialism places trust in Centralized Planning

A free market is one in which buyers and sellers are free to transact on terms determined solely by them, where entry and exit into the market are free and no third parties can restrict or subsidize any market participants. Most countries today have well-functioning, relatively free markets. However, every country in the world today engages in centralized planning of the *market for money* (aka the market for financial capital) itself.

No country in the world today has a free market for money, which is the most important market in any economy.

In a modern economy, the market for money consists of the markets *loanable funds* . These markets match savers with borrowers using the interest rate as their price signal. In a free market for loanable funds, the supply of loanable funds rises as the interest rate rises, as more people are willing to loan their savings out at a higher price. Conversely, the demand for loanable funds decreases as the interest rate rises, as less people are inclined to borrow funds at a higher price:



In a free market for money, the interest rate (the price of money) is determined by natural supply and demand dynamics. Central banks attempt to "manage" these market forces and in doing so create recessions and the boom-and-bust business cycle which is now considered "normal" in the modern era.

Notice that the interest rate in a free market for capital is always positive because of people's naturally positive time preference, meaning that no one would part with money unless they could receive more of it in the future. These natural market forces are artificially manipulated in every market for money in the world. All markets for money in the world today are centrally planned by central banks, who are responsible for "managing" the market for loanable funds using monetary policy tools. Since banks today also engage in fractional reserve banking, they lend out not only customers' savings, but also their demand deposits (monies available to customers on demand, like checking accounts). By loaning out demand deposits to a borrower while simultaneously keeping them available to the depositor, banks can effectively create new, artificial money (a part of the money creation process from earlier). Central banks have the power to manipulate the market for financial capital and can artificially increase the money supply by:

- Reducing interest rates, which increases demand for borrowing and money creation by banks
- Lowering the required reserve ratios, allowing banks to lend more money out than their capital reserves justify

- Purchasing government debt or other financial assets with newly created money in the open market
- Relaxing lending eligibility criteria, allowing banks to increase lending activities and money creation

In a free market for money, the exact amount of savings equals the exact amount of loanable funds available to borrowers for the production of capital goods. This is why the availability of capital goods, as we saw with Harold and Louis, is inexorably linked to a reduction in consumption. Again, scarcity is the starting point of all economics, and its most important implication is the notion that all decisions involve tradeoffs.

In the free market for money, the opportunity cost of saving is foregone consumption, and the opportunity cost of consumption is foregone saving — an indisputable economic reality.

No amount of centralized planning can alter this fundamental economic reality. This is why centrally planned markets always suffer from distortions (aka bubbles, surpluses or shortages) as political agendas run up against the underlying free market forces. Undeterred, central banks continually attempt to "manage" these market forces to achieve politically established policy goals. Most often, central banks are trying to spur economic growth and consumption, so they will increase the supply of loanable funds and lower the interest rate. With the price of loanable funds (the interest rate) artificially suppressed, producers take on more debt to start projects than there are savings to finance these projects. These artificially low interest rates don't provide any benefit to the economy, rather they simply disseminate distorted price signals that encourage producers to embark on projects which cannot realistically be financed from actual savings. This creates a market distortion (in other words, blows up another bubble) in which the value of consumption deferred is less than the value of the savings borrowed. This distortion can persist for some time but will inevitably unwind with disastrous consequences as economic reality cannot be fooled for long.

The excess supply of loanable funds, backed by no actual deferred consumption, initially encourages producers to borrow as they believe the funds will allow them to buy all the capital goods necessary for their project to succeed. As more producers borrow and bid for the same amount of capital goods, inflation sets in and prices begin to rise. At this point, the market manipulation is exposed since the projects become unprofitable after the rise in capital good prices (due to inflation) and suddenly begin to fail. Projects like these would not have been undertaken in the first place absent the distortions in the market for money created by central banks. An economy-wide simultaneous failure of overextended projects like this is called a *recession* . The boom and bust *business cycle* we have all grown accustomed to in the modern economy is an inevitable consequence of this centrally planned market

manipulation. The United States and Europe saw a great illustration of this process when the dot-com bubble of the late 1990s was replaced by the housing bubble of the mid-2000s.

Free market capitalism cannot function without a free market for money.

As with all well-functioning markets, the price of money must emerge through the natural interactions of supply and demand. Healthy markets require functional nervous systems, as market participants must have accurate price signals to make decisions effectively. Basic economics shows us clearly that central bank meddling in the market for money is the root cause of all recessions and the business cycle. By imposing an artificial price, in this case the interest rate on loanable funds, central banks inhibit natural price signals which coordinate allocation decisions among savers and borrowers. Their market manipulation creates market distortions and recessions. Attempting to remedy a recession by injecting more artificial liquidity into the system will only exacerbate the distortions which caused the crisis in the first place and blow up new bubbles. Only central planning of a soft money supply and its pricing mechanism can cause widespread failures in an economy like this, as an economy based on hard money remains firmly rooted in economic reality and resists market distortions.

Alignment with natural market forces like supply, demand and the price signal is the principal reason free market capitalism prevailed over socialism.

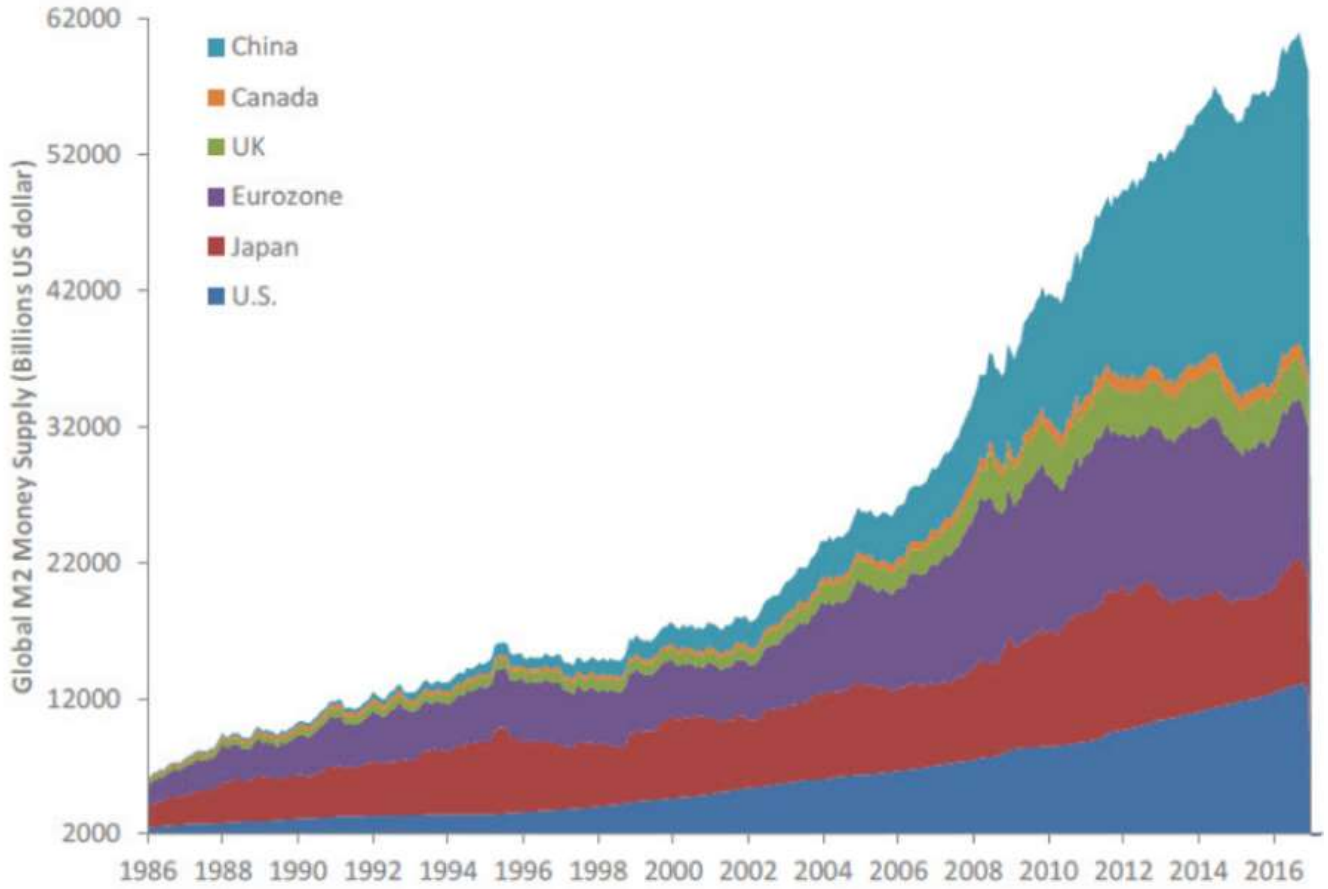
Failure of Government Fiat Money [1,3,4]

Seeing that governments have been forced to use coercive measures, such as confiscating gold and implementing legal tender laws, to enforce adoption of fiat money is a clear indication that soft money is inferior and doomed to fail in a free market. This severe inadequacy of government fiat money came to the forefront of global consciousness in the wake of the Great Recession that began in 2008. Due to gigantic market distortions driven by artificially low interest rates and credit ratings agencies with no skin in the game, US subprime real estate became the largest bubble in modern history. When it bursts, its affects were globally systemic, and central banks all over the world (predictably) began increasing their money supplies in an attempt to reflate their broken economies.

Instead of calling it what really is, central banks now deceptively refer to the act of printing money as *quantitative easing*. As we have learned, increasing the money supply creates no real economic value, it only causes market distortions and furthers the misallocation of capital. Injecting liquidity into an economic system experiencing a recession only provides illusory, temporary relief. Printing money delays and exacerbates the inevitable correction, as economic reality cannot be deceived

forever. Despite economic reality, central bank market manipulation is worse than ever.

Here we show the amount of government fiat money printed by the largest economies of the world since 1986:



Money supply growth by global central banks is accelerated after each recession. This artificial liquidity only provides illusory relief and further distorts the market signals which caused the distortions in the first place.

It was in the depths of the Great Recession that an anonymous individual named Satoshi Nakamoto introduced the open-source software project called Bitcoin to an online group of cryptographers. Many attempts at creating a digital cash had been made over the previous twenty years but none had succeeded. Initially, few in the group took Bitcoin seriously. However, Nakamoto was eventually able to convince a few other cryptographers to join and the Bitcoin network was born.

After ten years of virtually perfect operation, the Bitcoin network has gone from $0 to $80B in value stored on its network and has cleared $1.38T in total transactions. It is clear that this monetary technology is now competing successfully in the marketplace and is being used by many for real world purposes.

Synthesized Works & Further Reading

- [1] *The Bitcoin Standard: The Decentralized Alternative to Central Banking* by Saifedean Ammous (a masterful work on which much of this essay is based)
- [2] *The Rational Optimist* by Matt Ridley
- [3] *Skin in the Game* by Nassim Nicholas Taleb
- [4] *The Bullish Case for Bitcoin* by Vijay Boyapati
- [5] *The Age of Cryptocurrency* by Paul Vigna and Michael J. Casey
- [6] *Sapiens* by Yuval Harari
- [7] *Bitcoin is a Decentralized Organism, Part 1 and Part 2* by Brandon Quittem
- [8] *PoW is Efficient* by Dan Held
- [9] *The Fifth Protocol* by Naval Ravikant
- [10] *Unpacking Bitcoin's Social Contract* by Hasu
- [11] *Antifragile* by Nassim Nicholas Taleb
- [12] *Letter to Jamie Dimon* by Adam Ludwin
- [13] *Placeholder VC Investment Thesis Summary* by Joel Monegro and Chris Burniske
- [14] *Diffusion of Innovations* by Everett M. Rogers
- [15] *Why America Can't Regulate Bitcoin* by Beautyon
- [16] *Hyperbitcoinization* by Daniel Krawisz

Money, Bitcoin and Time: 2 of 3

By Robert Breedlove

Posted January 26, 2019

This is part 2 of a 3 part series

- Money, Bitcoin and Time: 1 of 3
- Money, Bitcoin and Time: 2 of 3
- Money, Bitcoin and Time: 3 of 3

The Simple Truth about Bitcoin: Bitcoin is the hardest form of money ever invented. It has successfully brought the advantages of physical cash money into the digital realm. Bitcoin is changing the way people organize themselves. The next chapter in the story of money is being written in a new language...

Grasping Bitcoin [7]

Bitcoin seems easy to understand at first (it's just magic internet money, right?), however truly grasping its significance is a formidable task. Once you think you have Bitcoin figured out, you'll see it from another perspective and realize how little you actually knew. This pursuit of understanding Bitcoin is like a mountain climber that continually encounters false peaks, which fool him into thinking he has reached the summit, only to realize it is higher still.

It has been said that you can judge the quality and importance of an idea by the vehemence of its opposition. Bitcoin has been called many things—digital gold, tulip mania 2.0, financial revolution, the MySpace of cryptocurrencies, environmental disaster, rat poison squared, libertarian idealism, apex predator of monetary technologies, the biggest bubble in history, the model-T of cryptocurrencies, a superior species of money—but it turns out that, in context of the history and nature of money, Bitcoin appears to be a distinct evolutionary leap forward. Bitcoin is not an internet application like MySpace, it is an internet protocol. Bitcoin is not the model-T of cryptocurrencies, it is a more like a global freeway system. Bitcoin is not like any type of gold coin, Bitcoin is more like the element gold. Its integrity is protected by the inviolable laws of mathematics. Human nature is one of its core components. It is a new form of social institution. Bitcoin is a living system unto itself that adapts to environmental changes.

This may sound mind blowing at first. Most innovations of this magnitude sound this way in the beginning as we struggle to communicate using outdated terms and analogies that cannot possibly convey their importance. However, history shows us that ignoring innovation is a terrible strategy. In light of its inherent complexity and novelty, we will view Bitcoin from many different perspectives in an attempt to create a mosaic of understanding in the minds of our readers. First and foremost, Bitcoin is *digital cash money* .

Digital Cash Money [1]

As the global economy becomes increasingly digitized and interconnected, new technological realities are taking shape which will cause the market to naturally select for the most effective species of money native to this new digital terrain. Bitcoin is the first truly digital solution to the problem of money. It is the world's first digital cash (in the original sense of the word cash discussed earlier) meaning that it is under the full control of its owner and can be used for final settlement in the same way as gold is today. Put another way, Bitcoin is digital cash money, a self-sovereign asset that contains within it all the trust factors and permissions necessary to transact with it. Bitcoin is not the liability of any counterparty, hence its nickname—digital gold.

Like gold, Bitcoin is a supranational form of money, meaning that no government needs to decree its value or permit its use, nor can it be eliminated unilaterally by regulation. The hardness of Bitcoin is superior to all forms of money, including gold, and its stock-to-flow ratio will eventually reach infinity. As a digital asset, Bitcoin has unprecedented levels of salability across scales, space and time. It is resistant to confiscation, censorship, inflation and counterfeit. Meritoriously, Bitcoin's value is attained entirely from the social consensus it earns by competing freely in the marketplace.

As one perspective of its monetary significance, Bitcoin can be understood as the successful fusion of the advantages associated with physical cash payments with the efficiencies and certainties enabled by digital technology. Cash payments have the advantage of being immediate, final and requiring no trust from either counterparty in each other nor any other intermediary. The drawback of cash payments was the need for parties to be present in the same space and time, which increases risks associated with physical custody, especially for larger transactions. As more business is conducted remotely, thanks to ever-advancing telecommunications technologies like the internet, physical cash transactions become increasingly impractical.

Since the inception of computers, the nature of all digital objects is that they were infinitely replicable. This meant that no digital object could be provably limited in quantity. For instance, when you "send" and email, you are actually sending a copy, as you still have the email in your sent folder. Before Bitcoin, there was no way to send a digital good that could not also be resent elsewhere at a later time. This presented an intractable issue for direct digital payments known as the *double-spend problem* . Without a trusted third-party intermediary to verify the payer was not double spending, digital payments were not possible. Using intermediated digital payments (like Venmo or PayPal) exposed parties to additional transaction costs, risk of censorship, fraud and transaction disputes.

The nature of digital objects also meant creating a digital cash was impossible, since its monetary units could be reproduced endlessly and would therefore suffer from unlimited inflation. Before Bitcoin, people had to rely on physical laws (rarity and chemistry, in the case of gold) or jurisdictional laws (government and central bank monopolies) to regulate money supplies. Innovatively, Bitcoin relies on mathematical laws to protect its monetary policy. Building on top of decades of innovative trial and error by other programmers and combining a wide range of proven technologies, Nakamoto successfully made Bitcoins the first digital objects that were verifiably scarce. As the world's first instance of *digital scarcity*, Bitcoin was able to solve the double-spend problem and become the world's first functional digital cash.

"That in order to make a person covet a thing, it is only necessary to make the thing difficult to attain." - Mark Twain

In this way, Bitcoin would bring the desirous advantages of physical cash to the digital realm and combine them with an immutable monetary policy to inoculate its holders from all unexpected inflation. Drawing on lessons learned by other programmers during two decades of attempts at this innovative breakthrough, Nakamoto finally achieved digital cash money by combining four key technologies:

- Proof-of-Work—mathematical puzzles which require energy expenditure to be solved, solutions are rewarded with newly issued Bitcoin and user transaction fees, functions as the skin in the game necessary to keep Bitcoin's distributed ledger truthful and maintain its monetary hardness
- Distributed peer-to-peer network—a record of Bitcoin's entire transaction history is maintained by each network participant (known as a node) who mathematically verify each other's work, making the entire system resistant to censorship and manipulation
- Hashing—a method of computer cryptography that transforms any stream of data into dataset of fixed size (known as a hash), this transformation is irreversible and is the foundation of trustless verification within the Bitcoin network
- Digital Signatures—a method of authentication that relies on a set of mathematically related elements called the private key, the public key and signatures—the private key (which must be kept secret) allows its holder to control the Bitcoin associated with it, meaning that the private key is a bearer instrument (holding Bitcoin is holding its private key, which makes it a self-sovereign monetary good like gold)

In the same way a monetary assessment of gold would not delve too deep into its chemical properties, this essay will not delve too deep into the technological properties of Bitcoin. We will instead focus on its monetary properties and its relevance in the story of money. However, some basic technical knowledge of Bitcoin

is warranted to fully appreciate the importance of the innovation that is digital cash money.

Technological Properties [1]

Bitcoin is *open-source software*, meaning its source code can be inspected by anyone. This makes Bitcoin a language, its source code and transaction history are universally transparent and can even be printed onto paper (interestingly, this makes it protected under the First Amendment in the United States, more on this later). As an open-source software project, Bitcoin is supported by a global network of volunteer programmers. These programmers are self-interested in the sense that they are almost always Bitcoin owners as they are aligned with its purpose philosophically, and therefore stand to gain financially from its expanding network. Their work over the years has greatly enhanced the functionality of the Bitcoin network. However, these programmers are unable to change the rules of Bitcoin (as we will see when we discuss Bitcoin's social contract).

To become a Bitcoin network member, known as a *node*, all that is necessary is to download and run the software on a computer. Once downloaded, the software will enable you to store Bitcoin and transact it with any other node in the world. Also, by becoming a node, the entire Bitcoin transaction history will be recorded on your machine and updated in perpetuity, just as it is on every other node in the world. This is the essence of Bitcoin's *decentralized architecture* . The Bitcoin network, similar to the internet, lives *everywhere and nowhere* .

Owning a Bitcoin means owning the private key that can authorize it to be used in a transaction. The private key is purely informational, meaning that it is just a string of alphanumeric characters. This makes it a self-sovereign form of money, giving its holder the presumption of rightful ownership, which makes Bitcoin an instrument of final settlement (like gold). Bitcoin is the world's first global, digital final settlement system.

Bitcoin is entirely reliant on verification, which allows its users to completely eliminate any need for trust. All Bitcoin transactions are recorded by every node on the network so that they all share one common ledger of balances and transactions (remarkably similar to the Rai Stone system used by the Yap Islanders). Transactions are grouped together approximately every ten minutes in what is known as a *block* . Each block is then added to the previous block of transactions, forming a chronological chain of inextricably linked blocks that stretches all the way back to the genesis block mined by Nakamoto himself exactly 10 years ago today. This is commonly called the Bitcoin *blockchain* . The blockchain is the common ledger of which each node maintains its own copy (commonly known as the distributed ledger). Each node verifies the accuracy of every other node's transaction inputs and

truth is established by consensus. In this way, the Bitcoin network relies 100% on verification and 0% on trust. This gives Bitcoin the unique property of *trustlessness*, meaning it is able to operate successfully without the need to trust any counterparty or intermediary whatsoever.

Blockchain, Energy and Mining [1,3,8,11]

Economic incentives and disincentives are used to maintain truthful records in the blockchain, it what is an ingenious application of the skin in the game concept. Nodes compete to solve complex mathematical puzzles in a process called *proof-of-work* . Nodes are incentivized to perform this computing task because the first one to solve the proof-of-work is awarded a batch of newly issued Bitcoin and the transaction fees generated within the latest block of transactions—called the *block reward* . A block is sealed approximately every ten minutes, which triggers the opening of the next block and proof-of-work competition. Nodes expend processing power (in the form of electricity) to solve these complicated mathematical problems, although considerably less and much more efficiently than the systems that support gold and government money today:

	Annual Cost ($USD)	Energy Consumption (GJ)	$USD per GJ
Gold Mining	$ 105,000,000,000	475,000,000	$ 221
Gold Recycling	$ 40,000,000,000	25,000,000	$ 1,600
Government Fiat Money Production	$ 28,000,000,000	39,000,000	$ 718
Banking System	$ 1,870,000,000,000	2,340,000,000	$ 799
Governments	$ 27,600,000,000,000	5,861,000,000	$ 4,709
Bitcoin Mining	$ 4,500,000,000	183,000,000	$ 25

Bitcoin mining is exceptionally energy efficient relative to other monetary systems and their institutions.

Proof-of-work energy expenditure is the thermodynamic bridge from the physical to the digital world. It transmutes the fundamental commodity of the universe, energy, into digital gold. This energy expenditure is essential to the functioning of the Bitcoin network, as it disincentivizes node dishonesty. If a node attempted to include a fraudulent transaction in a block, other nodes would reject it and it would incur the cost of processing power without the prospect of earning the block reward. This process is commonly referred to as *mining* and the competing nodes are called miners (or mining nodes). Mining is a truly capitalistic voting mechanism where energy expended equals hashes, which are votes for the proof-of-work solution, generated. The name mining is an ode to the arduous process of mining of gold. As we have learned, the costs and risks related to the mining of this monetary metal is necessary for it to maintain its hardness (skin in the game). Similarly, mining using proof-of-work is the only known method of creating digital cash money.

Money, which is the representation of the work required to generate goods, can also be considered a form of stored energy. In the early 20th century, free market proponents like Henry Ford and Thomas Edison were interested in replacing gold or the US dollar with an energy money. Showing great prescience, they foresaw the day when the world may exhaust its non-renewable energy sources and be forced to switch to alternatives. Convicted in their free market beliefs, they shared this idea and assumed a great deal of reputational risk in the process, as their views ran contrary to the established economic order. The concept of energy money was popular due to its hard money characteristics, as energy is costly to produce. However, energy money was technologically well before its time, as energy could not be transmitted or stored easily using technologies of the day. In championing a novel idea with the greater good at heart, Ford and Edison were exhibiting *soul in the game*, or the exposure to downside risks on behalf of others. As Edison said in 1931:

"I'd put my money on the sun and solar energy. What a source of power! I hope we don't have to wait until oil and coal run out before we tackle that."

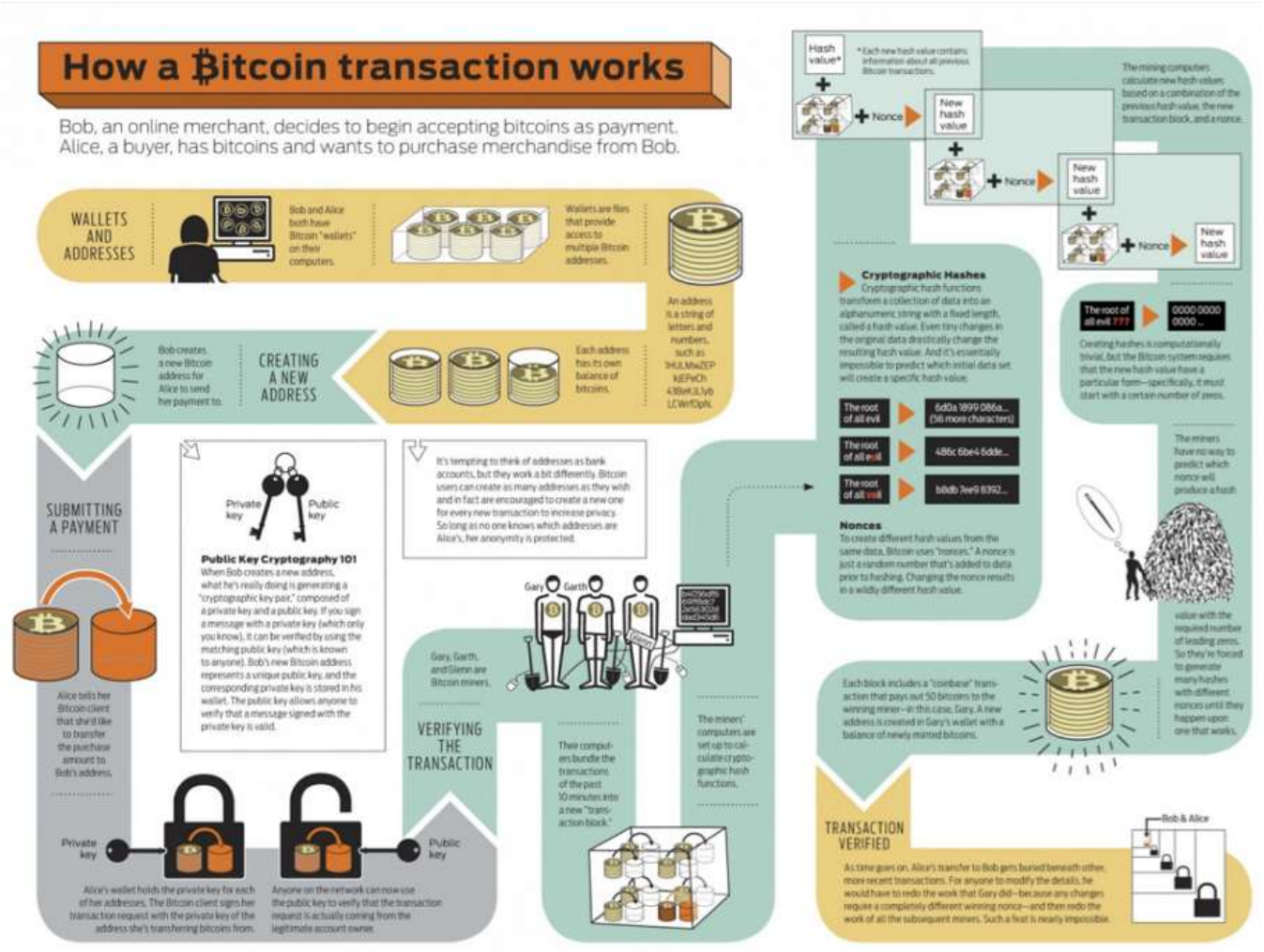
By using proof-of-work, which was originally invented as a measure to mitigate email spam, Bitcoin became the world's first functional energy money. With physical monetary goods, we were required to build walls to safeguard our money. With the Bitcoin network, we are required to expend energy to preserve the sanctity of its ledger, secure its network and enforce the immutability of its money supply. Proof-of-work is essential for Bitcoin to function as hard, digital cash money and enables it to serve as the buyer of last resort for electricity worldwide. The Bitcoin network provides a perpetual economic incentive for everyone in the world to invent more efficient methods of harnessing energy. This global incentive will increase the rate of innovation in energy technologies. As Bitcoin expert Nic Carter puts it:

"The Bitcoin network is a global energy net that liberates stranded assets and makes new ones viable. Imagine a 3D topographic map of the world with cheap energy hotspots being lower and expensive energy being higher. I imagine Bitcoin mining being akin to a glass of water poured over the surface, settling in the nooks and crannies, and smoothing it out."

As more nodes compete to solve the proof-of-work puzzle, the difficulty automatically increases so that new blocks are added on average once every ten minutes. This automatic algorithmic change is called the *difficulty adjustment* and is perhaps the most ingenious aspect of Bitcoin. It is the most reliable engineering solution for making and keeping money maximally hard and gives Bitcoin the unique ability to adapt its network security as it grows. As we have seen, when a form of money appreciates, people are immediately incentivized to increase its new supply flow, which reduces its stock-to-flow ratio and compromises its hardness. With Bitcoin, an increase in its price does not lead to the production of more Bitcoin

beyond its transparent and predictable supply schedule. Instead, it simply leads to an increase in processing power committed by miners which in turn makes the network more secure and difficult to compromise. Like a vault that becomes harder to crack the more money that is stored within it, Bitcoin offers people an incredibly effective means of value storage.

Next, we depict the entire process of a Bitcoin transaction:



How a bitcoin transaction works

The Internet of Value [9]

"The internet of value" is a popular moniker to describe Bitcoin. In reality, the Bitcoin *protocol* can be considered an integral and newly evolved layer of the commercial internet. In computer science, a protocol is a ruleset that governs the transmission of data. The internet as we know it is an integration of four successive layers of open-source protocols, called the Internet Protocol Suite, that maintain constant communication with one another:

- The Link Layer puts data packets on the wire
- The Internet Layer routes data packets across networks
- The Transport Layer persists communication across any given conversation
- The Application Layer delivers software files and applications

In this context, Bitcoin can be considered the fifth layer of the internet protocol suite:

- The Value Layer allocates scarce resources across networks

In the same way the internet is a set of open-source protocols for exchanging data, Bitcoin is an open-source protocol for exchanging value. It is trustless, as any machine can accept it from any other securely and at virtually zero cost. Bitcoin is also global and *permissionless*, meaning that any machine can speak its language and no central bank is required to authorize its use. This means that transactions on its network are essentially unstoppable as all trust factors and permissions necessary to transact with it are intrinsic to the act of holding a Bitcoin private key. Software protocol developments are being implemented that will make Bitcoin transactions even faster, cheaper, anonymous and capable of authentication. These can expand the utility of Bitcoin to enable the allocation of scarce network resources like computing power, verification of contracts or tracking identity and reputation.

Although Bitcoin is the fifth layer of the internet protocol suite, it is the base layer protocol for the value layer itself. This means that second and other higher order protocol layers may be built on top of it. A second layer protocol to Bitcoin, called the Lightning Network, is currently being implemented and is designed to sacrifice some degree of trustlessness to achieve higher transaction throughput, allowing Bitcoin to be used more effectively as a medium of exchange. The Lightning Network is an open-source protocol and functions by establishing trust channels among parties for faster, cheaper transactions that are then settled periodically to the Bitcoin blockchain. Higher order protocol development and integration is one of the many ways Bitcoin adapts to changes in its environment (more on this later).

In the same way that money is an emergent property of complex human interactions, Bitcoin is an emergent property of complex interactions occurring between people, machines and markets. Even if Nakamoto and Bitcoin never existed, it would still be necessary for us to invent the concept of cryptoassets to enable machines to exchange value to facilitate digital economies, use smart contracts and provide the substrate necessary for the 'internet of things' to come into existence. Not only is Bitcoin a prerequisite innovation to the digital economy, it is also the hardest monetary technology ever invented.

The Infinite Hardness of Bitcoin [1]

Bitcoin is the hardest form of money in existence. Its money supply is enforced mathematically and, like the other rules of Bitcoin, cannot be broken or changed. Only 21 million Bitcoins can and will ever exist:

$$\frac{\sum_{i=0}^{32} 210000 \left\lfloor \frac{50*10^8}{2^i} \right\rfloor}{10^8}$$

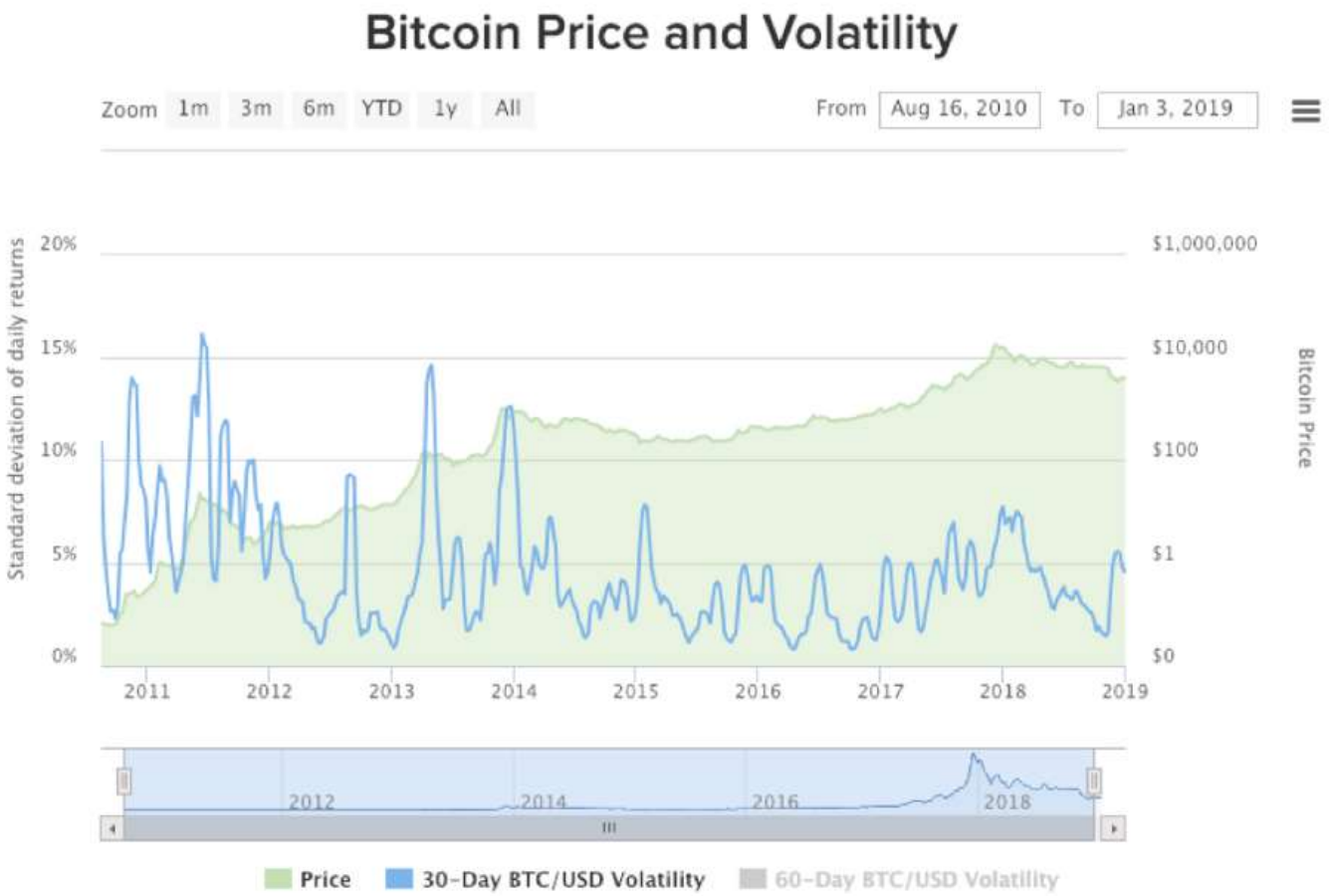
The monetary policy of Bitcoin is set in (mathematical) stone.

This strictly limited supply makes it the first monetary technology exhibiting *absolute scarcity* . Unlike gold and other monetary metals, no matter how much demand for Bitcoin increases there will never be any units produced in excess of its fully transparent, predictable and unchangeable monetary policy.

Before Bitcoin, only time itself had achieved the property of absolute scarcity.

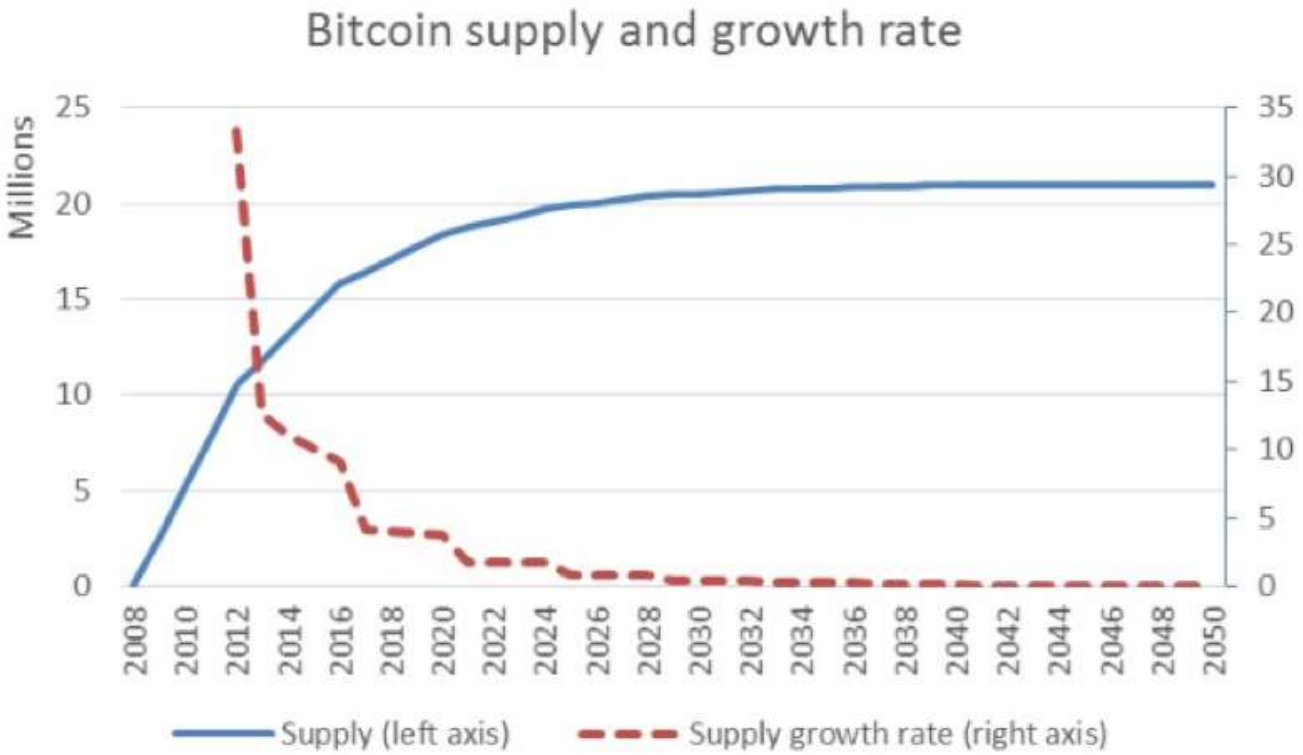
Since increased demand for Bitcoin cannot affect its supply, it can only be expressed in its price. Bitcoin has perfect *price inelasticity of supply*, meaning that it has zero supply-side response to increases in its price. Unlike gold and all other physical commodities, where an increase in demand will inevitably lead to larger supplies being produced over time, Bitcoin can only express an increase in demand by becoming more expensive (and a more secure network). A perfect price inelasticity of supply no doubt contributes to the notorious price volatility of Bitcoin it is exhibiting at the earliest stages of its growth we are witnessing today.

Absolute scarcity greatly exacerbates Bitcoin's price volatility. As its network continues to grow, the value of Bitcoin as an unstoppable payments channel and uninflatable money is steadily increasing over time while its price is constantly attempting to find it, dramatically overshooting and undershooting along the way. With a totally inflexible supply schedule, as long as Bitcoin is growing quickly, its price will behave like that of a startup company stock undergoing meteoric growth. Should Bitcoin achieve sufficient market penetration that its growth slows down, it would stop attracting high-risk investment flows and become a stable monetary asset expected to appreciate slightly each year as demand increases due to productivity and population growth—like any mature hard money should. As expected, over the long-run we are already seeing a decrease in Bitcoin's price volatility:



As expected, the price volatility of Bitcoin is gradually declining as its network value grows.

Bitcoin's immutable monetary policy ensures that its supply will continue to grow at a decreasing rate and will reach its maximum of 21 million units sometime in the year 2140. To maintain salability across scales, Nakamoto designed each Bitcoin to be further divisible into 100 million units, which are now commonly called Satoshis in his honor. Once the last Bitcoin is mined, its stock-to-flow ratio will become infinite as its flow will completely and irreversibly cease. Beyond this point, miners will be compensated exclusively by transaction fees. Bitcoin's decreasing growth rate means that the first 20 million coins will be mined by the year 2025, leaving the last 1 million to be mined over the subsequent 115 years:

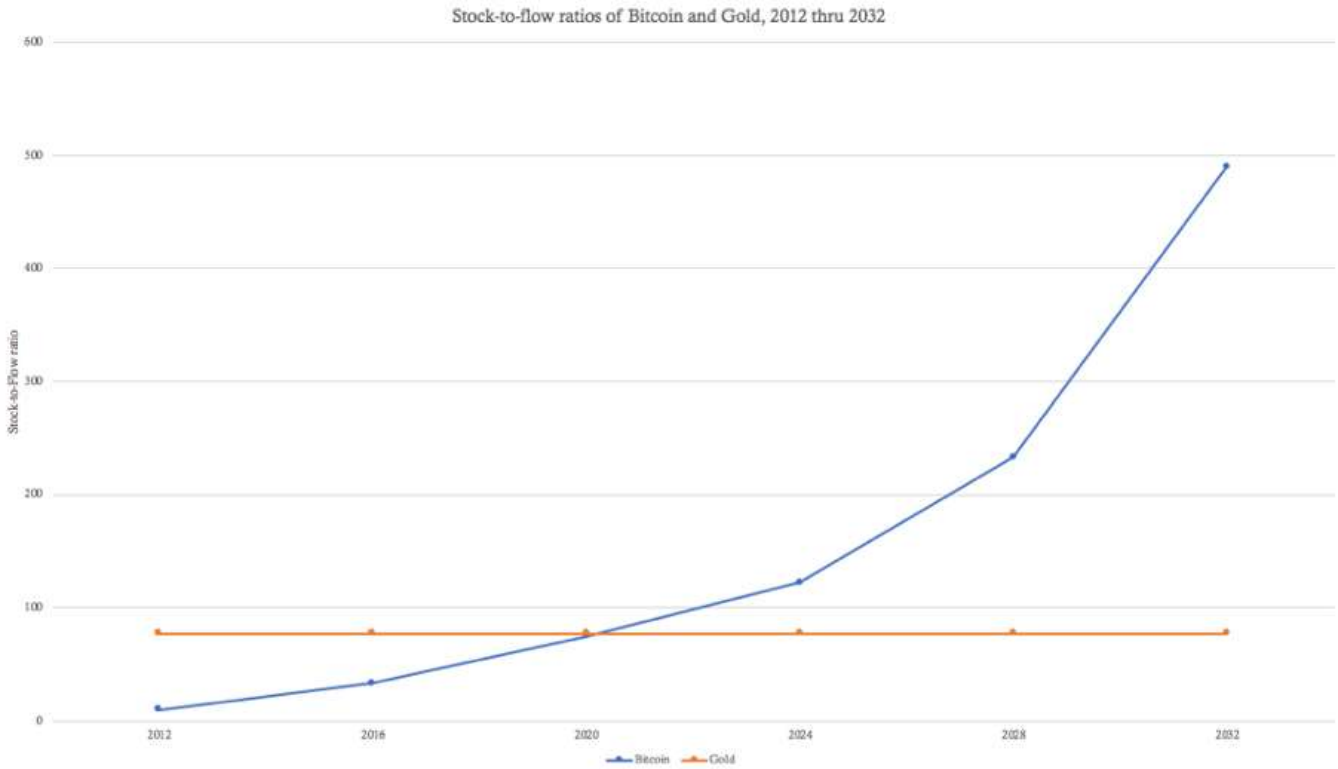


Due to its decreasing supply growth rate, over 95% of all Bitcoins will be mined by the year 2025.

This predictable, transparent and immutable supply schedule gives Bitcoin a significant advantage as it competes for the trust of the people to become a reliable store of value. Unlike government money or even gold, people know with absolute certainty that Bitcoin will never have its salability across time compromised by unexpected supply increases.

Bitcoin is uninflatable money in a world where wealth is continuously stolen via inflation.

As is the case with its other immutable laws, Bitcoin's monetary policy is enforced by the inviolable laws of mathematics. Inevitably, Bitcoin will surpass gold around the year 2020 to become the hardest form of money in history:



As sure as 1+1=2, Bitcoin will soon surpass gold to become the hardest form of money in history.

By virtue of its natively digital nature, Bitcoin is (critically) highly resistant to centralization. As we have learned, it was the centralization of gold that led to government money backed by gold, which made gold more salable across scales and encouraged a gold standard to flourish throughout most of the world. However, as the temptation to expand money supplies seems to be irresistible for humans, governments soon took control of the banking sector, printed money in excess of its gold reserves, eventually severed their currencies peg to gold and thereby destroyed the hardness of government money completely.

Historically, people who adopted hard money systems flourished—such as the Romans under Caesar, The Byzantines under Constantine and the Europeans under the gold standard—and people who had the hardness of their money compromised suffered enormous consequences—such as the Yap Islanders, West Africans using glass beads and the Chinese under a silver standard in the 19th century. Moving a society away from a hard money system has been a harbinger of economic crisis and societal decay, an outcome that can be explained as a social contract rescission.

Bitcoin's Social Contract [10]

Social contract theory starts with an assumed hypothetical state of nature full of violence that is unbearable for people to live in. Driven by a desire to improve their

circumstances, people come together and collectively agree to sacrifice some of their freedoms to establish a *social contract* and empower an institution to protect them. Government is the result of a social contract: people sacrifice some of their freedoms to give the state control over the monetary system and armed forces. The state, in turn, uses that power to manage the economy, redistribute wealth and fight crime. In the United States, our current social contract grants the government monopoly control of money (via the Federal Reserve) and violence (via the Police and Military).

Similarly, money itself can be thought of as a social contract. If enough people are unhappy with a barter economy, they can collectively agree to use money instead. This social contract entails sacrificing certainty (requiring trust that dollars will maintain their value over time) in exchange for convenience (using dollars as a medium of exchange). The social contract for money, as we have seen, emerges and evolves spontaneously based on market-driven natural selection. Each person continuously decides which outcomes they prefer and how best to achieve them. If enough people seek the same outcome, we call the result a social contract.

Throughout history, almost every government (a form of social contract) put in charge of the monetary system (another, often interrelated, form of social contract) has abused its power by forcibly confiscating assets, censoring private transactions and printing money to steal wealth via inflation. Using the virtually unlimited financial means provided by control over money supplies, these governmental social contracts grew in successive bureaucratic layers. The larger and more valuable these social contracts became; the more freedoms were forfeited and the more others sought control over them. This led to many instances of conflict (warfare or social revolution) in which old social contracts (dictatorships or tyrannical regimes) were rescinded in favor of new ones (new laws, treaties or governments). The principal point here is that people can agree they are in a terrible situation and come together to change it, but the resultant social contract is only as strong as its credibility and enforceability.

The invention of Bitcoin can be regarded as a new implementation of the social contract for money. Nakamoto settled on the following rules for this new implementation:

- Only the owner of a Bitcoin can produce the digital signature to spend it (confiscation resistance)
- Anyone can transact and store value in Bitcoins without permission (censorship resistance)
- There will only be 21 million Bitcoins, issued on a predictable schedule (inflation resistance)
- Anyone will always be able to verify all the rules of Bitcoin (counterfeit resistance)

Historically, social contracts intended to protect people, such as governments and their central banks, eventually became controlling and ultimately turned abusive. When a social contract loses sufficient trust of the people, it falls apart or is overthrown, by ballot or by bullet. This dynamic has resulted in a continuous cycle of rising and falling social contracts throughout history. Bitcoin is intended to break this cycle in two ways:

- Instead of seeking security from a powerful central entity (like a government or central bank) that can be corrupted or overthrown, Bitcoin creates a hypercompetitive market for its own protection. It turns security into a commodity and the security providers (miners) into harmless commodity producers.
- By requiring its security market participants (miners) to incur real world costs to generate their economic reward (skin in the game), Bitcoin incentivizes the market to reach consensus over who owns what at any given point in time.

In this sense, the Bitcoin social contract is composed of two distinct, self-reinforcing layers: the social layer and the protocol layer. The social layer is the social consensus itself, which determines the rules of Bitcoin and establishes its value. The protocol layer simply automates the enforcement of the rules set by the social layer:

In this sense, Bitcoin is more than just a technology. Indeed, it is a new institutional form. Viewing it in this way, we are better able to answer some of the more existential questions about Bitcoin:

Who Can Change the Rules of Bitcoin?

Since the rules of the Bitcoin social contract are decided at its social layer and enforced at its protocol layer, who can actually change its rules? Bitcoin, as computer

network, comes into existence when people run implementations that follow the same ruleset (think of these rulesets as speaking the same language). You remain in the network by following the same rules as everyone else. If you decided to change the ruleset on your local computer, you would simply be evicted from the network (you no longer speak the same language as everyone else). Your unilateral decision to change the rules would not impact the actual Bitcoin network in any way whatsoever.

The only way to change the rules of the Bitcoin social contract is to convince people to voluntarily accept your proposed rule changes at the social layer. As each network member is self-interested, they will only adopt rules that benefit them. Seeing as its current rules are already optimal for Bitcoin holders (resistance to confiscation, censorship, inflation and counterfeit) it would be extremely difficult to convince a majority of the approximately 30 million network participants to change rulesets. This asymmetrical governance dynamic virtually rules out any contentious changes from succeeding, as they would never get broad social consensus. Therefore, the Bitcoin network can be upgraded in ways that align with the collective best interests of its members and is at the same time highly resilient to changes that contradict these interests.

Can a Software Bug Kill Bitcoin?

In September 2018, a software bug arose in the main implementation of Bitcoin that opened up two potential attack vectors which theoretically could have been exploited to circumvent its counterfeit and inflation resistance properties. Bitcoin developers quickly fixed the bug before either vector was exploited, however this event left many people wondering what would have happened had the vulnerabilities not been discovered in time.

Any time the social layer and protocol layer diverge in the Bitcoin social contract, the protocol layer is always wrong. Again, all rules are set at the social layer whereas the protocol layer is only responsible for automating their enforcement. Had the software bug not been discovered in time, Bitcoin's blockchain would have undergone a *fork*—meaning its protocol layer would have been split it into two networks, one with the bug and one without it. Every Bitcoin holder would then have an equal number of coins in each network, but the value of these coins would be determined solely by the free market. This is true for all forms of money, as social consensus determines the value of money. At the social layer, each Bitcoin owner would then choose either the implementation with or without the bug. To protect the value of their Bitcoin, holders would rationally choose to migrate to the mended network and its blockchain would continue without interruption.

When the Bitcoin protocol layer successfully automates the enforcement of the rules determined at its social layer, the two layers are in sync. If they diverge for any reason, the social layer supersedes, and the protocol layer is mended to reflect the economic reality of the social consensus surrounding Bitcoin. Software bugs are inevitable, and Bitcoin's 2-layer social contract construction ensures that it can withstand them.

Can Forks Compromise the Immutability of Bitcoin's Rules?

Since Bitcoin is open-source software, anyone in the world can copy its code, change it and launch their own version. This is also a chain fork which, as established earlier, affects only the protocol layer of the Bitcoin social contract. Without changing the rules at the social layer first, a protocol layer fork only evicts you from the true Bitcoin network. To successfully change the rules of Bitcoin, you must successfully fork its social layer first. To accomplish this, you would need to convince as many people as possible that your proposed ruleset is meaningfully better for them, so that they take the risk of adopting your proposed software changes. Forks like these are difficult to pull off in reality because they require buy-in from thousands of people to be successful. This asymmetry between the cost of campaigning for ruleset changes and their potential benefit to network participants makes the Bitcoin network exhibit an extremely strong status quo bias when it comes to governance.

The key to understanding this is that the value of any form of money is purely a social construct or, in other words, is derived from social consensus. Individual Bitcoins, like US dollars or any other currency, receive their value exclusively from the shared belief of their users. Forking Bitcoin's protocol layer is worthless without forking the social layer from which it derives its value. In the rare cases that the social layer itself splits, as was the case with the Bitcoin Cash fork, the result is two weaker social contracts, each agreed upon by fewer people than before. The complete failure of the Bitcoin Cash fork (its price has declined from 0.21 to 0.04 Bitcoin over the past year) is yet another battle scar for Bitcoin that pays testament to its governance model and exemplifies the winner take all dynamics inherent to monetary competition.

So long as Bitcoin network participants continue to act in accordance with their own individual self-interest, the rules of Bitcoin (resistance to confiscation, censorship, inflation and counterfeit) are immutable and, therefore, as reliable as the laws of mathematics. It's clear from this perspective that Bitcoin is more than just a technological innovation. Although Bitcoin as a network and monetary technology is groundbreaking in many respects, its social contract implementation is revolutionary. Bitcoin is the first technology that incorporates human nature as one of its core moving parts.

In essence, by believing that mathematics and individual self-interest will persist, we can reliably believe in Bitcoin's value proposition and its ongoing successful operation.

Over the past 10 years, by inventively aligning human self-interest with its own self-interest, the Bitcoin network has managed to grow organically from $0 to $80B in value.

A New Form of Life [1]

Although Bitcoin is intended to be a monetary technology, it is a totally unique compared to other forms of money. Ralph Merkle, famous cryptographer and inventor of the Merkle tree data structure, has a remarkable way of describing Bitcoin:

"Bitcoin is the first example of a new form of life. It lives and breathes on the internet. It lives because it can pay people to keep it alive. It lives because it performs a useful service that people will pay it to perform. It lives because anyone, anywhere, can run a copy of its code. It lives because all the running copies are constantly talking to each other. It lives because if any one copy is corrupted it is discarded, quickly and without any fuss or muss. It lives because it is radically transparent: anyone can see its code and see exactly what it does. It can't be changed. It can't be argued with. It can't be tampered with. It can't be corrupted. It can't be stopped. It can't even be interrupted. If nuclear war destroyed half of our planet, it would continue to live, uncorrupted. It would continue to offer its services. It would continue to pay people to keep it alive. The only way to shut it down is to kill every server that hosts it. Which is hard, because a lot of servers host it, in a lot of countries, and a lot of people want to use it. Realistically, the only way to kill it is to make the service it offers so useless and obsolete that no one wants to use it. So obsolete that no one wants to pay for it, no one wants to host it. Then it will have no money to pay anyone. Then it will starve to death. But as long as there are people who want to use it, it's very hard to kill, or corrupt, or stop, or interrupt."

Bitcoin is a technology, like the hammer or the wheel, that survives for the same reason any other technology survives: it provides benefits to those who use it. It can be understood as a spontaneously emergent protocol that serves as a new form of uninflatable money and an unstoppable payments channel. Structurally, the Bitcoin network reflects a quintessential manifestation commonly found in nature.

The Decentralized Network Archetype [7]

The Bitcoin network mirrors one of the most successful evolutionary structures found in nature, the *decentralized network archetype*:

Clockwise from the top left: the human heart, lightning, the human brain, a fungal mycelium network, roots from a tree, an aerial view of the Grand Canyon, branches from a tree and a cosmic web of galactic superclusters in the deep Universe (which is the largest observable structure in the known Universe at over 1 billion lightyears across).

The decentralized network archetype is prevalent in nature because it is one of the most energy efficient structures possible. Energy is the fundamental commodity of the universe and nature always optimizes for its utilization. Atoms, bubbles and stars (in a state of equilibrium) always form spherical shapes, which is the most energy efficient form for minimizing surface area, precisely because they are energy conservation structures. Minimal surface area output per unit of energy input ensures that these structures optimally expend the finite energy of which they are composed. Spheres are figures of equilibrium with equal distribution their own inherent energy.

Conversely, decentralized networks always form in these tendrilled, circuitous and redundant shapes, which is the most energy efficient form of maximizing surface area, precisely because they are energy exchange structures. Maximal surface area output per unit of energy input ensures that these structures achieve the highest degree of spatial exposure to optimize the likelihood of successful exchange—whether their purpose is pumping blood, imbibing groundwater or seeking sunlight. Spheres and decentralized networks are antithetical in purpose and archetype. Decentralized networks are figures of disequilibrium which both disperse and gather energy within their environments. A decentralized form in organic systems confers advantages such as distributed intelligence, invulnerability to singular attack vectors and accelerated adaptivity.

The decentralized network archetype found in nature is the antecedent to paradigm shifting innovations throughout history such as the railroad system, the telegraph, the telephone, the power distribution grid, the internet, social media and now Bitcoin.

To illustrate the power of this natural archetype, let's consider the story behind the design of the Tokyo subway system. Scientists conducted an experiment where an ancient fungus, the slime mold, was incentivized to recreate the Tokyo subway system. Each subway stop (node) was marked with oat flakes, the favorite food of the slime mold. In a single day, the slime mold grew to connect all the subway stops in a more energetically efficient design than that proposed by the central planning committee of engineers who spent many months at great expense to the Japanese government in the design process:

Japanese subway design

As the Scientists later reported:

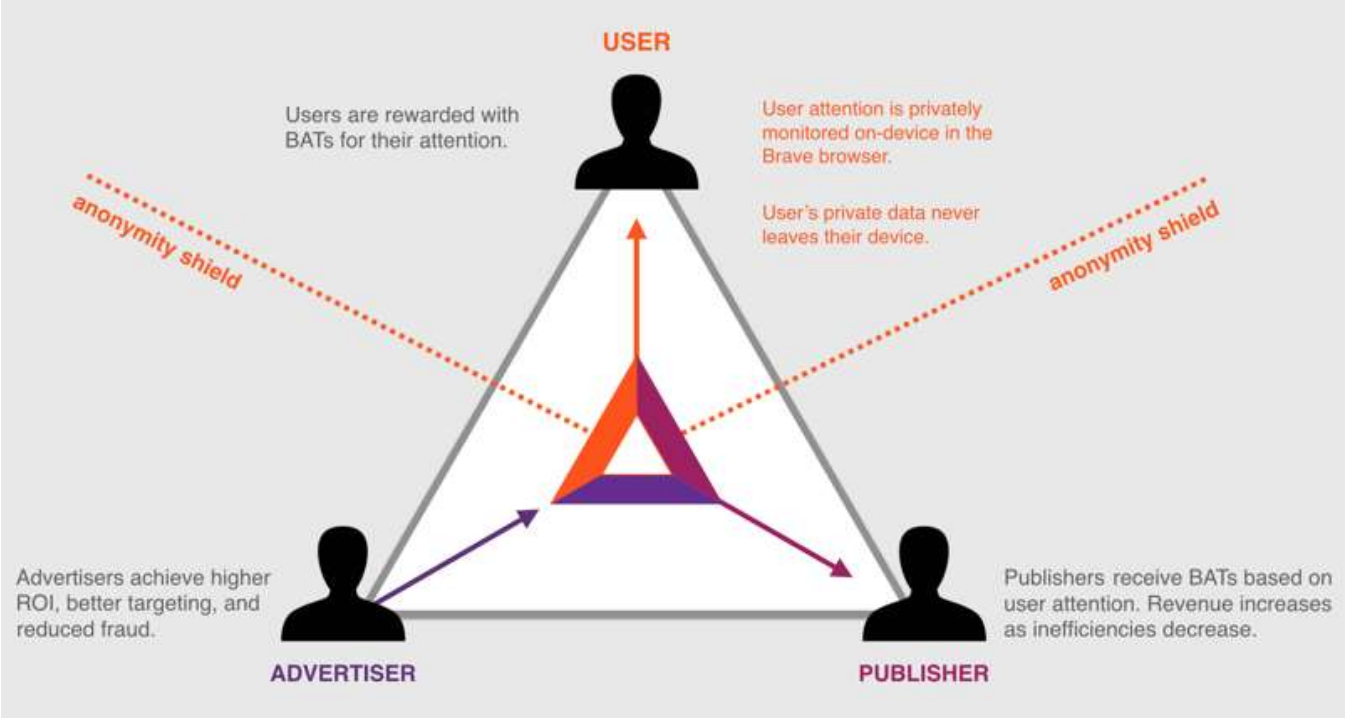
"Transport networks are ubiquitous in both social and biological systems. **Robust network performance involves a complex trade-off involving cost, transport efficiency, and fault tolerance. Biological networks have been honed by many cycles of evolutionary selection pressure and are likely to yield reasonable solutions to such combinatorial optimization problems. Furthermore, they develop without centralized control and may represent a readily scalable solution for growing networks in general.** We show that the slime mold Physarum polycephalum forms networks with comparable efficiency, fault tolerance, and cost to those of real-world infrastructure networks—in this case, the Tokyo rail system. The core mechanisms needed for adaptive network formation can be captured in a biologically inspired mathematical model that may be useful to guide network construction in other domains."

In a similar vein, Bitcoin and its network participants receive signals from the market to create features that satisfy unmet demands or improve the functionality of its network. When block space demand exceeds capacity, as it did it late 2017, transaction fees spike and encouraged the development of a second layer protocol to increase transaction throughout (the Lightning network discussed earlier). As rent-seeking businesses, like Western Union, continue charging exorbitant fees for international remittances, market demand shifts to Bitcoin's much more cost effective and permissionless payment channel. When governments crack down on Bitcoin exchanges, trading volume on peer-to-peer exchanges like LocalBitcoins.com flourishes. To enhance Bitcoin network accessibility, Blockstream launches satellites that provide global coverage for node synchronization. The Bitcoin network is

constantly adapting to optimize for its own expansion and the interconnectedness of its participants. Perhaps Bitcoin is less so digital gold, and more so digital slime mold (just kidding, or am I?).

In most forms of life, genes are only passed from parent to offspring in a process called *vertical gene transfer* . Certain fungal networks, which are modeled after the decentralized network archetype, are able to steal competitive advantages directly from physical contact with other similar organisms in a process called *horizontal gene transfer* . These fungal networks can grow to gargantuan sizes—indeed, the largest organism on Earth, at nearly 4 kilometers across, is a honey fungus in Oregon that is slowly consuming an entire forest. Fungal networks live in constant competition as they fight off predators, pests and pollutants. This environmental stress causes them to naturally synthesize a variety of enzymatic and chemical countermeasures and, when one of these measures is successful, it is stored in the distributed mind of the entire fungal network. The next time it encounters a menace for which it has even once synthesized an effective countermeasure, the fungal network will use it to neutralize the threat, no matter where the latest encounter occurs. Amazingly, these fungal networks are capable of absorbing countermeasures created by competitors in the same ecosystem purely from physical contact. Such organisms exhibit distributed intelligence, meaning they learn at the edges and distribute the lessons throughout their vast networks.

There is a common misconception that an alternative cryptoasset could develop a superior feature that will eventually outcompete Bitcoin. Similar to certain fungal networks, Bitcoin is able to subsume features that have been proven in the marketplace from cryptoasset competitors. For example, an alternative cryptoasset called Basic Attention Token (BAT) is designed to power an internet browser called Brave that allows users to shield themselves from advertisements:



BAT is a cryptoasset designed to allow web browser users to monetize their own attention. Using a set of open-source software extensions, today you can perform browser-based microtransactions similar to BAT but using Bitcoin instead. This effectively eliminates the need for a cryptoasset like BAT. The capacity of Bitcoin to subsume market-proven features from competitive cryptoassets fortifies it from disruption.

Brave users are then given the option to open their browsing sessions up to advertisements and are paid in BAT for their attention. This blockchain-based digital advertising solution is intended to allow users to monetize their own attention, whereas in most browsers advertising revenues are allocated mostly to the content publishers. Given Bitcoin's open-source nature, it is able to absorb competitive features like this in a process similar to horizontal gene transfer. Today, by using the Lightning Joule browser extension and running a full Bitcoin node, you can perform browser-based microtransactions similar to BAT but using Bitcoin instead. This effectively eliminates the need for a cryptoasset like BAT. Further, the technologies combined to make Bitcoin all came from previous attempts at digital cash, reiterating the point that open-source software is amenable to feature absorption. This ability accelerates the adaptivity of the Bitcoin network and insulates it from competitive disruption which further reinforces its position as the market leader.

Antifragility [1,11]

Seeing the ubiquity of the decentralized network archetype throughout nature in this way makes the invention of decentralized digital money seem less novel and

more inevitable. An open and decentralized nature also enables Bitcoin to benefit from adversity. In light of its track record, Bitcoin is an excellent incarnation of Nassim Taleb's concept of *Antifragility*:

"Wind extinguishes a candle and energizes fire... 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. 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, the rise of cities, legal systems, equatorial forests, bacterial resistance... even our own existence as a species on this planet."

Fragility can be defined as sensitivity to disorder, whereas robustness is insensitivity to disorder. Antifragility is a property of anything that benefits from disorder, stress or adversity. The many failed attempts at killing Bitcoin thus far have only made it stronger by drawing attention to attack vectors or vulnerabilities that its global team of self-interested, volunteer programmers can then fix. These improvements have only increased the network's operational efficiency. Also, each time it withstands an external attack or a chain fork (as we are witnessing with the abject failure of Bitcoin Cash), its reputation for network security and immutability is strengthened. The resiliency of Bitcoin is hardened by hostility.

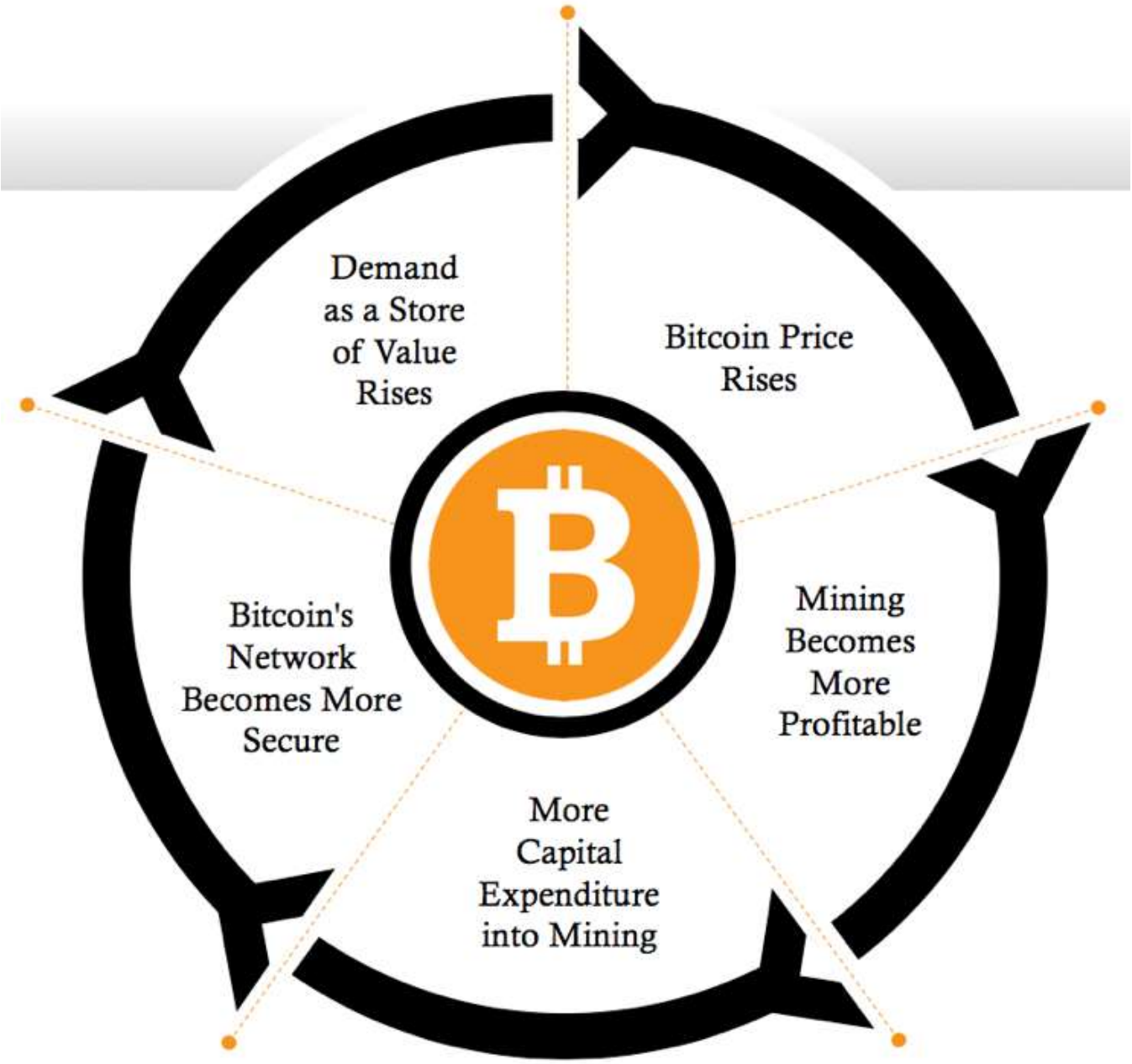
As Bitcoin has fluctuated wildly in price over the years, each new crash has triggered widespread declarations of its demise. Over 330 prominent articles declaring the death of Bitcoin, known as Bitcoin obituaries, have been written over the past 10 years. These publicity attacks on Bitcoin brought it to the attention of ever-wider audiences. As obituaries intensified, Bitcoin's network processing power, transaction volume and market capitalization all continued to ascend relentlessly—a confirmatory example of the saying 'all publicity is good publicity'.

When China took a heavy-handed approach to regulation by shutting down Bitcoin exchanges in 2017, we witnessed several informal exchanges and OTC markets appear following the demise of each centralized exchange. Although the liquidity for Bitcoin was negatively impacted initially, soon transactions started happening off exchange in China, with volume on websites like localbitcoins.com exploding. The regulatory attack also encouraged people to hold Bitcoin for longer periods, as evidenced by a steep decline in sell volumes, which only reduced the amount of Bitcoin being traded and put upward pressure on its price. Also, these regulatory actions backfired by triggering the *Streisand Effect*, which is a phenomenon whereby an attempt to hide, remove or censor information has the unintended consequence of publicizing the information more widely, usually facilitated by the

internet. As the world watched the situation in China unfold, both the Bitcoin price and global internet searches for the term Bitcoin reached new all-time highs.

Bitcoin's Positive Feedback Loop [1,4]

All of the adversity Bitcoin has faced so far has only fed its growth. Absent any top-down authority, Bitcoin is organic in the sense that it has grown from the bottom-up based solely on its own merits as money. Bitcoin perpetuates the expansion of its network and maintains truthful records by relying on asymmetric economic incentives that make fraud far costlier than its potential rewards. Network participants are all rewarded economically for their interactions with Bitcoin, which creates a flywheel effect on its price and network security:



Bitcoin autonomously proliferates its network by economically rewarding everyone who interacts with it.

As the Bitcoin network adapts to better meet the demands of its constituents, it in turn recruits more network participants. This positive feedback loop promotes the sustained growth of its network and fuels powerful, multi-sided network effects.

Bitcoin's Network Effects [1,4,5]

Bitcoin's meteoric growth has been both supported and protected by its unique multi-sided network effects. The basic example of a powerful 1-sided network effect

is a social network (or a telephone network, as outlined earlier). The more people on a social network, the more valuable it is for others to be on it, as there are exponentially more possible connections. It can, however, be disrupted by a competitor that provides a more valuable service to its single customer cohort, the users, who might then transition to the new service (as happened when Facebook disrupted MySpace).

Successful 2-sided markets (like eBay or Craigslist) are significantly more difficult to disrupt. Consumers want to be there because merchants are there, and merchants want to be there because consumers are there. To disrupt a 2-sided network, you have to simultaneously introduce a superior value proposition for both parties, otherwise nobody moves. That is why Craigslist, despite its limited innovation over the years, has been able to leverage its early 2-sided lead and is still a dominant website today.

Bitcoin has a unique 4-sided network effect that insulates it from disruption and supports its growth. These are the four constituencies that participate in expanding the value of Bitcoin as a result of their own self-interested interaction with its network:

- Consumers who pay with Bitcoin
- Merchants who accept Bitcoin
- Nodes that maintain the distributed ledger
- Developers and entrepreneurs who are building onto and on top of Bitcoin

This 4-sided network effect makes Bitcoin's first mover advantage seemingly indomitable. As an adaptive monetary technology, its network effects encompass the liquidity of its market, the number of network participants, the community of software developers who support it and Bitcoin's brand awareness. Large investors will always seek the most liquid market for ease of entry and exit. Consumers, merchants and developers tend to join the largest of each of their respective Bitcoin communities, which only reinforces their social interconnectivity and cohesion. Brand awareness is innately self-reinforcing, as any cryptoasset competitor will inevitably be mentioned in comparison to Bitcoin.

An aside on Bitcoin's brand awareness: As we have learned, the value of any money is derived from its social consensus, or the mutual beliefs of its users. The notion of a "believer" has religious connotations, as the notion of one having an epiphany once the "truth" is revealed. Such religious undertones are prevalent in most forms of money (In God We Trust on the US Dollar) and they are also part of Bitcoin's aura (The Genesis Block, Bitcoin Evangelists). The most important of these quasi-religious ideas is the mythological bedrock Nakamoto laid with his enigmatic appearance in 2008 and then with his mysterious disappearance 3 years later. Whoever he/she/they were, Nakamoto gave Bitcoin its *creation myth* . As market strategist Nicolas Colas said:

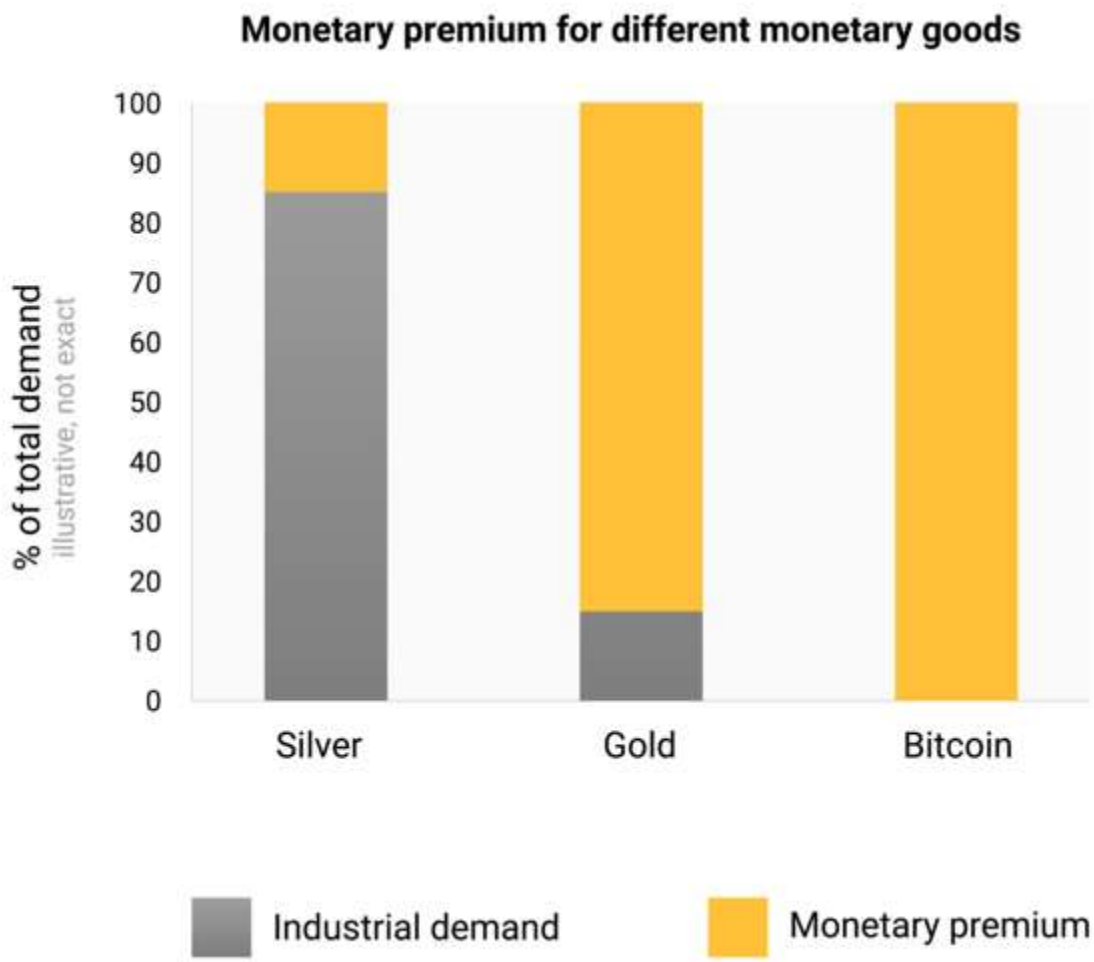
“In business, creation stories reinforce the role of the individual as a societal agent of change and speak to a core audience of customers. They are the bedrock for what marketers call a brand and the source waters for Wall Street’s shareholder value.”

Assuming Nakamoto was a lone wolf, it is arguable that his disappearance transformed him from a person into a mythological figure. This mystery fuels the brand awareness of Bitcoin and reinforces its quality of decentralization, as there is no single individual to vilify, denigrate or otherwise target in an attempt tarnish Bitcoin’s symbolism. Like a super hero with a secret identity, all we have is the icon of Nakamoto as a cryptic genius—the godhead of Bitcoin.

As we have learned, the value of a network is a reflection of the total number of possible connections it allows. Therefore, each new Bitcoin owner increases the value of the Bitcoin network, which benefits all existing owners. This new owner is then incentivized to evangelize the benefits of Bitcoin to others, creating the next wave of new owners, and the cycle continues. As the price increases, so too do the incentives to secure the network which draws in more capital expenditure from miners, making Bitcoin’s network effects even stronger and self-reinforcing as price appreciation reflexively energizes Bitcoin’s positive feedback loop outlined earlier.

Since money is a social network, the price of a monetary good is a reflection of how widely adopted it has become or is expected to become. The price of a monetary good in excess of its industrial demand is its *monetary premium* . This is the only rational basis for the common criticism that Bitcoin is a bubble, as it is purely a monetary technology and has no industrial demand whatsoever. However, this premium is the defining characteristic of all forms of money, as all monetary value is based on the optionality it gives its user for exchange across scales, space and time.

Actual bubbles occur when price exceeds fair value, such as the market distortions created by central bank monetary manipulation. However, some mistake monetary premia for bubbles since they cause prices of monetary goods to exceed their underlying industrial values. If monetary premia are bubbles, then money is the bubble that never pops. Paradoxically, in this sense a monetary technology can presently be both a bubble and significantly undervalued if it later achieves widespread adoption:



As a pure bred monetary technology, Bitcoin derives none of its value from alternative uses.

Although there is no established price pattern for a digital good that is becoming monetized, Bitcoin's price appears to follow a fractal (a recursive, self-similar shape) wave pattern of increasing magnitude commensurate with its level of user adoption. The volatility of this price pattern is exacerbated by Bitcoin's perfect price inelasticity of supply (as discussed earlier). Each iteration of the *fractal wave pattern* appears to match the standard shape of the *Gartner hype cycle*, which provides a graphical and conceptual representation of emerging technologies undergoing five phases of maturation:

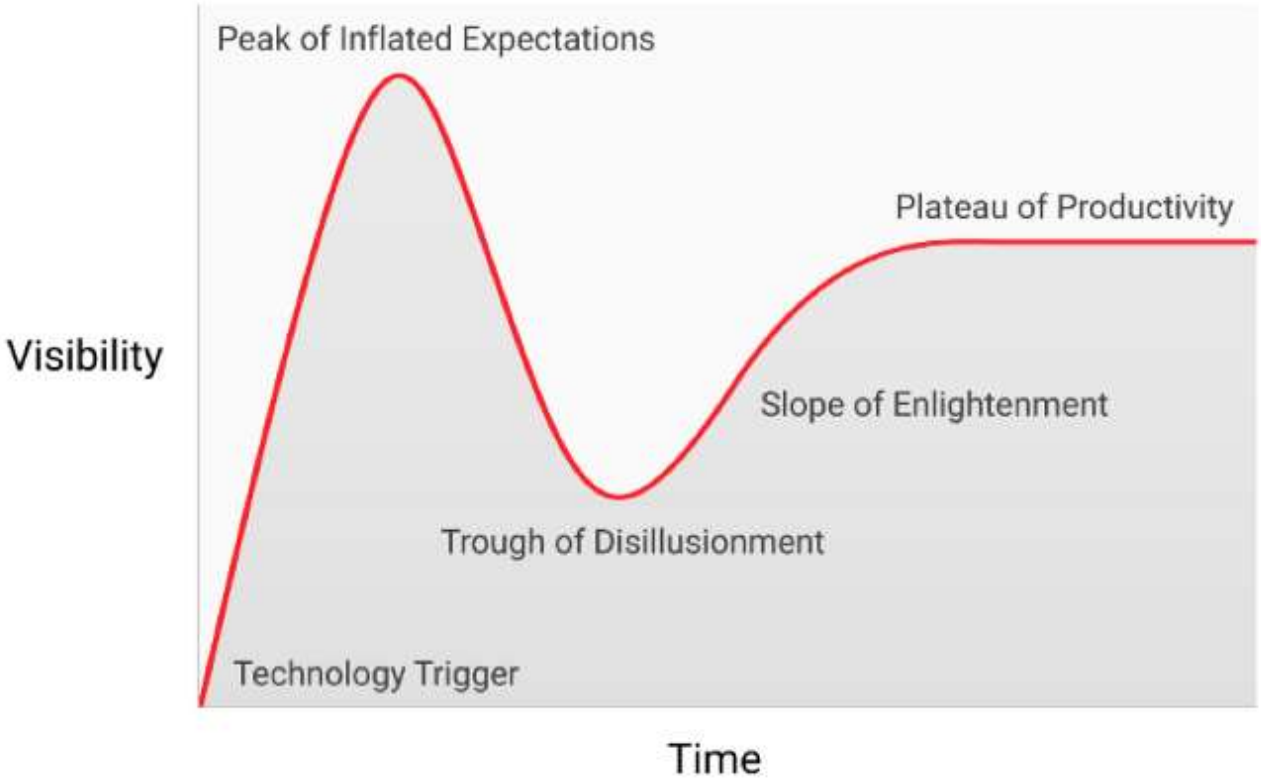


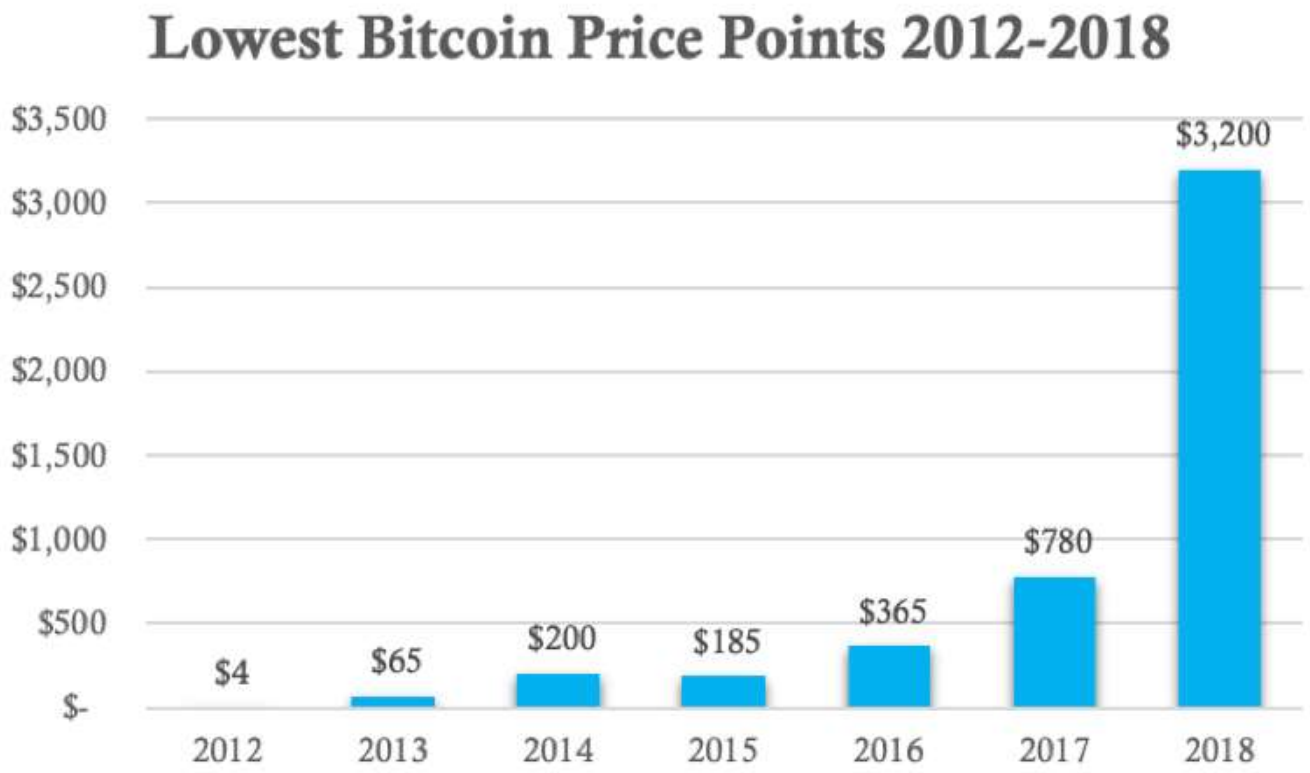
Figure 1 Bitcoin's price appears to follow a fractal wave pattern based on the archetypal Gartner hype cycle.

Bitcoin's growth, in terms of price and transactions, has been dramatic to say the least. Indeed, it is the fastest growing asset in history. Its price has gone from $0.000994 on October 5, 2009, in its first recorded transaction, to about $4,000 today—a total increase of over 400,000,000% in 10 years. By its 10th birthday, Bitcoin had processed about $1.38T USD worth of transactions, with USD value calculated at the time of each transaction. Here we show Bitcoin's entire price history, from a logarithmic perspective, with the Gartner hype cycle fractal wave pattern iterations located inside boxes:

Bitcoin is the fastest growing and most volatile asset in history, although both are leveling off as it grows.

These extreme price cycles draw in new Bitcoin owners as each fractal wave crests. Some of these new owners buy in near the peak, only to be crushed in the trough. Most will capitulate, but those who remain because of their long-term conviction in Bitcoin (typically the most studious of history and monetary evolution among them) become the newest *hodlers of last resort* . Hodl, which began as a chat room typo in the early days of Bitcoin, has morphed into a memetic phrase that denotes "hodling" Bitcoin long term without regard to its price volatility. Layers of these stubborn

hodlers have been added throughout each of Bitcoin's four major price cycles. A good proxy for the depth of these layers is the lowest price Bitcoin hits each year, which indicates the rising collective obstinacy of these hodlers:



The annual low prices of Bitcoin provide an effective proxy for the collective intransigence of its hodlers.

These layers form the base for the next iteration of each fractal wave pattern. As more observers recognize the survivability of Bitcoin following each price crash, they realize that investing in it may not be as risky as they once thought. This larger base of believers sets the stage for the next iteration of the fractal wave pattern which will support a much larger set of newcomers at a far greater magnitude of peak price. Few people are able to accurately predict how high prices will go in each fractal wave cycle, and they usually reach levels that would seem absurd to most investors at the earliest stages of the cycle. The best proxy for the timing of these fractal wave patterns has been the quadrennial Bitcoin inflation rate adjustment, when the amount of new Bitcoin rewarded at the close of each block is reduced by half, an event commonly known as the *halving*. Historically, Bitcoin achieves a new all-time high price within 18 months of its last halving. The next halving will occur in May 2020:

Every four years, the Bitcoin supply growth rate is cut in half. Each halving also cuts the Bitcoin sell pressure from miners in half and creates upward pressure on its price. Historically, this quadrennial event is the best proxy for the timing of Bitcoin price fractal wave patterns.

The fractal wave patterns inevitably crescendo and begin to crash, usually attributed to myriad factors by mainstream media. However, the Gartner Hype cycle is an archetypal market pricing pattern that is driven entirely by human psychology, game theory and the ultimate exhaustion of market participants reachable in each iteration. The magnitude of each cycle is exacerbated by Bitcoin's absolutely fixed supply schedule, as increases in demand are expressed exclusively through its price, which historically leads to market frenzies at each peak. The long game for Bitcoin, and its final fractal wave pattern, will begin when and if central banks begin accumulating it as a reserve asset (more on this later). In this way, the bedrock of the Bitcoin network's expansion is the intransigency of its hodlers of last resort. Although they constitute a small minority of the whole, these stubborn hodlers will contribute to ongoing Bitcoin adoption in a meaningful way.

Minority Rule [3]

When it comes to group preferences, certain types of minorities—those who stubbornly insist on a particular preference—that constitute even a small level of the total population (often less than 4%) can cause the majority to submit to their preferences. Another clever concept from Nassim Taleb, called the *minority rule*, is the result of complex system dynamics, like those inherent to human interaction.

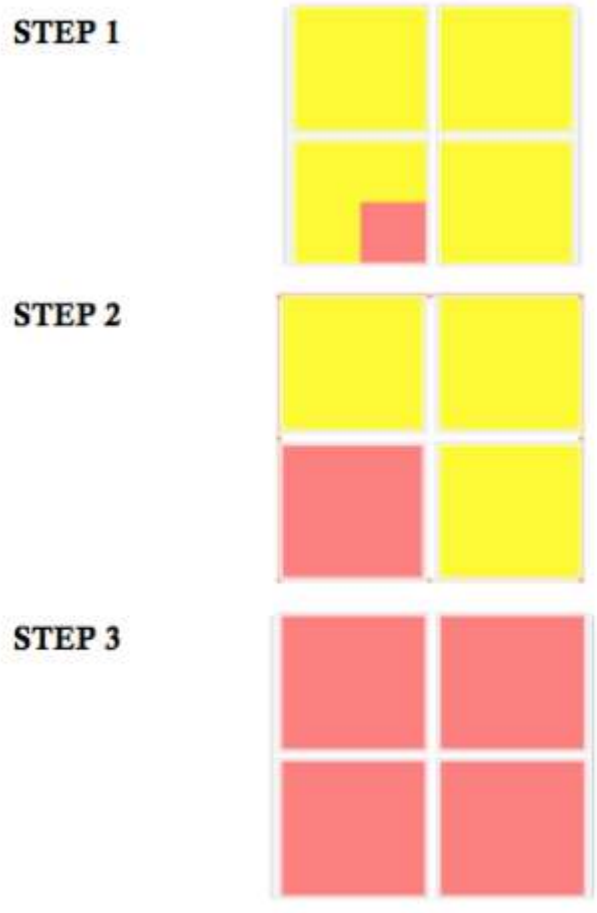
The nature of complex systems (society) is that the collective behaves in a way not predicted by its individual constituents (people). The interactions between its constituents matter more than their individual natures. Studying individual ants will never give us an idea on how the ant colony operates. For that, one needs to understand an ant colony as an ant colony, not just a collection of ants. This is called an emergent property of the whole. In other words, the whole is more than the sum of its parts because what matters is the interactions between the parts. These interactions, while complex, can obey simple rules, like the minority rule (or the rule that barter economies settle on a medium of exchange or that the hardest form of money always outcompetes). Many domains are impacted by the minority rule such as:

- Markets—Market prices are not the consensus of market participants, but instead reflect the activities of the most motivated buyers and sellers. In 2008, a single $50B order, less than 0.2% of the stock market's total value of about $30T, caused the market to drop by almost 10%, causing losses of around $3T. The order was activated by the Parisian Bank Société Générale who discovered a hidden trade by a rogue trader and wanted to reverse the purchase. The market reacted disproportionately because there was only a desire to sell and no way to change the stubborn seller's mind.
- Science—Similar to markets, science is not the consensus of scientists, it is the minority body of knowledge remaining after removing disproven hypotheses.
- Law—A law abiding citizen will never commit criminal acts but a criminal will readily engage in legal acts, and criminal behavior has been shown to be contagious within certain social groups.
- Imports—In the United Kingdom, where the (practicing) Muslim population is only around 4%, a very high proportion of the meat we find is halal (or Kosher). Close to 70% of lamb imports from New Zealand are halal. The same population and import proportions hold true in South Africa (the case of imports is closely related to the example below).

Today, in the United States and Europe, companies are selling more and more non-GMO food precisely because of the minority rule. Given the possibility of food containing GMOs, food not bearing the label "non-GMO" may be assumed by some to contain GMOs which, according to the minority, contain unknown risks. People who

eat GMO food will readily eat non-GMO food, but not the reverse. Assuming the price and distribution costs differences between GMO and non-GMO are sufficiently small and the intransigent minority is distributed somewhat evenly throughout the population, this will have the effect of disproportionately increasing the demand for non-GMO food in the long run. This dynamic of scale can be explained quantitatively. In mathematical physics, renormalization groups are an apparatus that allow us to see how things scale up or down.

Here we show how the minority rule can renormalize the preferences of the majority.



Our graphic depicts:

- Three vertically-stacked large boxes, each representing one sequential step in the minority rule renormalization process
- Four medium boxes in each step, each representing a family of four
- Four smaller boxes contained within each medium box, each representing an individual member within each family of four

Assume that in Step 1, the daughter in the family of four is the intransigent minority (the small pink box) who eats only non-GMO food. As we move to Step 2, the group renormalizes as the stubborn daughter manages to impose her rule on her three family members (who are now all pink) as they are flexible on the matter and consistency simplifies their grocery shopping and administrative process. In Step 3, the family of four goes to a backyard barbecue attended by three other families. As their family is known for their strict eating habits, the host will only serve non-GMO food as the other families are flexible and consistency simplifies the food preparation process, thereby making all four families (which are now all pink) adopt the minority rule originally set by the intransigent daughter in Step 1.

This minority rule will continue imposing and proliferating itself as these families attend other social events, which gradually shifts customer preferences in the neighborhood and eventually causes the local grocery store to switch to non-GMO foods to simplify its procurement processes, which impacts the local wholesaler, and so on up the supply chain. The real world result of this dynamic is the preferences of 4% of a population (practicing Muslims) driving the market preferences of 70% of their respective populations (in the UK, New Zealand and South Africa). As we can see, the minority rule spreads by interaction and renormalizes the entire group to conform with its preferences. Its proliferation is accelerated if there are incentives to switch, low switching costs or anticipated future benefits from switching (as superiorly hard digital cash money, Bitcoin offers all three). In this example, a minority constituting 6.3% of the total population imposed its rules on the majority using pure intransigence. In reality, the minority rule often takes effect when minorities become 4% or less of the total population.

Languages also often adhere to the minority rule. For instance, French was originally intended to be the language of diplomacy as civil servants from aristocratic backgrounds used it, while English was reserved for those engaged in commerce. In the rivalry between the two languages, which are still considered two of the international languages (a third, Spanish, was added later because of its widespread use), English won as commerce came to dominate modern life. This gives us some intuition as to how the emergence of *Lingua Franca* languages, those commonly spoken across cultures, can come from minority rules. As Taleb puts it:

“Aramaic is a Semitic language which succeeded Canaanite (that is, Phoenician-Hebrew) in the Levant and resembles Arabic; it was the language Jesus Christ spoke. The reason it came to dominate the Levant and Egypt isn’t because of any particular imperial Semitic power or the fact that they have interesting noses. It was the Persians –who speak an Indo-European language –who spread Aramaic, the language of Assyria, Syria, and Babylon. Persians taught Egyptians a language that was not their own. Simply, when the Persians invaded Babylon they found an administration

with scribes who could only use Aramaic and didn't know Persian, so Aramaic became the state language. If your secretary can only take dictation in Aramaic, Aramaic is what you will use. This led to the oddity of Aramaic being used in Mongolia, as records were maintained in the Syriac alphabet (Syriac is the Eastern dialect of Aramaic). And centuries later, the story would repeat itself in reverse, with the Arabs using Greek in their early administration in the seventh and eighth's centuries. For during the Hellenistic era, Greek replaced Aramaic as the lingua franca in the Levant, and the scribes of Damascus maintained their records in Greek. But it was not the Greeks who spread Greek around the Mediterranean—Alexander (himself not Greek but Macedonian and spoke a different dialect of Greek) did not lead to an immediate deep cultural Hellenization. It was the Romans who accelerated the spreading of Greek, as they used it in their administration across the Eastern empire."

There is an asymmetry that those who do not have English as their first language usually know basic English, but native English speakers knowing other languages is less likely. If a meeting is taking place in an international office in say, Istanbul, among twenty executives from a sufficiently international corporation and one of the attendees does not speak Turkish, then the entire meeting will be run in English (the commercial Lingua Franca). This is the minority rule in action.

Money is an emergent property, as it is an expected result of complex human interactions within a barter economy. Similar to language, it is a means of expression, only it is used to express value instead of information or emotion. The US Dollar is the Lingua Franca of money today, as it belongs to one of the world's largest economies (an economy which also happens to effectively control the global banking system).

As the digital age matures and the world becomes increasingly interconnected, ever-more commerce and administration will be conducted over the internet. Also, fully interconnected trade networks will level the terrain of commerce and increase free market competition among different forms of money. Considering the significant market lead already enjoyed by Bitcoin, its superior hardness, its multi-sided network effects, the impotency of capital controls on digital cash and the winner take all dynamic inherent to monetary competition; it's likely that Bitcoin will continue to outcompete and its adoption rate will increase. By considering the application of the minority rule to adoption of Bitcoin in the digital age, we can reasonably expect the following:

- Once a sufficient minority of the world's population, say 4% or less, have realized the advantages of hard money and digital cash money, their intransigent hoarding of Bitcoin will drive its price upward (Gresham's Law) and begin imposing itself economically on all other holders of money in the world. This will put downward price pressure on government fiat money,

further accelerate Bitcoin's adoption rate and drastically improve Bitcoin's chances for global acceptance over the long run.
- As the first natively digital form of cash money, Bitcoin will become the Lingua Franca of digital commerce and the dominant value exchange protocol, thereby capturing nearly all the value transacted online (e-commerce alone is estimated to be nearly $5T annually by the year 2021) over the long run.
- Bitcoin may also become the base layer for other tools of cryptographic certainty in commerce, such as smart contracts and TrustNet applications (more on these later).

The minority rule is based on a fundamental asymmetry between the intransigence of the minority and the flexibility of the majority. The minority rule shows us that a small number of unyielding people with skin or soul in the game can change the shape of the majority. Bitcoin already has the advantage of being the hardest form of money ever invented, and its rules are immutable, which is the highest form of intransigency possible. It also has unrivaled brand awareness, fed by the mystery of its creation myth, and the support of free market fanatics all over the world. Once its obstinate minority reaches a certain size, the unbreakable rules of Bitcoin will begin to stubbornly impose themselves on the established economic order. In the words of Margaret Mead:

"Never doubt that a small group of thoughtful, committed citizens can change the world; indeed, it's the only thing that ever has."

A Superior Species of Money [1,4,12]

Bitcoin also introduces three new traits of money never before seen—censorship resistance, adaptivity and programmability. Censorship resistance means that no group or individual in the world can stop payments made on its network. Bitcoin gains censorship resistance by virtue of its decentralized architecture. Adaptivity refers to the ability for Bitcoin's network to become more secure as it stores more value, its open-source nature which aligns the incentives of its global team of volunteer programmers with its own to ensure it is always up to date with state-of-the-art software enhancements and its ability to subsume features from competitors that have been proven in the marketplace. Programmability refers to the digital nature of Bitcoin and its ability to interface with smart contracts and other decentralized applications. As we have learned, the free market for money is a competitive environment that is shaped by continuous market-driven natural selection; as a competitor in this domain Bitcoin is a superior species:

Bitcoin is a Superior Species of Money

Money is a social technology used to solve a problem which has persisted for all of humanity's existence: how to move economic value across time and space. Competition is at all times alive between different forms of money, subject to market-driven natural selection.

Traits of Money	Gold	Government Money	Bitcoin
Fungibility (interchangeable units)	High	Medium	High
Hardness (stock-to-flow ratio)	Medium	Low	High
Portability	Medium	High	High
Durability	High	Medium	High
Divisibility	Low	Medium	High
Security (cannot be counterfeited)	Medium	Medium	High
Easily Transactable	Low	High	High
Scarcity (predictable supply)	Medium	Low	High
Self-Sovereign (permissionless)	High	Low	High
Government Issued	Low	High	Low
Decentralized (censorship resistant)	Low	Low	High
Smart (adaptive & programmable)	Low	Low	High

The technology that is enabling Bitcoin to compete effectively in the market for money is also being applied to create new markets or disintermediate other existing markets. In technical parlance, the Bitcoin network is the world's first decentralized application. A decentralized application is a service that no single entity owns or operates. It is a new form of software and human organization that eliminates single points of failure, resists external attacks and reduces the need for intermediaries. Decentralized applications are enabled by cryptoassets. In the same way corporate equities serve companies and government bonds serve nations, cryptoassets serve decentralized applications. Owning a cryptoasset (like Bitcoin) is the only way to own a piece of a decentralized application (like the Bitcoin network). Technically, a cryptoasset is a cryptographically protected digital token representing rights within an economic network. A cryptoasset is to a decentralized application what oil is to an engine; it provides functionality and liquidity for the network and its constituents. A defining feature of cryptoassets and decentralized applications, and arguably their most alluring, is their organic nature; they are not centrally owned, governed or developed—making them highly resistant against censorship and manipulation.

Bitcoin (the OG cryptoasset) is superior in the market for money because it possesses all the ideal features of digital cash money and enjoys a market dominant position by

virtue of its serendipitous first mover advantage which is fortified from disruption by its open-source design and multi-sided network effects. With the invention of Bitcoin, the world finally has a synthetic form of money with a stock-to-flow ratio that is guaranteed to increase (until it reaches infinity) and an unstoppable, permissionless payments channel. Its digital nature makes it salable across space in a way never before seen, as it can be stored in the human mind and transmitted at the speed of light. The deep divisibility of each Bitcoin into 100 million Satoshis makes them supremely salable across scales. Its informational and nonperishable nature, when considered in combination with its superior hardness, gives Bitcoin unprecedented salability across time. This design makes it an impeccable store of value. Finally, by eliminating all intermediary control (which is inherent to government money) Bitcoin resists debasement, censorship and confiscation. It removes the central banks, macroeconomists, politicians, presidents, dictators and military leaders from monetary policy and payments authorization once and for all. The masterful book (from which much of this essay adapted) titled "The Bitcoin Standard" by Saifedean Ammous sums up Bitcoin's historical relevance nicely:

"If the modern world is ancient Rome, suffering the economic consequences of monetary collapse, with the dollar our aureus, then Satoshi Nakamoto is our Constantine, Bitcoin is his solidus, and the Internet is our Constantinople. Bitcoin serves as a monetary lifeboat for people forced to transact and save in monetary media constantly debased by governments... the real advantage of Bitcoin lies in it being a reliable long term store of value, and a sovereign form of money that allows individuals to conduct permissionless transactions."

Bitcoin is a tool for freedom. As the most accessible asymmetric bet in history, Bitcoin is also a unique investment opportunity.

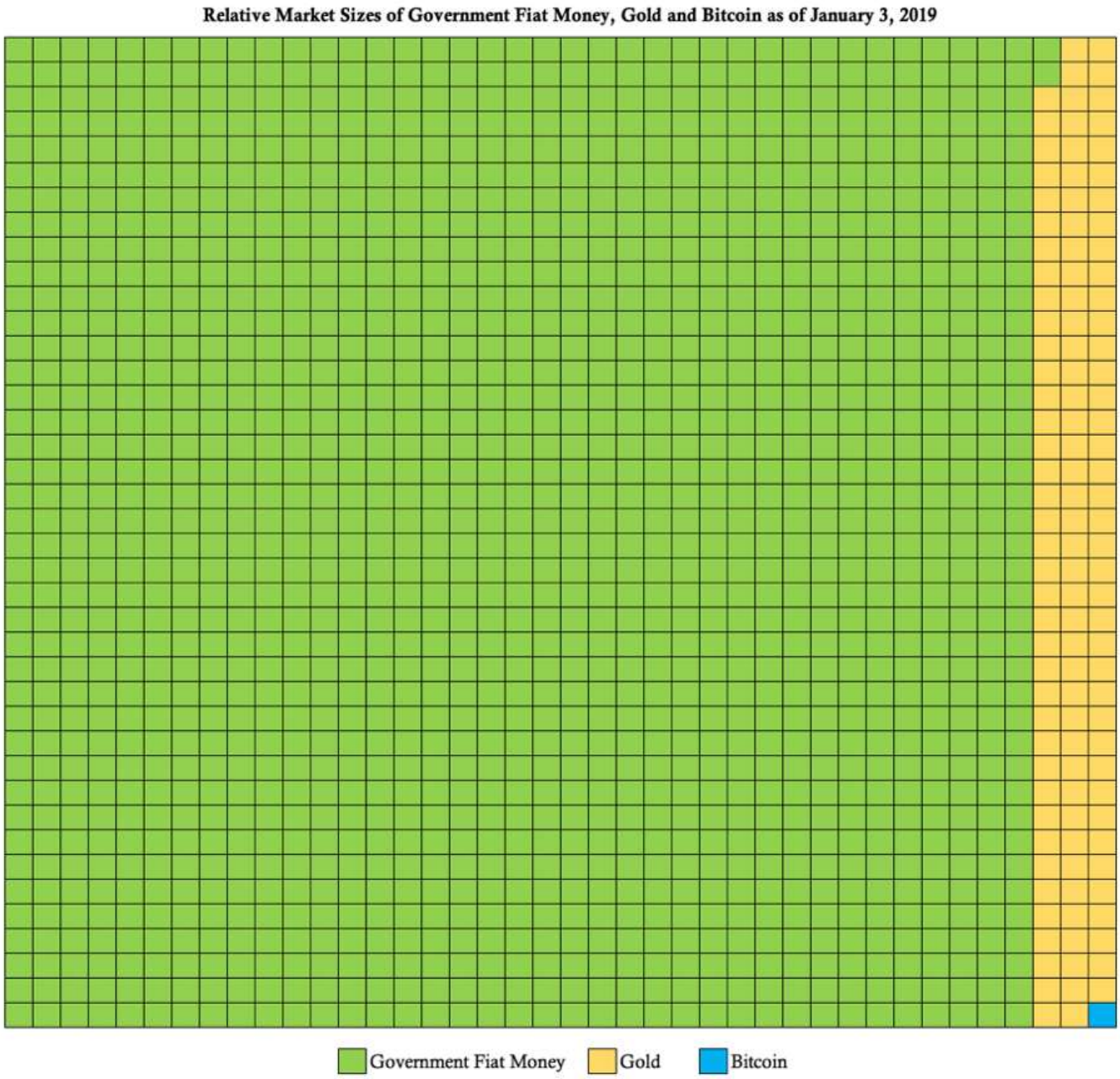
Investing in Bitcoin [1,5,13]

Investing is all about taking intelligent risks. As Daniel Kahneman, a Nobel Prize-winning psychologist, describes it:

"Intelligent risks are based on wide and voracious data gathering checked against gut instinct; while dumb decisions are built from too narrow a base on inputs."

Bitcoin is often referred to as digital gold, in reference to its hardness, self-sovereignty and as an instrument for final settlement. Following this analogy, there will only be one digital equivalent to gold (due to winner take all dynamics inherent to the free market for money), and if you were going to bet on which one will succeed you'd want to bet heaviest on the biggest (due to its deep liquidity and multi-sided network effects), most renowned (due to the minority rule) and the longest lived (due to the Lindy Effect, more on this later). As people tend to think by analogy, this comparison to gold mostly works well, although it is incomplete.

As we have seen, Bitcoin is a far superior monetary technology to the golden inert metal. Technologically, Bitcoin needs little to no protocol improvement to continue to compete effectively in the market for money. There are no unsolved computer science problems standing between Bitcoin and its widespread adoption. Therefore, its primary aim is to remain extant as digital cash money, hence its minimal level of protocol functionality and the status quo bias it exhibits in relation to governance. By merely existing, Bitcoin provides a gateway for people to opt out of the prevailing inflationary monetary order. As long as it continues to operate successfully in its current form, Bitcoin will function healthily as the stateless base money protocol for the digital age—which makes it a viable contender in the $100T market for global money:



Bitcoin is competitively superior to both gold and government fiat money, and has plenty of room to grow.

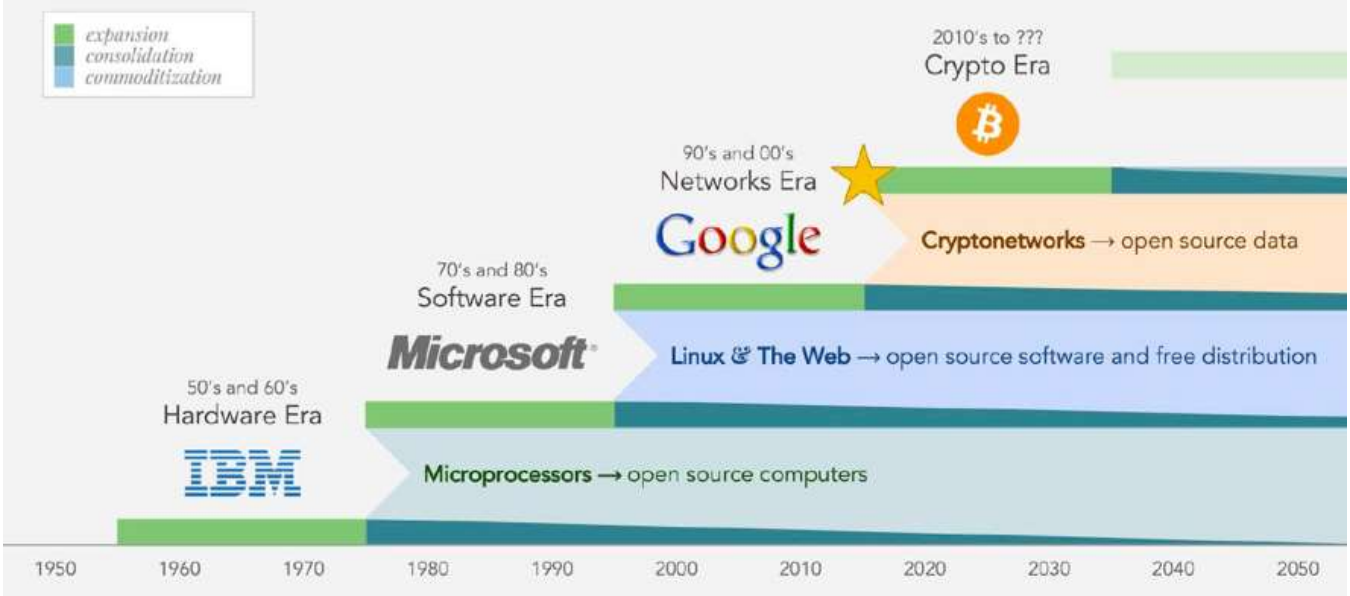
Since it is still extremely small relative to its total addressable market, which consists mostly of gold and government fiat money, Bitcoin still has room to grow by orders of magnitude in both its network size and price. Like a call option, a bet on Bitcoin is asymmetric, meaning that an investor's downside is limited to 1x whereas their potential upside is 100x or more. Should Bitcoin achieve a majority share of the global market for money, its level of demand will become far more predictable and steady, leading to a stabilization in its price.

Investing in Bitcoin can be considered a bet on its adoption as an uninflatable, politically neutral store of value and as an unstoppable, permissionless payments channel.

Bitcoin may also become part of a much bigger wave of innovation. Although the Bitcoin network and the decentralized applications it has inspired are poorly understood by most today (similar to the internet in the early 1990s) we believe that the world will gradually awaken to the paradigmatic shift that is underway for money and markets in general. The greatest wealth is created by being an early investor in innovation. Making such investments requires believing in something before the majority of people understand it—which also often entails enduring mockery, ridicule and criticism for your non-consensus perspective. As Mark Yusko, one of my favorite hedge fund managers, describes the coming crypto era:

"Technology follows 14-year innovation cycles. These began with the Mainframe in 1954, then the Microchip in 1968, the Personal Computer in 1982, the Internet in 1996 and most recently the Mobilenet in 2010. As a result of the innovations introduced by Bitcoin, soon we will christen 2024 as the dawn of the Trustnet."

The *TrustNet* can be thought of as the dawn of trustworthy computing. In theory, it will enable new technologies such as the internet of things, decentralized autonomous organizations, self-owning commercial assets, decentralized internet provisioning, decentralization of energy distribution, reputation markets, computing power markets, stateless identity, immutable media, AI-run organizations, token curated registries, prediction markets and circles of trust. This anticipated innovation wave is consistent with a multi-decade cycle of information technology expansion, consolidation and commoditization:



As innovations in information technology age, they inevitably become commoditized and create the bedrock upon which future waves of innovation are built.

Bitcoin, as the original and driving force of this innovation expansion cycle, will likely function as the systemic core and base money system of the Trustnet. During this cycle, all markets that are enabled by this technology will likely rely on the Bitcoin blockchain as a common value system, final settlement mechanism and temporal anchor point.

A Momentous Innovation [1,4,5,7,8,10]

Bitcoin is a momentous innovation of the digital age. As such, it has many unique characteristics, properties and capabilities never before seen in a monetary technology:

- Immutable Monetary Policy—Predictable, transparent and unchangeable money supply schedule. The most critical aspect to outcompeting in the free market for money, as people will naturally come to favor the hardest form of money available to them (uninflatable money).
- Digital Scarcity—Necessary to solve the double-spend problem and bring the speed and finality of physical cash settlement into the digital
- Absolute Scarcity—The only asset in the world which has an absolutely finite supply, like time itself.
- Global Final Settlement System—A permissionless, unstoppable payments system with zero counterparty risk (like gold, only digital) that can be used to quickly and efficiently provide finality of settlement across scales and space.

- Self-Sovereign Network—A self-sovereign monetary good (an informational bearer instrument) whose network operates autonomously in full accordance with its own immutable rules as reliably as the laws of mathematics.
- Stateless Money—The first globally connected payments system that is politically neutral. Possible catalyst for the separation of money and state over the long
- Revolutionary Social Contract Implementation—A unique 2-layer social contract implementation that decentralizes power among its constituents and creates a hypercompetitive market for its own network security. A new form of social institution.
- Global Consensus—Perhaps the only truly objective set of facts in world history, its distributed ledger is created by converting processing power into indisputable truth.
- Global Energy Buyer of Last Resort—Enables anyone in the world to convert excess electricity into digital gold on demand. A perpetual incentive for everyone in the world to develop more energy efficient innovations.
- A New Form of Life—Feeds on human self-interest and electricity to provide uninflatable money, an unstoppable payments channel and immutable governance.
- Adaptive Security—By virtue of the mining difficulty adjustment, as more value is stored on its network, the network adapts to become more secure.
- Adaptive Functionality—As an open-source software project, programmers around the world are constantly improving Bitcoin's codebase, however it is up to the users to adopt these changes, which creates a governance equilibrium in which only those changes that are in the collective best interests of users will be adopted. Enables Bitcoin to subsume superior features from competitors that are market-proven, making it highly resilient to disruption.
- Programmability—As a digitally native form of money, it can be used as a form of payment, collateral or fuel for a variety of smart contracts (self-executing software or commercial agreements). Can interface with other decentralized applications. Could function as the core value system for the TrustNet, the anticipated wave of innovation triggered by the emergence of Bitcoin.

Bitcoin has made a major impact in the world in its 10 years of existence, and it still holds a great deal of promise for the future. All in good time. Given its inextricable relationship with money and Bitcoin, the concept of time is worth exploring more deeply. It turns out that time's role in our lives, individually and collectively, is the key to understanding prosperity and the ways in which Bitcoin could play a key role.

Synthesized Works & Further Reading

- [1] *The Bitcoin Standard: The Decentralized Alternative to Central Banking* by Saifedean Ammous (a masterful work on which much of this essay is based)
- [2] *The Rational Optimist* by Matt Ridley

- [3] *Skin in the Game* by Nassim Nicholas Taleb
- [4] *The Bullish Case for Bitcoin* by Vijay Boyapati
- [5] *The Age of Cryptocurrency* by Paul Vigna and Michael J. Casey
- [6] *Sapiens* by Yuval Harari
- [7] *Bitcoin is a Decentralized Organism, Part 1 and Part 2* by Brandon Quittem
- [8] *PoW is Efficient* by Dan Held
- [9] *The Fifth Protocol* by Naval Ravikant
- [10] *Unpacking Bitcoin's Social Contract* by Hasu
- [11] *Antifragile* by Nassim Nicholas Taleb
- [12] *Letter to Jamie Dimon* by Adam Ludwin
- [13] *Placeholder VC Investment Thesis Summary* by Joel Monegro and Chris Burniske
- [14] *Diffusion of Innovations* by Everett M. Rogers
- [15] *Why America Can't Regulate Bitcoin* by Beautyon
- [16] *Hyperbitcoinization* by Daniel Krawisz

Money, Bitcoin and Time: 3 of 3

By Robert Breedlove

Posted January 26, 2019

This is part 3 of a 3 part series

- Money, Bitcoin and Time: 1 of 3
- Money, Bitcoin and Time: 2 of 3
- Money, Bitcoin and Time: 3 of 3

7 The Simple Truth about Time: Time is the ultimate resource. Its absolute scarcity bounds the entirety our stories, both as individuals and societies.

With economics, we strive to use it more effectively. As the destroyer of all things and the healer of

The Ultimate Resource [1]

Scarcity is the starting point of all economics. It is commonly believed that natural resources are inherently scarce, which is true in a sense, as there is only so much gold within the Earth, for instance. However, this finite quantity of gold in the Earth is still too large for humans to even measure and in no way constitutes an actual limit to the amount we can conceivably mine. We have literally 'just scratched the surface', as our mining efforts haven't even taken us half way into the Earth's crust, its thinnest and outermost layer. Driven by need, humans have always found a way to explore farther and dig deeper to uncover ever-more natural resources. Therefore, the actual practical limit to the quantity of any natural resource is always and only the amount of human time, effort and ingenuity devoted to its production. For human beings then, the only truly scarce resource is time.

Individually, the only scarcity we face is our limited time on Earth. As a society, the only scarcity we deal with is the total amount of human time, effort and ingenuity available to be directed at the production of goods. This scarce resource, which we will call *human time*, is the ultimate societal means of production. Humans have never fully exhausted any single natural resource. The price of all natural resources, in terms of human time, has always decreased steadily over the long-run as our technological advancements have dramatically increased our productivity. Not only have we not depleted any natural resource, but the proven reserves (the amount of natural resources still within the Earth) continue to increase despite our increasing rates of production, as new technologies enable us to discover and excavate ever-more natural resources.

Oil, the lifeblood of the industrial economy, is a great example of this concept. Even as oil production has increased every year, its proven reserves increase at an even faster rate. According to data from BP's statistical review, annual oil production increased 50% from 1980 to 2015. Oil reserves, on the other hand, have increased 148% during the same 35 year period, around triple the increase in oil production. Similar statistics exist for all natural resources prevalent in the Earth's crust. Some are more common (iron, copper) and some are rare (gold, silver) but the limit of how much we can produce of any particular natural resource is always and only the amount of human time directed at its production. The best evidence of this simple fact is gold: if the annual production of the one of the rarest metals in the Earth's crust goes up every year, then it makes no sense to consider any other natural resource being scarce in any practical sense. Echoing back to the fundamental market realities related to deferred consumption and investment—the real cost of anything is always its opportunity cost in terms of goods forgone to produce it. In

terms of natural resources, only human time is truly scarce, which makes time the ultimate resource.

Frozen Time [1]

As more humans exist, there is more human time to direct towards the extraction and production of natural resources. As we have learned, productive output per unit of human time (productivity) can be amplified by leveraging technological solutions to problems (tools). In economics, a tool or technology is considered to be both:

- A non-excludable good—once one person invents something, all others can copy it and benefit from it
- A non-rival good—a person benefiting from an invention does not reduce the utility that accrues to the others who use it

For example, once one person invented the wheel, everyone else could copy its design and make their own, and their use of this design would in no way reduce others' ability to benefit from it. Innovations like this spread and their benefits compound over time, leading to ever-higher productivity and division of labor. Like the candle whose flame burns undiminished even after igniting a thousand others, the benefits of innovation ultimately accrue to everyone without detracting from the innovator in any way.

Natural resources and innovation are always and only the product of human time. Therefore, in terms of production, human time is the ultimate resource and essence of value. To keep score, people needed a way to reliably store the value they produce with their time, so that they can exchange it in the future for other peoples' time, effort and ingenuity. Conceptually then, money is frozen time. It is earned by sacrificing human time and can be traded for commensurate sacrifices from others. The age-old problem faced by people is collectively deciding which monetary technology can best serve this purpose.

Technologically, money is a spontaneous emergent property that humans ascribe to a particular good. People, acting in self-interest, live within technological and economic realities that shape their decisions and provide them incentives to persist, adapt, change or innovate. It is from the countless collisions of these complex human interactions that spontaneous monetary orders have emerged and decayed. History has shown us myriad cases of a good being subjected to market-driven natural selection, achieving a monetary role and subsequently having its role taken by a superior technology.

Whatever monetary media people chose as a store of value was always subject to being produced in greater quantity, so the producers could acquire the value stored in it. The Yapese witnessed this play out when O'Keefe produced Rai Stones using

explosives. West Africans had their wealth confiscated by Europeans who shipped in boat loads of cheaply produced glass beads. Citizens in modern economies continuously have their wealth usurped as central banks gradually or quickly erode the value of government fiat money. Gold came close to solving this problem as it is indestructible, expensive to mine and its flow is relatively predictable. However, gold's physicality led to its centralization within bank vaults and its compulsory replacement with soft government money.

Until the invention of Bitcoin, all forms of money were subject to having their value stolen by producers of the monetary good. This made all monetary technologies before Bitcoin imperfect in their ability to store value across time. Bitcoin's finite supply makes it the best medium to store the value produced by finite human time. In other words, Bitcoin is the best store of value humanity has ever invented, as it is the only monetary technology that cannot be debased over time. The informational, intangible and purely digital nature of Bitcoin enables it to achieve absolute scarcity, a property that was previously exclusive to time itself.

The absolute scarcity of Bitcoin makes it the perfect modality for freezing and transacting the only other absolutely scarce resource — time.

No matter how many people use the network, how advanced mining equipment becomes or how much its price increases, there can only ever be 21 million Bitcoins in existence. In time, it is likely that Bitcoin will be regarded as the best technology for saving ever invented.

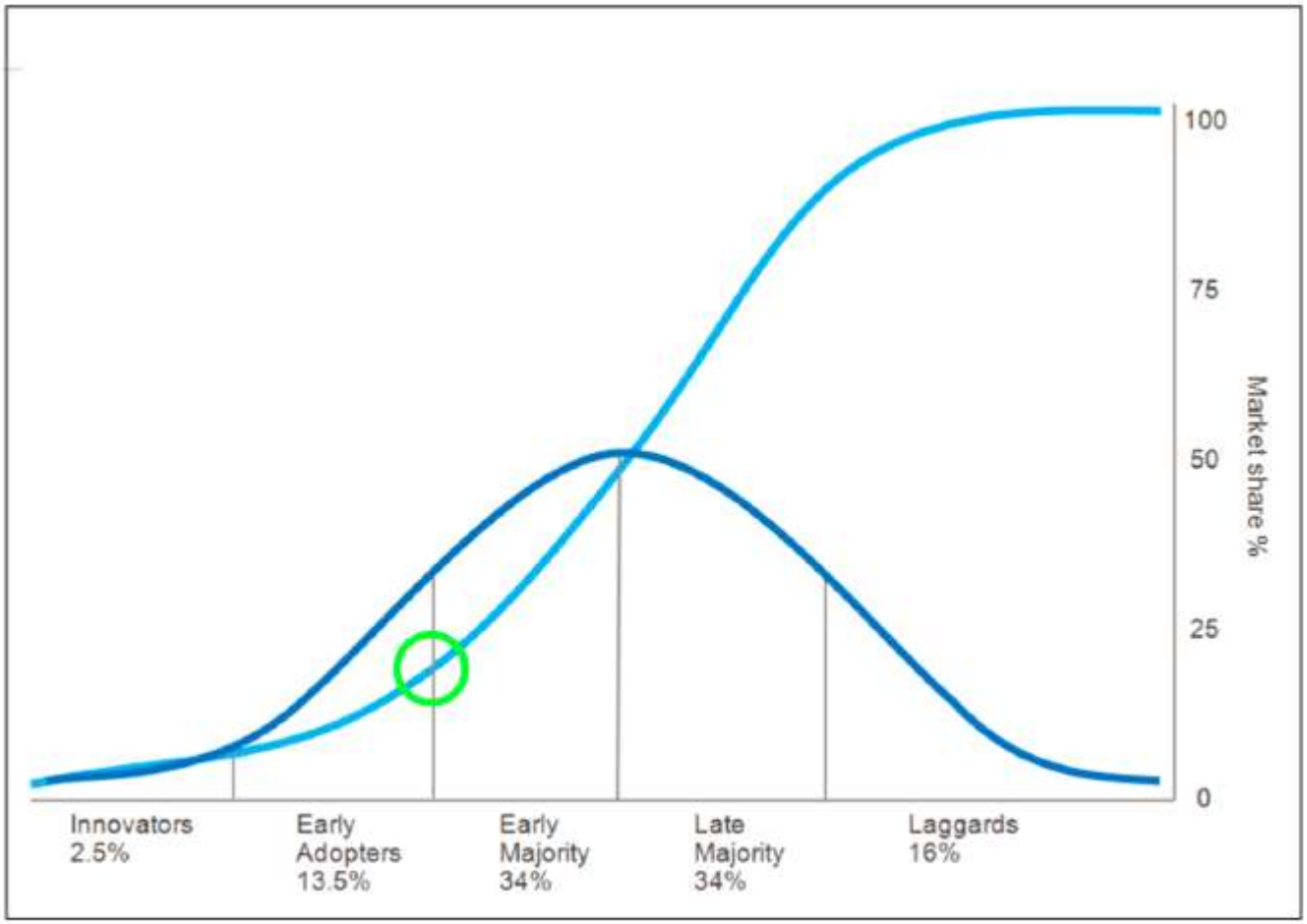
Time Arbitrage [2,13,14]

Innovations of this magnitude are virtually impossible to predict; however, they do follow a familiar adoption pattern. The book titled 'Diffusion of Innovations' lays out a framework that seeks to explain how, why and at what rate new ideas and technologies spread. Diffusion is the process by which an innovation is communicated and adopted by participants in a social system over time. There are four main elements that influence the spread of the new idea:

- The nature of the innovation
- Communication channels
- Time elapsed since ideation
- The social systems under which it is adopted

Once a certain rate of adoption is achieved, the innovation reaches a tipping point and its continuous spread becomes practically unstoppable (a concept of preferences closely related to the minority rule discussed earlier) as people naturally prefer superior technology solutions. Such an adoption curve is especially true of, and often completed faster for, network-based technologies such as the internet and

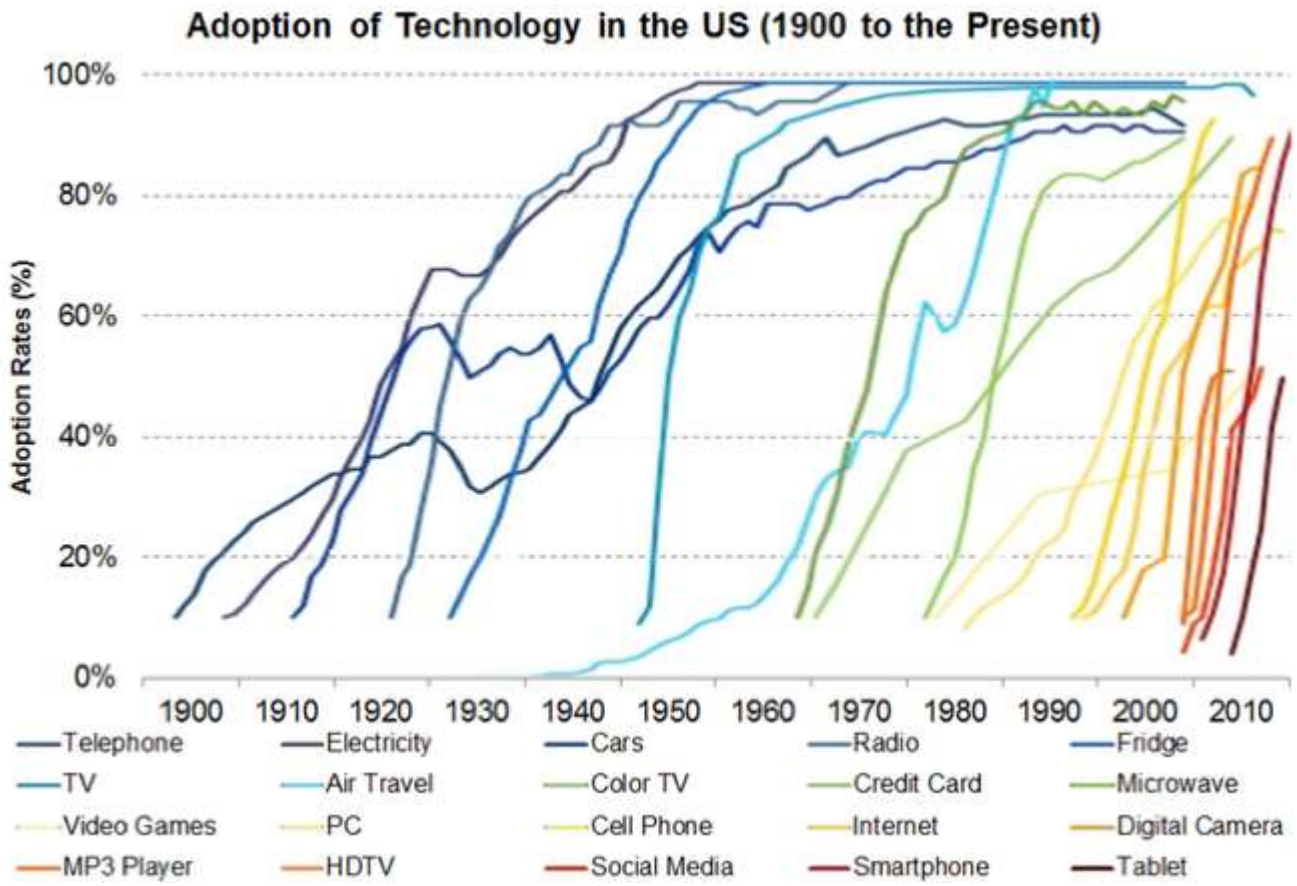
Bitcoin; as their general acceptance is driven harder and faster by network effects. Based on its estimated number of users, we are just beginning to enter the early adopter phase for Bitcoin:



The S-curve of adoption. As succesive groups adopt a new technology or idea market share rises. The tipping point (green circle) marks an inflection point and leads to rapid growth in adoption.

In investing, the concept of *time arbitrage* refers to an asset becoming oversold based on a short-term or emotional market sentiment despite its long-term outlook or investment fundamentals remaining unchanged or even improving. Time arbitrage is essentially another form of the old investment adage "Buy on bad news, sell on good news". Times such as these present savvy investors with an opportunity to enter a position with the same or improved value fundamentals at a lower price point.

All ubiquitous technologies today, beginning as fledgling innovations themselves, have traversed this path to mainstream adoption. Here we show some of the most impactful innovations since the year 1900 and the rapidity with which they were adopted:



telecommunication networks have become more advanced and ubiquitous, the user adoption rates of new innovations have accelerated dramatically.

As we can see, advances in telecommunications and distribution methods have accelerated the pace with which new innovations are adopted. Today, the internet causes breakthrough innovations to spread like a wildfire throughout the minds of people all over the world. Since it is a nascent monetary technology that is not fully understood by the vast majority of the world, Bitcoin still has low levels of adoption and therefore significant upside prospects. Also, owning a piece of the Bitcoin network today is over 80% cheaper than about a year ago even though its utility in terms of throughput, transaction fee efficiency and network security have all improved substantially over the same period. This confluence of factors indicates that now is an opportune time to take advantage of time arbitrage and invest in the Bitcoin network. Also, as a technology, the Bitcoin network's value will continue to grow with every passing day that it successfully operates.

Lindy Effect [4,11]

Things in this world fall into one of two general categories: perishable and nonperishable. The distinction between the perishable (humans, single items) and the nonperishable is that the latter does not have a natural, unavoidable expiration

date. The perishable is typically physical in nature, meaning it is subject to physical degradation, whereas the nonperishable is typically informational in nature. A single car is perishable, but the automobile as a technology has survived for a century and can be reasonably expected to persist for at least another one. An individual man will die, but his genes (which are digital) can be passed on for innumerable generations. This heuristic from Nassim Taleb, known as the *Lindy Effect*, can be summarized as follows:

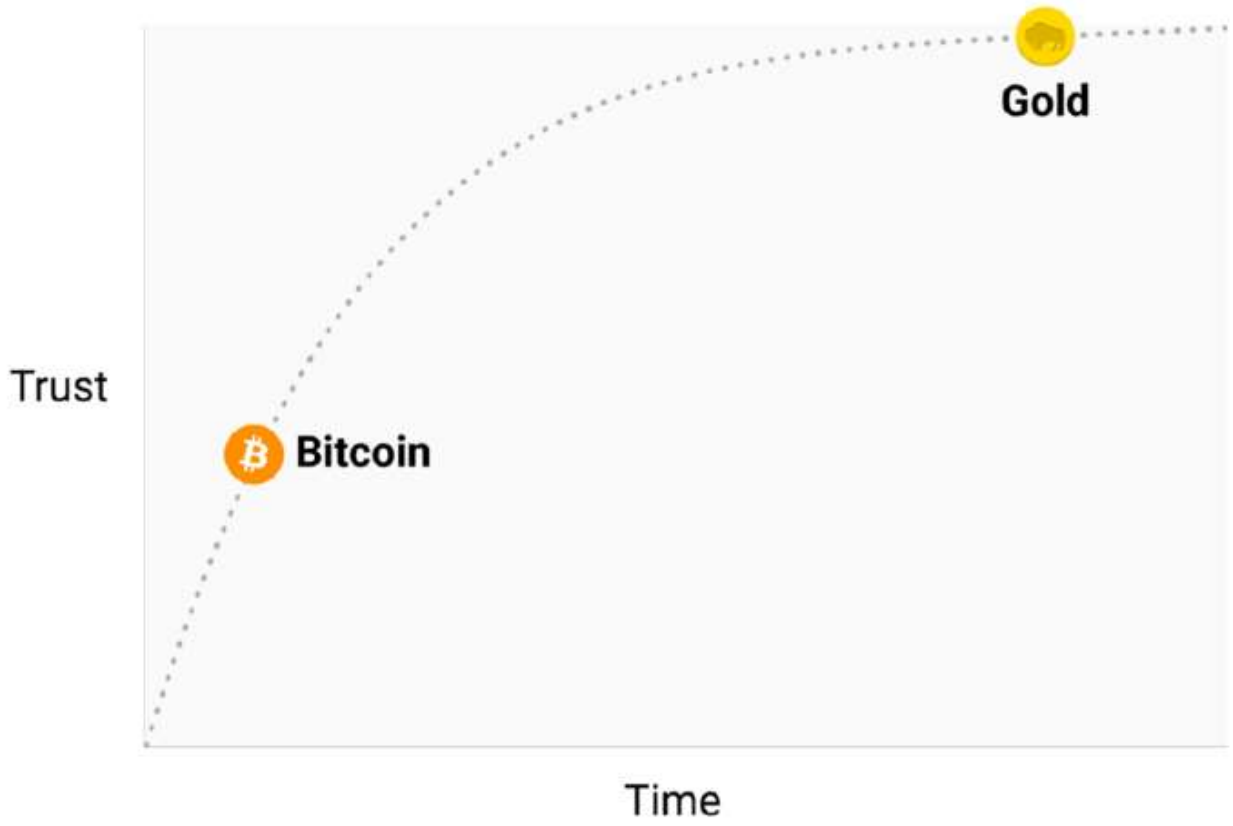
- For the perishable, every additional day of life translates into a shorter additional life expectancy.
- For the nonperishable, every additional day of life may imply a longer life expectancy.

The only effective judge of things is time, as time is the ultimate destroyer of all things. The Lindy Effect is closely related to antifragility, as the ravages of time are a potent form of adversity. Anything that gains from temporally-driven increases in disorder is antifragile and benefits from the Lindy Effect. Using arbitrary math for simplicity, if a book is still in print after 50 years, it can be expected to remain in print for another 50 years. If it's still in print for another 50 years after that, then perhaps it can then be expected to remain in print for at least an additional 120 years. At some point, the Lindy Effect may imply an unlimited life expectancy. A book like the Bible, which has been in print for thousands of years, can be reasonably expected to remain in print for the rest of human history.

If you had conducted a survey in 1995 and asked people whether they believed the internet would be a permanent feature of their lives, you would have probably received mixed responses. If you conducted the same survey today, people would resoundingly agree that the internet is here to stay. A technology, being informational rather than physical in nature, does not age in the same way humans do. A technology like the wheel is not "old" in the sense of experiencing degradation, it is a technological design that has persisted for millennia and can be reasonably expected to persist for many more.

So, the longer a technology lives, the longer it can be expected to live. Since Bitcoin is a technology, every day that it continues to successfully operate increases its life expectancy. Further, as we have learned, the core moving parts of Bitcoin are mathematics and human nature—two concepts which are very "Lindy" and can be reasonably expected to persist for the rest of human history. Bitcoin's ever-growing life expectancy increases its perceived trustworthiness and eventually it will be regarded as a permanent feature of our modern lives in the same way the internet is today. This heuristic helps explain why gold will likely continue to be regarded as a

monetary metal for many years to come, whereas Bitcoin is still in the process earning people's trust:



Hard monetary technologies become more trusted over time as they offer peace of mind to their users.

The Lindy Effect is universally applicable across time. The same competitive dynamics that caused the ascent of gold into a dominant monetary role are now driving Bitcoin adoption. In this sense, the future is in the past. As the Arabic proverb says: *he who does not have a past has no future.* Notwithstanding the past century of central bank coercion, hard money is the norm of human history and we are witnessing its reemergence with the rise of Bitcoin. As Bitcoin continues to persist, knowledge of its fundamental nature and functional capabilities will continue to spread. Threatened by its continued growth, incumbents will ratchet up their efforts to prevent Bitcoin's ascent and protect the monopoly on money they have enjoyed over the past century.

Future of Regulation [1,4,5,15]

There is a good reason why the gold standard was forcibly ended and no good store of value has yet risen to fill the void. To preserve seigniorage profits governments must enforce an inflationary monetary policy. Otherwise, if a sound store of value

existed that was accessible to its citizenry, their business model would be jeopardized as people would exit depreciating fiat currencies to shield their wealth from further confiscation. As Alan Greenspan, former Chairman of the Federal Reserve (the central bank of the United States) said in 1966:

"In the absence of the gold standard, there is no way to protect savings from confiscation through inflation. There is no safe store of value. If there were, the government would have to make its holding illegal, as was done in the case of gold.** If everyone decided, for example, to convert all his bank deposits to silver or copper or any other good, and thereafter declined to accept checks as payment for goods, bank deposits would lose their purchasing power and government-created bank credit would be worthless as a claim on goods. **The financial policy of the welfare state requires that there be no way for the owners of wealth to protect themselves."**

Clearly, central banks are aware that free market competition against hard money poses significant risk to the continuity of their socialistic business model. To protect central bank monopoly positions, governments have resorted to passing onerous laws against their citizens. Governments seek to insulate their national currencies from free market competition employing legal measures such as:

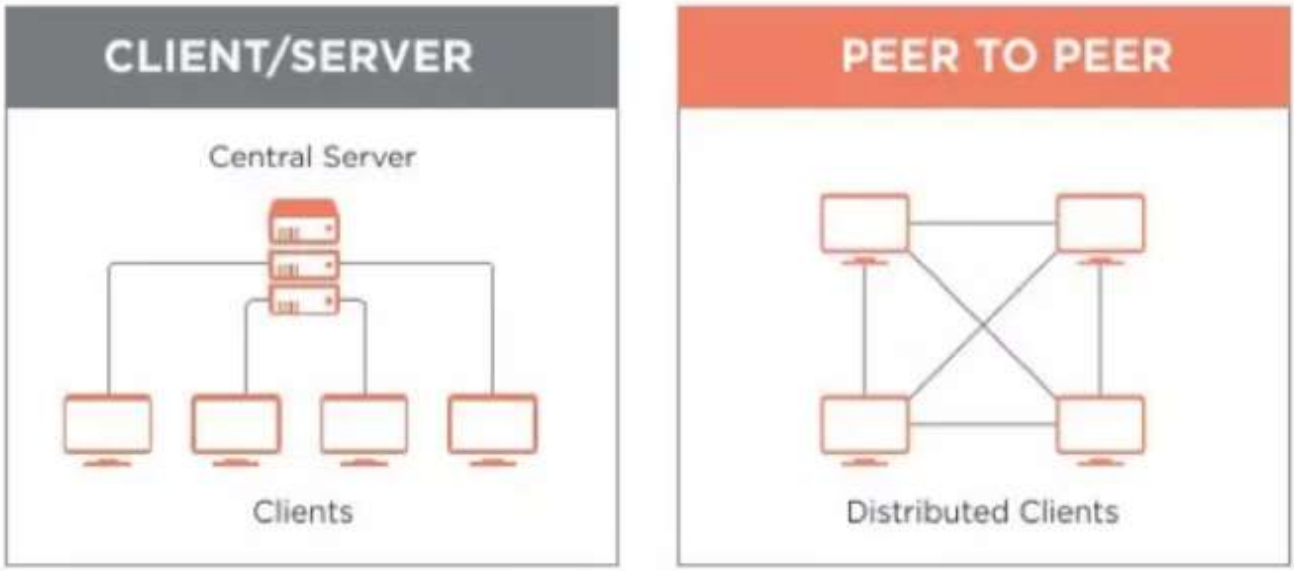
- Capital Controls—which prohibit the movement of money into or out of a country
- Confiscatory Orders—forceful seizure of assets, like Executive Order 6102 in 1933 which outlawed private ownership of gold in the United States
- Legal Tender laws—which create artificial demand for government fiat money by requiring that it be accepted in settlement of debts

With Bitcoin, regulators face a unique dilemma. Bitcoin exists orthogonally to the law, and there is virtually nothing that any authority (or anyone for that matter) can do to affect its operation. Regulations were designed to govern people and entities and are not equipped to deal with a decentralized network that autonomously proliferates itself. Regulators are really good at targeting centralized marks, like an individual business or its CEO, and enforcing laws against them. However, regulations have proven to be largely impotent against decentralized services.

To understand this point, consider the case of BitTorrent, a decentralized peer-to-peer file sharing service. In the earlier days of the internet, file sharing platforms like Napster and Kazaa had become an extremely popular way for users to share movies, music and other media directly with one another. With these free services, users would upload media to and download media from the companies' computer servers. This client-server file sharing directly threatened media monopoly profits, as it completely circumvented copyright law. Incumbent organizations quickly

responded with heavy litigation. Since services like Napster and Kazaa were hosted by centralized companies complete with a headquarters, executive team and computer servers, they were vulnerable to being shut down. Filing a lawsuit, knocking on some doors, levying some fines and decommissioning some computer servers was all it took to shut down these services and protect media industry monopolists.

The introduction of BitTorrent, an open-source decentralized protocol for peer-to-peer file sharing, was a game changer. Once installed on a computer, BitTorrent enables user nodes to upload and download movies, music and other media directly from one another using encrypted communication channels. Since files on its network do not come from a single source, BitTorrent was also able to offer superior download speeds by fragmenting the media files and pulling from multiple nodes simultaneously. Unlike the failed client-server models of centralized platforms, the BitTorrent protocol never holds any of the media files, it only facilitates the transfer of files between individual users:



Like the proven model of BitTorrent, Bitcoin sports a decentralized architecture that makes it highly resistant to external attack and censorship.

Architecturally, the entire software codebase of the protocol exists on every user machine that downloads it, making it virtually impossible for a regulator to target and shutdown as there is no single point of vulnerability (censorship resistance). The BitTorrent protocol exists everywhere and nowhere by virtue of its decentralized network architecture, a model that would be later employed by Bitcoin. Indeed, without a centralized target to shut down, regulators were incapable of stopping BitTorrent and the other protocols it inspired. By 2009, peer-to-peer file sharing using

decentralized protocols like BitTorrent accounted for up to 70% of internet traffic worldwide.

Bitcoin has already exhibited similar properties to BitTorrent as regulators have been incapable of containing the expansion of its network or shutting it down. It cannot be contained by capital controls, as it exists entirely outside the legacy financial system. Confiscation of Bitcoin, unlike that of gold, is extremely difficult given its informational nature. This leaves legal tender laws, which are still enforceable and could therefore require Bitcoin users to convert some of their holdings into government fiat money to pay their taxes. So, the exchanges and OTC markets where Bitcoin is traded are the only viable targets for regulators. As such, these financial gateways that connect Bitcoin to the traditional financial system are likely to see continuous intensification of regulatory scrutiny and enforcement actions. However, as we saw in China, escalated efforts will likely only highlight the need for Bitcoin, expand its brand awareness and spawn off exchange transactions (Streisand Effect).

In essence, open-source software projects like Bitcoin are just information—software written in a computer language called code. Since it is just code, Bitcoin can be printed out, written down, spoken or memorized. Bitcoin is also a form of money, so it makes money and information the same thing. This concept was summed up nicely by Naval Ravikant in 2017:

“This is one of the crazy things about this concept because money and speech turned out to be the same thing — money, information and math - they’re the same thing. In a Bitcoin world, I can literally write down my Bitcoin address and keys on a piece of paper and put it in a safety deposit box. It’s basically in cold storage, I could even put it in my head. I can memorize the key phrases and I could cross national borders with $1 billion in my brain. It’s a very powerful but literally mind bending concept in that sense.”

The First amendment of the United States Constitution guarantees that all Americans have the power to exercise their right to publish and distribute anything they like, without restriction or prior restraint—which includes software code like that which constitutes Bitcoin. Established legal precedent in the United States explicitly protects software code under the First Amendment. Consider the case of PGP:

“In 1995, the US Government had on the statute books, laws that restrict the export of encryption software products from America without a license. These goods are classified as ‘munitions’. The first versions of the breakthrough Public Key Encryption software “Pretty Good Privacy” or “PGP”, written by Philip Zimmerman had already escaped the USA via Bulletin Board Systems from the moment it was first distributed, but all copies of PGP outside of the United States were “illegal”. In order to fix the problem of all copies of PGP outside of America being encumbered by this

perception, an ingenious plan was put into motion, using the first Amendment as the means of making it happen legally. The source code for PGP was printed out . It's as simple as that. Once the source code for PGP was printed in book form, it instantly and more importantly, unambiguously, fell under the protection of the First Amendment."

Bitcoin unambiguously falls under the Freedom of Speech Protections offered by the First Amendment to the United States Constitution.

For these reasons, it is unlikely that any major government would attempt to ban Bitcoin outright as, not only would it contradict freedom of speech laws, it would also create a tidal wave of publicity (again, Streisand Effect). Central banks have acknowledged this reality. Former chairwoman of the Federal Reserve Janet Yellen confirmed:

"The Federal Reserve simply does not have the authority to supervise or regulate Bitcoin in any way."

So, Bitcoin can't be shut down, is virtually immune to regulation and leverages economic incentives to grow relentlessly. Its very existence is a game changer for almost everyone in this world, especially central banks who now face an existential threat to their business model.

The Long Game [1,4,16]

Money is how we keep score in the game of life. *Game theory* explores how rational people make strategic decisions in different scenarios. It is based in purely mathematical terms and has applications in any domain where people must choose whether to cooperate or compete with each other. The standard game analyzed by game theory is the Prisoner's Dilemma:

Two members of a criminal gang, Alex and Bobby, are arrested and imprisoned. Each prisoner is in solitary confinement with no means of communicating with the other. The prosecutors lack sufficient evidence to convict the pair on the principal charge, but they have enough to convict both on a lesser charge. Simultaneously, the prosecutors offer each prisoner a bargain. Each prisoner is given the opportunity either to betray the other by testifying against them, or to cooperate with the other by remaining silent. The possible decisions and outcomes are:

- *If Alex and Bobby both betray each other, each of them serves 2 years in prison*
- *If Alex betrays Bobby but Bobby remains silent, Alex will be set free and Bobby will serve 3 years in prison*
- *If Bobby betrays Alex but Alex remains silent, Bobby will be set free and Alex will serve 3 years in prison*

- *If Alex and Bobby both remain silent, both of them will only serve 1 year in prison (on the lesser charge)*

This game decisions and its outcomes are summarized in this table:

		Bobby's decisions	
		Bobby stays silent (cooperates)	Bobby testifies (betrays)
Alex's Decisions	Alex stays silent (cooperates)	Alex and Bobby each serve 1 year	Alex serves 3 years, Bobby goes free
	Alex testifies (betrays)	Alex goes free, Bobby serves 3 years	Alex and Bobby each serve 2 years

Game theory shows us that adversaries will often behave contrary to their mutual best interests.

This Prisoner's Dilemma game converges on a *Schelling Point*, which is a solution that people will tend towards in the absence of communication or definitive trust (in other words, in an adversarial environment). The Schelling Point in the Prisoner's Dilemma is that Alex and Bobby both choose to betray each other, as each would risk 3 years in prison if one chose to remain silent and the other testified. Since both have an incentive to testify, the optimal strategy for this game is that they both betray, despite their mutual silence offering the best outcome for them both.

Since money is an adversarial game (there are winners and losers) express communications between players cannot always be trusted. Therefore, the Schelling Point of monetary competition is to choose the available good which exhibits the highest hardness, because people (potential adversaries) must be restrained from creating new monetary units to steal the value stored within them. This is exactly the reason market-driven natural selection is so ruthlessly effective at promulgating hard money, as people are constantly seeking to acquire value and store it in the most reliably hard monetary technology available.

Monetary goods, like Bitcoin, are valued based on their game theoretic qualities—meaning each market participant values a monetary good based on their appraisal of whether and how much other participants will value it (in the same way that prisoners Alex and Bobby must anticipate each other's decisions to make effective decisions of their own). The earlier one is able to anticipate the future demand for a monetary good, the greater the advantage conferred to the prognosticator; as it can be acquired more cheaply than when it becomes widely demanded at a later time. Further, when one acquires a good expecting that it will be demanded as a future

store of value, it actually hastens the adoption of the good by others for that particular purpose, as their selection of a store of value is partly influenced by their perception of your intentions which drove you to acquire the monetary good in the first place. This seeming circularity is another positive feedback loop that drives societies to converge on a single store of value (another aspect of the winner take all dynamic):

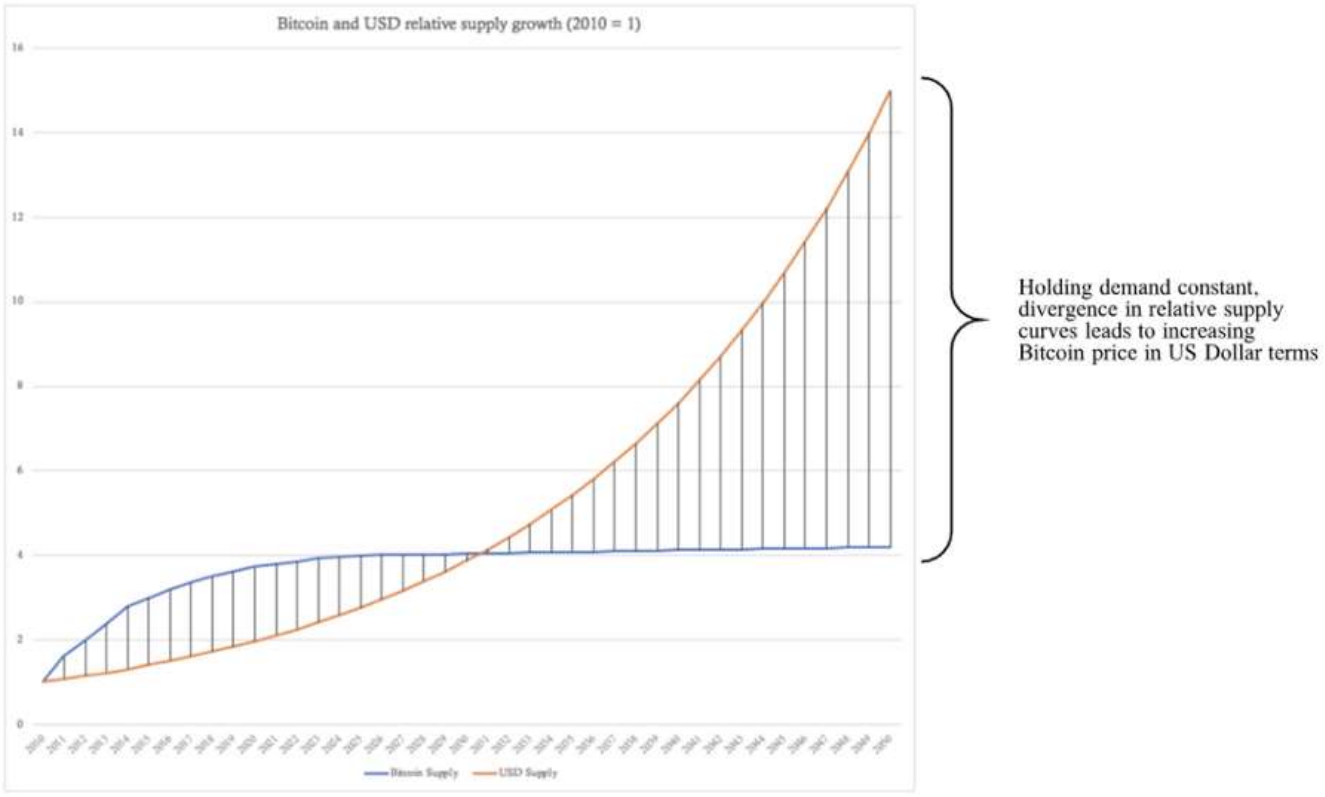
The game theoretic properties of the monetization process encourage people to converge on a singular money

In game theoretic terms, total market dominance by a single store of value with a superior stock-to-flow ratio is known as a *Nash Equilibrium*—a game state where no player has an incentive to deviate from his chosen strategy after anticipating the most likely choices of all his opponents. Throughout all human history, societal convergence on a single form of superiorly hard money is the Nash Equilibrium of monetary competition. As we saw with gold in the 19th century, when multiple societies converge on a single store of value, they see a substantial decrease in trade costs and an attendant increase in free trade and capital accumulation (La Belle Époque). Only the past century, dominated by government fiat money, is anomalous in this respect.

Hard money is the norm of human history, and we are seeing its reemergence with Bitcoin.

The monetization process, as we saw with gold and are now seeing with Bitcoin, is game theoretic. People must decide individually how best to store the value created by their time spent in production. This decision is based on the anticipated beliefs, decisions and actions of others in relation to the monetary technologies available to them. The complex interaction of these decision dynamics is how people spontaneously ascribe a good the role of money and why the hardest money always wins. In this way, hard money is an emergent property of indirect exchange just like money is an emergent property of direct exchange.

This emergent property perspective is exactly why value stored in softer forms of money is totally absorbed by hard money every time they interact within an economic network. Existing amid the expansionary monetary policies being practiced by every central bank in the world today, Bitcoin's price will continue to increase as the ratio of government fiat money in circulation to Bitcoin units in circulation diverges ever-further:



This graphic, which is strictly illustrative, simply shows that divergence in supply curves of Bitcoin and US Dollars will lead to the appreciation of Bitcoin in US Dollar terms, even without any increase in the demand for Bitcoin (as we have seen, demand for Bitcoin has been surging). The same dynamic is applicable to all modern government monies, as every central bank in the world is engaged in aggressive expansionary monetary policy. In the game of international government fiat monetary competition, the Nash Equilibrium is all currencies inflated into worthlessness. On this race to the bottom, those with easiest access to freshly printed money will expropriate as much value as possible (via the Cantillon Effect) and use it to acquire real estate, gold or other inflation resistant assets (such as Bitcoin). This game theoretic perspective clearly explains why virtually all soft government fiat currencies have trended towards eventual worthlessness.

Next, we show how all major fiat currencies have depreciated almost completely against gold since 1900 (notice the steep decline in 1971 when the peg to gold was completely severed):

All major currencies depreciation v gold

As we have seen throughout history, every time hard money encounters soft money in a trade network, it has outcompeted it into extinction. We saw earlier how gold, possessing superior hardness, demonetized silver with dire economic consequences

for those societies that remained on a silver standard the longest, such as China and India. Now it is gold that faces a monetary competitor with superior hardness, and it is likely that it will gradually become demonetized as people convert to Bitcoin for its unparalleled store of value properties. This will happen slowly, and gold may indeed maintain some of its monetary use case given the vast holdings of central banks, mankind's deep history with the monetary metal (Lindy Effect), its relatively high and predictable stock-to-flow ratio and the fact that some people may always prefer a tangible store of value over a digital alternative. For government money, the competitive situation is much more dire.

The Event Horizon [1,4,16]

Hyperinflation is a particular type of demonetization, unique to government fiat money, that did not exist under the gold standard. Hyperinflation occurs when a government produces new monetary units at an accelerating pace to finance expenditures or service debt burdens, which pushes the value of its currency down at the same accelerating rate. The value of a hyperinflating currency collapses against the most liquid goods available to the society first (like gold or the US dollar) and then, depending on relative availability, against real goods such as real estate and commodities. This sequence is caused by individual's attempting to maximize their exchange optionality as they escape their failing currency and prepare to navigate highly uncertain economic conditions. When hyperinflation intensifies, currencies begin falling against perishable goods. It is common to see grocery stores completely emptied out in societies suffering from the late stages of hyperinflation. Eventually, the society will either devolve to a barter economy or adopt a new medium of exchange, as we saw in Zimbabwe when its failing dollar was ultimately replaced by the US dollar. This process is arduous as the replacement currency is often scarce as foreign banking institutions are either reluctant to or restricted from providing liquidity.

As Bitcoin is the hardest form of money in existence, it will continue to appreciate against a backdrop of hyperinflating, soft government fiat currencies even without any increase in demand for Bitcoin (as illustrated in the above graphic). Eventually, this will lead to an inflection point in some economies where users rush to exit from their failing currency to get into Bitcoin to protect their wealth from further confiscation. This transition will have similar dynamics to other demonetization and hyperinflation events, however it will also be different given Bitcoin's unique properties as a monetary technology. A Bitcoin-induced currency demonetization is called a *hyperbitcoinization event* and is different from hyperinflation in two critical respects.

First, hyperinflation occurs with restricted competition with other fiat currencies, since a government can easily enforce capital controls that selectively prohibit

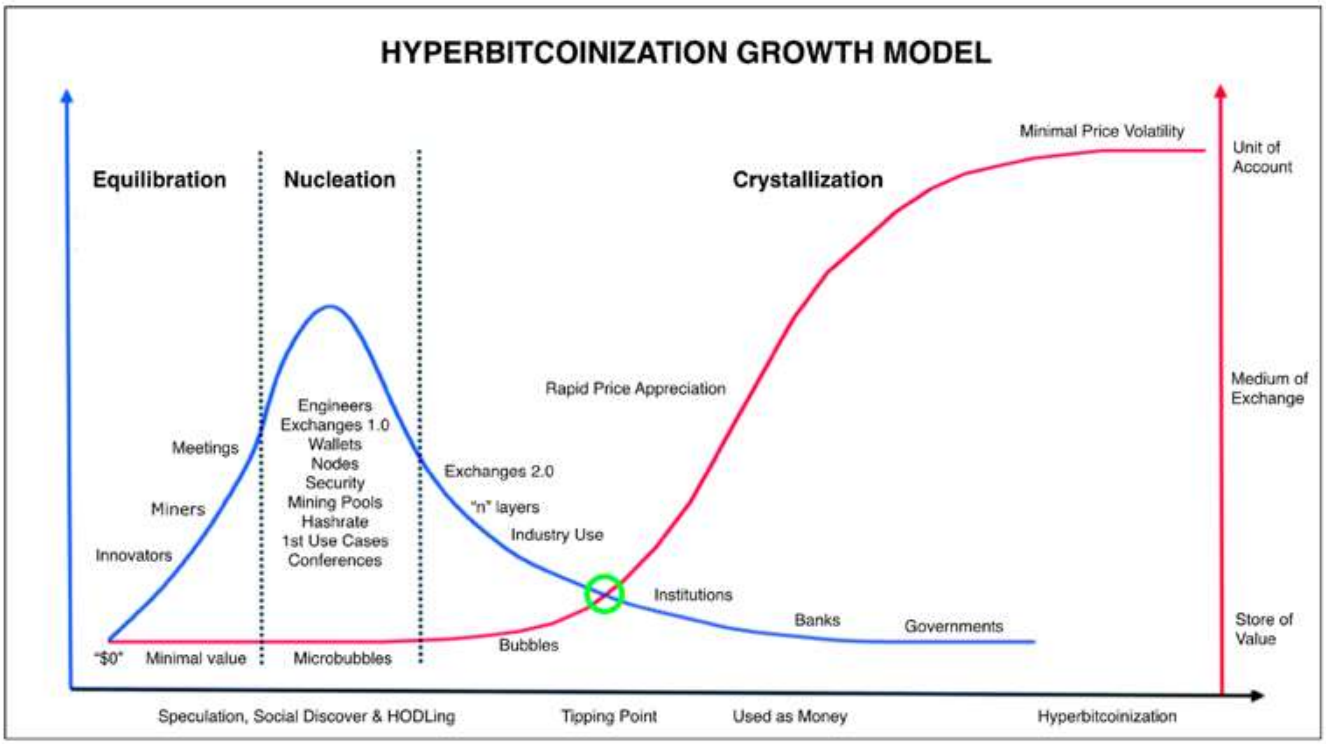
inflows or outflows of government money, whereas hyperbitcoinization occurs because of direct competition with Bitcoin, which can easily cross borders as it is immune to capital controls. This will cause hyperbitcoinization to happen much faster than a hyperinflation event, since governments will have great difficulty preventing Bitcoin trading within their borders due to its purely informational nature. Given governments' inability to shield their local currencies from direct competition with Bitcoin and the high opportunity cost of holding a depreciating form of money, once a hyperbitcoinization event reaches a critical mass it will happen quickly.

Second, in hyperinflation, the governments expand money supplies in an attempt to outpace people's inflation expectations. As governments forms a habit of inflating money supplies, people form a habit of anticipating rising prices and seek alternative stores of value. Governments, in turn, must print incrementally more money to stay ahead of inflation expectations and generate the same economic effect with each new monetary unit produced. With no alternative monetary media in which to escape, prices surge until a breaking point is reached. Hyperinflation is extremely disruptive to an economy as it forces people to switch from the worst form of government fiat money available to them to some other soft government fiat money (at best) or ends in total economic collapse (at worst). In hyperbitcoinization, users have a supranational monetary media in which to escape centrally planned economies. Therefore, a hyperbitcoinization event should be much less disruptive to the economy, as people will be trading in an inferior form of money for a superior one. Seeing as hyperbitcoinization should happen fast, people will quickly become accustomed to dealing in Bitcoin, which will protect deteriorating wealth and stabilize economic conditions.

Hyperbitcoinization will likely be a confusing, potentially chaotic, time for many people. Initially, it will probably occur at the periphery, with the countries inflating their currencies the fastest experiencing it first. Stories of this will spread quickly in the digital age and add to the believability of Bitcoin, all while it continues to benefit from the resultant increases in demand, network effects and the Lindy Effect. As more people wake up to the reality of hard money, we would expect the pace of this global transition to accelerate until all soft money is outcompeted into extinction. Fortunately, it will happen relatively quickly, since Bitcoin is immune to capital controls, and act as a stabilizing force for the world economy going forward (since hard money resists market distortions and remains firmly rooted in economic reality).

Like a star orbiting a black hole, any established monetary order that goes beyond the event horizon of hyperbitcoinization will inevitably collapse into Bitcoin's singularity.

Next, we show how a hyperbitcoinization event is likely to unfold:



Once Bitcoin's ecosystem is seeded a crystallization process begins. Growth becomes exponential and self-reinforcing. In this model, the tipping point (green circle) represents a dramatic change at which point many people and oganizations adopt Bitcoin.

The estimates of how valuable Bitcoin would become after global hyperbitcoinization vary based on what weighting is included for different stores of value (gold, government money, real estate, stocks, bonds, art, oil and other commodities are all used for this purpose today) but, using simple math for our directional analysis, if Bitcoin demonetizes just gold it would be valued at about $400K per coin ($8T/20M coins in 2025). If it demonetizes government money as well, it would be valued at about $5M per coin ($100T/20M coins in 2025). As awareness of Bitcoin and its potential impact spread, the long game becomes even more interesting. Considering Bitcoin represents an existential threat to government fiat money and central banks, we must also consider their decisions from a game theoretic perspective.

Reverse Bank Run [1,4,5]

Although it is still considered magic internet money by most people today, its continued existence and appreciation will attract more attention from high-net-worth individuals, institutional investors and then, possibly, central banks. As we have learned, central banks still rely on gold as a means of final settlement, as it was (before Bitcoin) the only monetary medium entirely free of counterparty risk (cash money). However, transporting and securing gold is an extremely expensive process fraught with operational risk. These costs and risks are the reason final settlements between banks occur very infrequently.

With the transaction throughput available on the Bitcoin network today, the global group of 850 central banks can perform daily final settlement with one another. With each central bank serving an average of 10 million customers, this would more than cover the entire world's population. In a world in which central banks adopted a Bitcoin standard, governments would no longer have the ability to increase the money supply and banks would begin to compete freely with one another by offering various physical and digital Bitcoin-backed monetary instruments and payment solutions. By using the technologies introduced by Bitcoin, cryptographic digital certainty can be applied to bank accounting and help expose those that engage in fractional reserve banking. This may lead to Bitcoin realizing its ultimate use case: the fastest and most efficient system for global final settlement across long distances and national borders. Despite the clear advantages of a system such as this, central banks are unlikely to give up their monopoly control over the existing monetary order willingly.

As people begin to voluntarily exit fiat currencies into Bitcoin to protect their wealth, as is already taking place in countries like Venezuela today, it will likely grab even more attention from central banks. As central banks are effectively losing customers, they will need to hedge the *going concern risk* posed to their business model. Central banks today hold reserves mainly in US Dollars, Euros, British Pounds, IMF Standard Drawing Rights and gold. These reserves are used to settle accounts and defend the market price of their respective currencies. Should Bitcoin remain on its current trajectory, and considering its superiority as a final settlement layer, it is possible that at least one central bank somewhere in the world will add Bitcoin to its reserves, if for no other reason than to defend the market price of its government fiat money, as is consistent with their strategy for gold.

The most likely scenario is that a central bank will seek to own part of the Bitcoin network as an insurance policy against it succeeding. Strategically, it makes sense for a central bank to spend a small amount acquiring some of Bitcoin's supply today. For example, consider that the authorities of a central bank today judge that, although chances of a hyperbitcoinization event are extremely remote, it would represent an extinction-level event for their business. Mathematically, using Bitcoin's approximate price today of $4K and its expected post-hyperbitcoinization price of $5M, unless the central bank is more than 99.92% certain that this event will NOT happen then it is prudent to allocate at least 0.08% of their assets into Bitcoin as a perfect hedge against its success (since price growth from $4K to $5M is a 1250x increase, an allocation of 0.08% of assets would keep a central bank at even-money should a hyperbitcoinization event play out).

Game theory tells us that the first central bank to buy Bitcoin will trigger a reverse bank run, as its decision will alert the rest of the central banks who will be compelled

by self-interest to follow suit. The first purchase by a central bank will cause the price of Bitcoin to rise significantly, causing others to move in based on their anticipation of future demand and compounding the effect as more central banks enter the market; making it progressively more expensive for later entrants. As central banks keep trying to anticipate the moves and strategies of one another, a game theoretic positive feedback loop will ensue that converges on a hard money Schelling point similar to that of free market monetary competition, thus triggering a global competition among central banks for maximal Bitcoin accumulation. A smart play for a central bank under the circumstances would be for it be the first to buy a small share of the Bitcoin network. An even smarter play would be for a central bank to purchase Bitcoin without announcing it, allowing it to begin accumulation at lower prices.

Similar to the transition to the gold standard in the 19th century, network effects would eventually take hold as more central banks bought some Bitcoin, increasing its liquidity and making it more marketable, thus creating ever-larger incentives for other central banks to join. After a sufficient minority of central banks have purchased part of the Bitcoin network, the minority rule will reach its final step and begin imposing the immutable rules of Bitcoin on the established monetary order. Once this reverse bank run on Bitcoin became public knowledge (as tends to happen easily in the digital age), it would be the ultimate seal of legitimacy for Bitcoin adoption and would add even more force to its ascent in the marketplace as this global game of Bitcoin accumulation would reach a fever pitch. Even at the largest scales of the financial system, Bitcoin converts individual self-interest into the growth of its network.

You may find this prospect hard to believe. About 25 years ago, handheld touchscreen supercomputers with wireless global interconnectivity were hard to believe too. Change keeps happening faster and faster. Remember, each central bank will value Bitcoin based on its appraisal of whether and how much other central banks will ultimately value it. As they will all be conducting the same strategic analyses, they will undoubtedly realize the dilemma they face—either ignore Bitcoin and watch it continue to outcompete and accelerate the failure rate of fiat currencies thereby loosening their control over the established economic order or choose to adopt Bitcoin as a reserve asset and trigger a game of accumulation against other central banks and legitimize it as an asset which will culminate in the loss of their monopoly position in the market for money. Operating in an adversarial environment, game theory tells us that so long as Bitcoin continues to operate in its current form, central banks (like the prisoners Alex and Bobby) will eventually be faced with strategic choices such as these to protect their own interests. At some point, the substantial advantage imparted to the central bank that moves first will

become an overwhelming incentive to at least one, causing it to be the first to make its move, thereby triggering the reverse bank run on Bitcoin.

A Path to Prosperity [1–16]

Making predictions is risky business, wrong answers are innumerable, and the right answer is singular. Accurate predictions are rare. By weaving together historical knowledge and awareness of current trends, one can develop a perspective on what technological innovations are possible. The biggest mistakes people make when making such predictions are:

- Forming an opinion on the innovative potential without considering it deeply (Blockbuster quickly reaching a decision to pass on buying Netflix for $50M)
- Disregarding an innovation because it contradicts a closely held worldview (Kodak refusing to accept the disruptive potential of digital photography as they spent 100 years building a business model centered on chemical film)
- Overlooking an innovation because it is too small or threatens a position of power (major newspapers refusing to develop an online presence early on)

Practicing a beginner's mindset and reasoning from first principles is critical for effective foresight. Pulling together everything we have discussed in this paper, we will now propose a potential path forward for Bitcoin based on the historical competitive dynamics of money, current macroeconomic trends and game theory. We will start from the inception of Bitcoin:

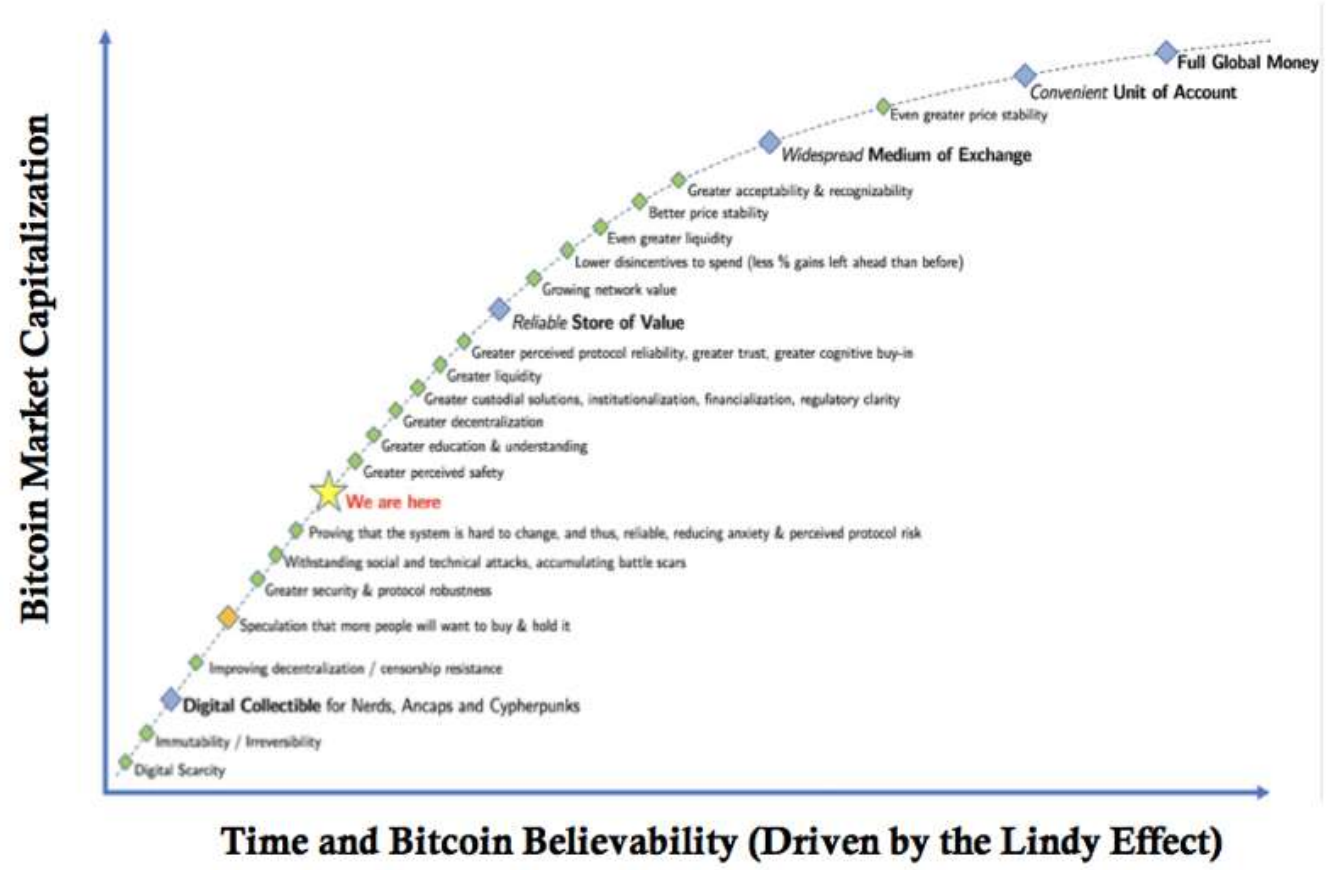
1. *Bitcoin is first perceived as an internet toy for cryptographers (Minority Rule — Step 1)*
2. *Its rapid price increase makes a small group of people rich, engages free market fanatics and brings media attention. Its hyper-volatile price presents itself early (Hodlers of Last Resort — Layer 1).*
3. *The media, financial and tech establishments — having failed to buy Bitcoin early and benefit from its meteoric rise — denounce it as a Ponzi scheme, the MySpace of Cryptocurrencies and the greatest bubble of all time (Streisand Effect).*
4. *A large number of scammers jump onto the Bitcoin hype-train and create their own cryptocurrencies claiming to be superior though lacking critical qualities including decentralization, security and immutable governance. Bitcoin's serendipitous first mover advantage, multi-sided network effects and its brand awareness fueled by the Nakamoto creation myth preserves its market dominant position.*
5. *Retail investors, venture capitalists and hedge funds — lacking understanding of monetary economics and applying inappropriate valuation models — invest into other cryptocurrencies, creating more noise and confusion as the prices of these altcoins increase at a rate higher than*

6. *Well-connected venture capitalists and hedge funds are given discounts on the investments only to then dump much of what they bought onto retail investors.*
7. *Given their high correlation to Bitcoin and lacking utility, the world watches as the bear markets continue to wipe out more and more alternative cryptoassets as most fail to deliver any useful product, although some succeed in other market spaces. Features that are proven in the market by other cryptoassets are subsumed by Bitcoin (Decentralized Network Archetype). Bitcoin price volatility persists but annual low prices continue to ascend relentlessly (Holders of Last Resort — Layer 2).*
8. *Trust in Bitcoin increases over time (Lindy Effect) and its market price continues its upward yet volatile trajectory (Fractal Wave Patterns).*
9. *People, burned in the altcoin craze, witness and learn about Bitcoin's undisputed superiority across all monetary characteristics, especially its hardness (Holders of Last Resort — Layer 3).*
10. *On the eve of and during the next bull markets, Bitcoin's absolute scarcity and antifragile characteristics exacerbate investor FOMO (Game Theoretic Positive Feedback Loop). Some investors are inevitably caught in the subsequent Bitcoin price crash (Fractal Wave Pattern)(Hodlers of Last Resort — Layer 4).*
11. *Hyperinflating fiat currencies are further contributing to the adoption of Bitcoin as it becomes the only means of preserving wealth for many people, making Bitcoin a legitimate store of value. Governments scramble to try and enforce capital controls and create propaganda against Bitcoin, just like they did to gold in the 20th century. Capital controls prove to be impotent and the propaganda against Bitcoin incites internet and media narratives that regard it as a tool for freedom (Antifragility). Government dissent highlights the need for Bitcoin in the first place (Streisand Effect).*
12. *Investors and high net-worth individuals are convinced to allocate a small portion of their assets into Bitcoin to capture further growth, hedge against inflation and increase the risk adjusted returns of their traditional portfolios (Minority Rule — Step 2)*
13. *Increases in demand for Bitcoin necessarily involve a reduction in demand for fiat currencies, causing even higher inflation rates (Gresham's Law). At great expense and effort, governments messily issue their own cryptocurrencies but fail to relinquish control over monetary policy, which makes them uncompetitive against Bitcoin (Market-Driven Natural Selection). Governments covertly attempt to attack the Bitcoin network, which only strengthens it (Antifragility). Media coverage about Bitcoin shifts towards its use as hard money (Skin in the Game) and its importance for prosperity (Hodlers of Last Resort — Layer 5).*
14. *Activists share the message that soft money creates social inequality (Soul in the Game) by disproportionately taxing the poorest via inflation (Cantillon Effect). This message spreads fast in a world of ever-more crashing fiat*

currencies and people rush to exit their local currencies for the safety of Bitcoin, triggering the first hyperbitcoinization events (Hodlers of Last Resort — Layer 6). Bitcoin mining hardware becomes commoditized and many citizens join mining pools (Decentralized Network Archetype)(Skin in the Game).

15. *Central banks, in an attempt to adapt to the new conditions and hedge going concern risks, quietly start to accumulate Bitcoin as a reserve asset, consistent with their gold strategy. A former central bank employee leaks a confidential strategy document regarding Bitcoin (Soul in the Game) which triggers other central banks to begin purchasing Bitcoin, causing its price and perceived legitimacy to increase at an accelerating rate (Game Theoretic Positive Feedback Loop)(Final Fractal Wave Pattern)(Hodlers of Last Resort — Layer 7).*
16. *Bitcoin's market capitalization reaches tens of trillions in US Dollar terms. Bitcoin's volatility subsides as both its market capitalization and liquidity are larger than ever (Mature Hard Money).*
17. *Early Bitcoin investors are now sitting on significant unrealized gains and are willing to part with some of their Bitcoin to pay for their purchases. With its purchasing power stabilized, the opportunity cost of transacting with Bitcoin is diminished and its use as a Medium of Exchange increases.*
18. *With the world more digitized than ever before, people increasingly demand to be paid in Bitcoin now that it has proven to be a good store of value given its disinflationary, and later deflationary, monetary policy (Schelling Point)(Hodlers of Last Resort — Layer 8).*
19. *With the addition of highly performant transaction layers, Bitcoin's use as a Medium of Exchange becomes a widespread. Bitcoin, functioning as the core of a new innovation wave called the TrustNet, is christened as a momentous innovation.*
20. *As more consumers and merchants become accustomed to transacting in Bitcoin, it gradually becomes used as a Unit of Account.*
21. *Due to the emergence of a superior, uninflatable monetary standard, people increasingly store their wealth in Bitcoin rather than fiat currencies (Minority Rule — Step 3)(Hodlers of Last Resort — Layer 9).*
22. *Central bank monopolies on money are described by historians as a relic of the past. Bitcoin is regarded as the catalytic innovation behind the separation of money and state. A free market for money is now the defining feature of free market capitalism (Nash Equilibrium).*

This path to full global money will take Bitcoin through many stages:



Time Will Tell

All time beyond the present is unknown. All predictions should always be taken with a grain of salt. The future is uncertain, and the end can always be near. Anyone who claims they can tell you what is going to happen in the future is wrong. All we can do is study the patterns of the past and use them as our map to navigate the ever-advancing territory of the future.

In a free market, hard money has always outcompeted soft money into extinction. Hard money has been the norm throughout all of human history, except for the past 100 years in which we have been coerced into using soft government fiat money. Societies operating on hard money systems optimize for the allocation of the ultimate resource, human time, which increases prosperity for everyone.

In the digital age, markets are increasingly interconnected. Bitcoin is digital cash money. It is a new social institution that lives in accordance with its own laws. Its core components are human self-interest and mathematics. Bitcoin is the hardest monetary technology in history. Will it continue to outcompete and win the throne of full global money?

Only time will tell.

Synthesized Works & Further Reading

- [1] *The Bitcoin Standard: The Decentralized Alternative to Central Banking* by Saifedean Ammous (a masterful work on which much of this essay is based)
- [2] *The Rational Optimist* by Matt Ridley
- [3] *Skin in the Game* by Nassim Nicholas Taleb
- [4] *The Bullish Case for Bitcoin* by Vijay Boyapati
- [5] *The Age of Cryptocurrency* by Paul Vigna and Michael J. Casey
- [6] *Sapiens* by Yuval Harari
- [7] *Bitcoin is a Decentralized Organism, Part 1 and Part 2* by Brandon Quittem
- [8] *PoW is Efficient* by Dan Held
- [9] *The Fifth Protocol* by Naval Ravikant
- [10] *Unpacking Bitcoin's Social Contract* by Hasu
- [11] *Antifragile* by Nassim Nicholas Taleb
- [12] *Letter to Jamie Dimon* by Adam Ludwin
- [13] *Placeholder VC Investment Thesis Summary* by Joel Monegro and Chris Burniske
- [14] *Diffusion of Innovations* by Everett M. Rogers
- [15] *Why America Can't Regulate Bitcoin* by Beautyon
- [16] *Hyperbitcoinization* by Daniel Krawisz

A Conflict of Crypto Visions

Why do we fight? A framework suggests deeper reasons

By Yassine Elmandjra and Arjun Balaji

Posted January 29, 2019

Conflicts raging within "crypto" are endless. Heated debates take place on a wide spectrum of issues, with little attempt to devise compromises acceptable to both sides. Interestingly, it is the same people who consistently position themselves on opposite sides of these issues. From monetary maximalism and wealth distribution to governance and consensus algorithms, the issues vary tremendously while the formed groups of opposition remain the same. Naturally, this creates an unproductive habit of each side blindly talking past the other.

In *A Conflict of Visions* and *The Vision of the Anointed*, political economist and social theorist Thomas Sowell argues that this phenomenon comes from fundamental differences in people's assumptions about the nature of systems and their

limitations. While seldom consciously recognized, these sets of assumptions are the largest drivers influencing people's opinions. Since visions are rarely examined but have profound impact, Sowell introduces the "conflict of visions" as a mechanism to think about these assumptions.

By highlighting how these assumptions play a fundamental role in shaping our views, we shed light on the "conflict of visions" and ideological battles raging within proponents of cryptocurrencies.

We begin our analysis by laying out the framework of conflicting visions. Using this framework, we proceed to explain the conflict of ***"crypto"*** visions. From an understanding of the conflict of crypto visions, we then comment on the structure of arguments taking place within crypto, before diving into the meat of our analysis: an exposition of four episodes exemplifying the conflict of crypto visions.

Setting The Scene

- I. Defining Visions
- II. The Conflict of "Crypto" Visions
- III. The Structure of Arguments

Episodes

- IV. Episode 1: Monetary Maximalism vs. Multicoinery
- V. Episode 2: The "Fairness" of Crypto Distribution
- VI. Episode 3: Governance
- VII. Episode 4: Proof-of-work vs. Proof-of-stake
- VIII. The Future Remains To Be Built

Defining Visions

In order to understand the conflict of "crypto" visions, it is important to first establish *what a vision is* per Sowell's work. Simply, a vision is a gut feeling about how things *should* work—a set of assumptions about the limitations and nature of the world that enables someone to understand (or at least believe to understand) why things work the way they do. Sowell defines two opposing sets of assumptions and assigns them the terms "constrained" and "unconstrained."

Constrained Vision

At the core of each vision is some strong belief or recognition of limitations. Those with a constrained vision see certain realities as unalterable, "scarcity, self-interest, human fallibility, evil." [1] Under the constrained vision, the only way to improve is to

understand the fundamental laws of nature and the only way to innovate is to remain consistent with the specific parameters set forth by these laws.

The constrained vision realizes that while A may be better than B, it does not matter if A simply cannot be done. For instance, while achieving flight by wishing away gravity or ending war by wishing away violence would be great, it is simply not within the realm of possibilities. Consistent with the constrained vision are concepts like Smith's Invisible Hand and Zhuangzi's Spontaneous Order, which recognize the limitations of man and prescribe ideas that transform these limitations into progress.

The constrained vision encourages decision making by identifying tradeoffs rather than solutions. Given the limited options available, the constrained vision attempts to make the best trade-offs with an understanding that "unmet needs" will necessarily remain. As such, "particular solutions to particular problems are far less important than having and maintaining the right processes for making trade-offs and correcting inevitable mistakes." [2]

Unconstrained Vision

Those with an *unconstrained* vision believe that the only limitation to achieving a desired outcome is our lack of imagination. Through this lens, the underlying problems in any system exist only because people are not wise, caring, imaginative, or bold enough: with the right mindset, scarcity can be eliminated, man's self-interest can be corrected, imperfections perfected, and all evil eradicated. Instead of building mechanisms to work around any fundamental limitations, the unconstrained vision sees it possible to re-engineer the world to eliminate its flaws. As such, "intractable problems with painful trade-offs are simply not part of the unconstrained vision." [3]

The questions posed under the unconstrained vision are centered around how to remove particular negative features in an existing situation to create a solution. By doing so, decision making boils down to choosing the perfect solution instead of identifying tradeoffs. With the right innovation in place, few, if any, sacrifices must be made to achieve a particular improvement. In the unconstrained vision, questions of feasibility are not of primary concern, as trade-offs merely reflect varying scales of preferences and circumstances among individuals.

In both cases, regardless of the assumptions held, the desired outcome remains the same. **The goal in both visions is to create the best possible outcome.** As these assumptions are so fundamental to decision making, very rarely is there agreement on how to achieve desired outcomes. Both visions acknowledge that the world has unlimited desires and believe there to be an optimal way to accommodate for these desires.

As the labels “constrained” and “unconstrained” suggest, one vision acknowledges that we cannot get everything we want (constrained) and the other affirms our potential to be limitless (unconstrained). It should therefore come as no surprise that each vision reaches opposite conclusions on how to accommodate for a desired outcome.

The Conflict of “Crypto” Visions

With this framing in mind, it is easy to begin to see how many of crypto’s major intellectual fault lines lie along the constrained/unconstrained divide. The space is nascent: a large canvas with a massive surface area for experimentation and tens of thousands of participants, each with their own distinct end game.

In the absence of widespread adoption, participants fall back to narrative. When defining these narratives, we see intra-blockchain divides—is the end vision of “crypto” a hyper-capitalist Galt’s Gulch or a radical markets-inspired disintermediated society (or both)? Even inter-blockchain narratives are inconsistent as we’ve seen narratives around Bitcoin and Ethereum transform over time.

This post builds on prior work from Nic Carter and Hasu exploring Bitcoin’s evolving narratives (and Felipe Pereira’s similar efforts with Ethereum). While researchers have focused on describing how narratives have evolved over time, less analysis has been done to frame these evolutions in context: are these evolutions simply opportunistic, the result of shifting commercial (and investment) opportunity in the cryptocurrency ecosystem, or do they reflect more fundamentally disjointed philosophical orientations?

The most salient distinction people have made, between “money crypto” and “tech crypto”, is a good starting point but incomplete. In our view, these distinctions don’t come down to “Silicon Valley” v. “cypherpunk”—many cypherpunks are not strong advocates of base-layer privacy and many SV entrepreneurs are wary of the “move fast and break things” culture of their peers—these distinctions are more foundational, reflective of constrained and unconstrained views of the future that technologies can help build.

The Structure of Arguments

Hasu's model of Bitcoin's_ _social contract_ _illustrates the dualistic relationship between the social contract and implementation details in public blockchains.

Virtually every debate about cryptocurrencies happens at the social layer. This is for good reason, given the nature of the network governance models many public blockchains follow, decisions around consensus often reinforce precedents for the future. As such, design is approached carefully and with thoughtful consideration in some major historical debates:

- Is it possible to have a sustainable long-term security model with a fixed money supply (v. mild or high inflation)?
- How important is programmability and expressiveness considering the increased attack surface and increased security cost?
- Is "absolute" base-layer privacy worthwhile if it increases the difficulty of verification of the money supply (or requires greater trust in the issuers or maintainers of the system)?
- Is increasing the block-size—lowering transaction fees and allowing full node cost to scale up linearly—a short-sighted decision given the uncertainty of future advancements?

These debates are rarely presented as such. Rather than presenting ideas as a question of tradeoffs, discourse—whether in a tiny Telegram chat or on stage at a conference—devolves into religious fervor and ad hominem. Cryptocurrency prices serve as a real-time scoreboard for winning narratives, with ownership creating bias as people "shill their bags" in the face of presenting debates with nuance.

Much of the debate ends up substituting opaque proclamation for arguments. Enthusiasts fall back to simple quips and vacuous rhetoric—technical features that are favored and already exist are "here to stay" while proposed features are

"inevitable." Unpopular existing features are "obsolete" and unpopular, ambitious pitches are "unrealistic."

To see through this vacuous rhetoric, Sowell suggests applying general principles of common sense (which are nevertheless often ignored) illustrated below:

1. All statements are true, if you are free to redefine their terms
2. Any statistic can be extrapolated
3. A can always exceed B if not all of B is counted or if A is exaggerated
4. For every expert there is an equal and opposite expert, but for every fact there is not necessarily an equal and opposite fact.
5. Every policy is a success by sufficiently low standards and a failure by sufficiently high standards.
6. Most variables can show either an upward trend or a downward trend, depending on the base year chosen.
7. You can always create a fraction by putting one variable upstairs and another variable downstairs, but that does not establish any causal relationship between them, nor does the resulting quotient have any necessary relationship to anything in the real world

A careful examination of Sowell's principles sheds light on the lack of thoughtful consideration that much of "crypto" debate is predicated upon.

Episode I: Monetary Maximalism vs. Multicoinery

First, we only had Bitcoin, released by Satoshi, who by all evidence was likely an outsider to the establishment. As Bitcoin was strictly focused on offering a new electronic cash system without the reliance of a trusted central mint, the utmost focus of enthusiasts and developers has always been security (of the codebase) and security again (of the monetary policy). Historically, changes to Bitcoin have been debated not just on their merits but in their second and third-order effects on security.

The original grassroots cypherpunk movement of Bitcoin was never focused on "blockchain technology". To this day, the majority of "Bitcoin maximalists" or "shitcoin minimalists" see Bitcoin's focus as a grassroots bottom-up effort in engineering in stark contrast to the more formal top-down efforts employed by projects like Ethereum, Tezos, and others.

Inspired by the view of Austrian economists, Bitcoiners have historically opted for a "simplistic" & "adversarial" view of the world, grounded in an understanding of

monetary history: that the “killer app” is money and that Bitcoin, a potential global money competitor, has the largest potential TAM. In their view, other projects attempting to create a better Bitcoin and iterate on its “fundamental design limitations” misunderstand its intended use.

What Bitcoiners attack with historicism, multi-coiners defend with vision, often criticizing this limited, “simplistic” view held. The unconstrained vision believes it to be “a major failure of imagination (or really just plain observation, frankly) to think that crypto has nothing more to offer than a slow and volatile form of sound money.”

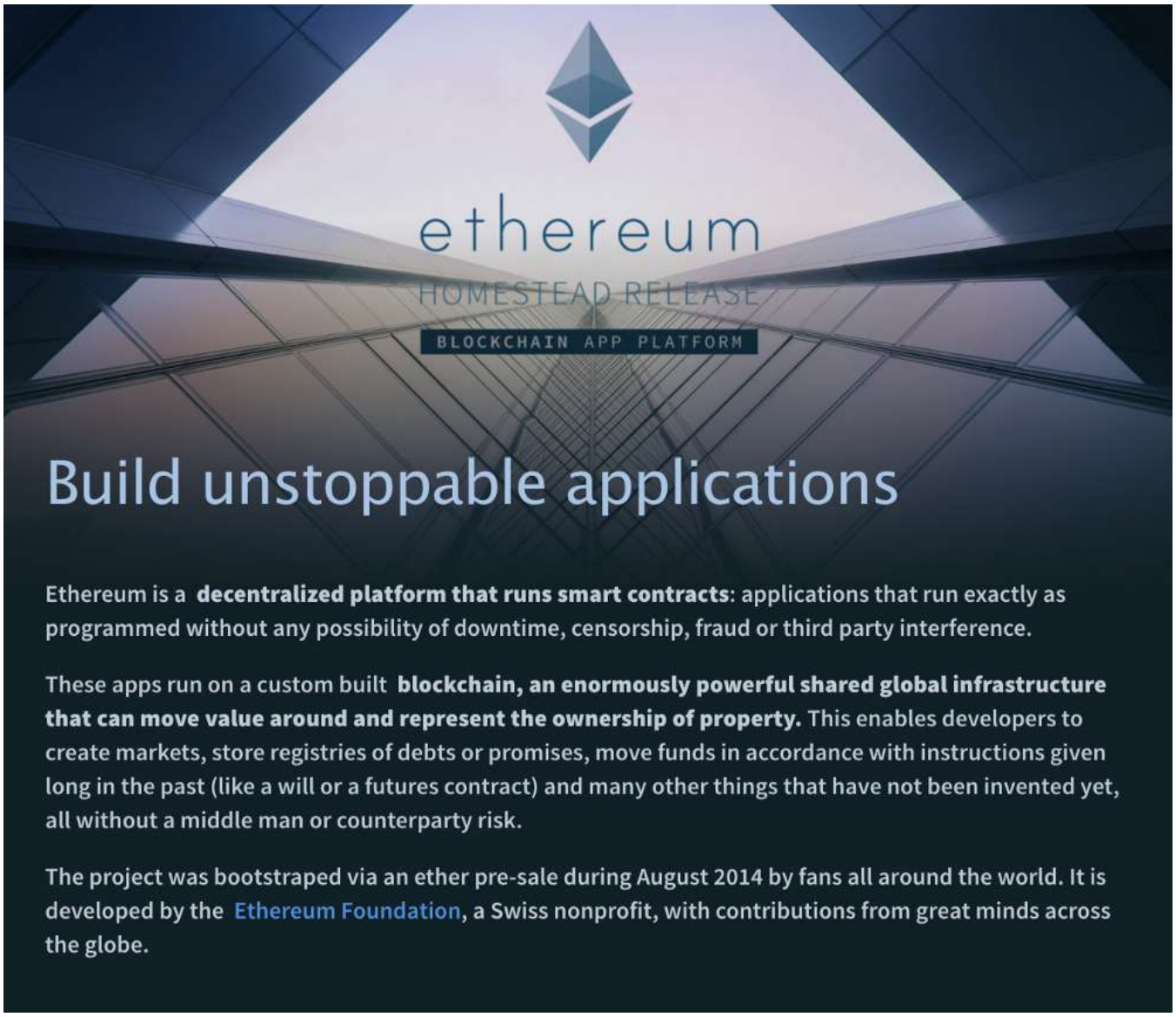
Under these sets of unconstrained assumptions, Bitcoin might instead be described as a part of the “calculator era” of cryptocurrencies, as recently explained by Andreessen Horowitz partner Jesse Walden:

Many argue that that the most important property of a decentralized money system is security, not programmability, and that a limited scripting language is thus a feature, not a bug. Through that lens, we can view Bitcoin as more of a calculator than a computer (and that is intended as a positive remark!). **It is purpose built and good at its task, but for developers keen to tinker and build new applications an evolution to a new architecture was required.**

To people biased with an unconstrained view of the world, Bitcoin suffers from a lack of vision. As such, the same feature (e.g. complex programmability) might be viewed by the constrained vision as a bug and by the unconstrained vision as a feature. Sowell (135) clarifies this distinction:

To those with the unconstrained the question is: What will remove particular negative features in the existing situation to create a solution? Those with the tragic vision ask: What must be sacrificed to achieve this particular improvement?

On the other hand, to the constrained vision **there are no solutions, only trade offs** . Bitcoin developers like Jimmy Song argue that blockchain technology comes with significant tradeoffs ranging from the high costs of development and maintenance, to the challenges of coordinating complex incentives across many parties. Bitcoiners view capital-b “Blockchain” and “tokenization” advocates as missing the point: with a distributed ledger hammer, every incentive problem looks like a nail.



Ethereum's marketing from late 2016 proposed "unstoppable applications", enabling developers to do lots of things, many of which have not been invented yet. While Turing Completeness may have its advantages, it does not come without significant tradeoffs.

Many Silicon Valley investors have historically thought of the killer app of blockchains as creating new markets, with Naval Ravikant famously noting that blockchains can replace networks with markets. Pantera Capital CIO Joey Krug sees disintermediation of traditional companies as a core part of their "blockchain technology" thesis, suggesting that in their strongest form, blockchains can create marketplaces in industries far from financial services, massively up-ending traditional businesses in the process:

Blockchain tech is good for multi-sided marketplaces—particularly for finance. Other use cases, which really just converge with financial markets, include: file storage markets like Filecoin; computational markets; markets for items in video games; namespaces like Handshake; regular betting/gambling like FunFair; and sharing economy protocols like Origin. **These projects will fuel a classic disintermediation play: cut out the existing profit-seeking corporations and replace them with software. As software eats the world, software is eating software.**

Silicon Valley's bias for the unconstrained view is straight-forward. By defining networks like Bitcoin as software-first, the role of the technologist precedes that of a monetarist. As such, "blockchain" simply becomes one amongst a number of emergent platforms in the ever-evolving internet infrastructure (Web 3.0). In "What comes after open source?", Andreessen Horowitz's Denis Nazarov elegantly explains this view:

Years of state accumulated by innovative companies produced tremendously useful services (search, maps, social, commerce), but further combinatorial innovation is off-limits to outside developers and entrepreneurs. **Rebuilding services from scratch on the same terms and this late in the game is hopeless.**

As crypto networks evolve, they are likely to provide strong incentives to unlock further state and create open services in many areas dominated by closed ones today. **Open services powered by crypto networks will present unprecedented opportunity for a new generation of developers and entrepreneurs to innovate.**

The Use of Language

The technologist's articulation of the potential of blockchain technology rejects current constraints with a bias to technological progress. Not seeing this vision is often attributed to a lack of imagination on the part of the "doubters." Who could've seen the potential of the internet in 1995 given the nascent state of internet architecture or the explosion of mobile applications transforming the world given the limited capabilities of the first iPhone? Sowell clarifies:

Intractable problems with painful trade-offs are simply not part of the vision of the unconstrained. **Problems exist only because other people are not as wise or as caring, or not as imaginative and bold, as the unconstrained.**

This is visible even in the linguistic choices of the unconstrained view, with Sowell noting that "the vocabulary of the unconstrained is filled with words reflecting their rejection of incremental trade-offs and advocacy in categorical solutions."

More generally, the use of language becomes a strong reflection of an individual's views. The term "shitcoin minimalist", for instance, indicates a constrained view of the potential of blockchain-based solutions to human problems.

The term "Bitcoin maximalism" itself was a derogatory claim made by Vitalik Buterin, who started Ethereum after categorical rejection of his proposals to materially expand the available feature set on Bitcoin. It has since been weaponized, with Vitalik noting that "I do wish ill on *bitcoin maximalism*, but only because bitcoin maximalism as an ideology seeks elimination of all non-bitcoin platforms." While the term has been co-opted by Bitcoiners to reflect a descriptive monetarist view rather than a prescriptive ideology, it is still a major point in the multi-coiners sieve to discount Bitcoiners' claims, with Vitalik clarifying his view, even going so far as to *use* the word "constrain":

Because **I view single-coin maximalism as an oligarchic rent-seeking ideology that seriously *constrains* the possibilities of cryptocurrency innovation** and makes it dependent on a political process (Bitcoin governance) rather than market competition?

Sowell preempts this conflict in his work, clarifying that "the anointed often place permanent labels on people, on the basis of transient circumstances" in order to more solidly position themselves as the underdog, fortifying "us v. them" dynamics. These labels aren't useful—the interests of a few "toxic" Bitcoiners don't reflect the views of most bitcoin holders, who are not even aware of the nuances of online cryptocurrency discourse.

Bitcoiners push back on this unconstrained view further, noting that they are largely divorced from science. Even the strongest proponents of the unconstrained view acknowledge the delta between the realities of today's technology and appeal to tomorrow's, with Walden further noting:

How exactly this will work is very much in the realm of open research. Proponents of "server era" architectures posit that a "cloud era" experience will emerge through standardization and abstraction of inter-blockchain communication among heterogeneous blockchains. Others, like Ethereum 2.0 (Serenity) and Dfinity, are converging on sharded versions of homogenous, turing-complete chains. And still others are researching entirely new architectures that move computation off-chain.

Through the lens of technological utopianism, or nirvana fallacy, feasibility is an after-thought to be attacked by a portfolio of diversified bets—the venture capital model—rather than an exploration of tradeoffs in an ever-exploding design space.

Episode II: The "fairness" of crypto distribution

Since the very beginning, debates about the "fairness" of various cryptocurrencies have sparked fiery conversation about what future wealth distribution should look like. This is expected—if cryptocurrencies actualize the full cypherpunk vision for the future, they represent one of the greatest wealth transfers of all time. With discussions of current income inequalities dominating global discourse, the potential for cryptocurrencies to exacerbate existing problems have been top of mind for many.

Over the years, there have been many attempts to quantify this disparity, including Balaji Srinivasan's work exploring different networks' Gini coefficients. These research efforts have sparked outrage from cryptocurrency enthusiasts and external critics alike, including:

Dogecoin creator Jackson Palmer:

The institutionalization of cryptocurrency will heavily re-centralize both power structures and token distribution. So you can say goodbye to much of the original vision for the technology.

Cryptocurrency analyst Ferdous Bhai:

80%+ Bitcoins have been distributed. 1) What type of people own these coins? 2) Do we want to enrich these holders via hyperbitcoinization? 3) Will the Bitcoin-rich use their wealth for good, or will they continue to oppress and exploit? Nobody talks about this.

Additionally, NYU professor and notorious cryptocurrency critic Nouriel Roubini remarks that "the inequality coefficient of BTC is worse than North Korea that has the worst inequality on earth."

This conflict is another example of the strain between bottom-up constrained views of Bitcoiners, who believe attempting to design "ideal" wealth distribution is futile, and critics, who believe that Bitcoiners are "unfairly" rewarded for their early adoption. Defenders of the constrained view maintain that Bitcoin's purpose is simply offering a non-sovereign money alternative—explicitly money that is designed *not* to be confiscated or debased—and that the distribution of bitcoins is perfectly calibrated by the free market to reward investors based on their place in the risk curve. Some further argue that given empirical suggestions that ownership concentration turns over with market cycles, concern over distribution is excessive—a problem solved by free markets.

Where holders of the unconstrained view project their desire for a certain wealth distribution in society, the constrained view clarifies that this is a violation of Bitcoin's single purpose: preventing forced wealth redistribution. Sowell, once again, thoughtfully comments on wealth disparities in practice:

If one believes that income and wealth should not originate as they do now, but should instead be distributed as largess from some central point, then that argument should be made openly, plainly, and honestly. But to talk as if we currently have a certain distribution result A which should be changed to distribution result B is to misstate the issue and disguise a radical institutional change as simple adjustment of preferences. The word 'distribution' can of course be used in more than one sense.... **What is really being said is that numbers don't look right to the [unconstrained]–and that this is what matters, that all the myriad purposes of the millions of human beings who are transacting with one another in the marketplace must be subordinated to the goal of presenting a certain statistical tableau to [unconstrained] observers.**

Despite this, conflicting visions persist. More ambitious experiments than ever are being pushed, including attempts to create "UBI via mass airdrop" or Bitcoin-alternative money systems specifically designed to prevent long-time wealth hoarding. Subscribers to the constrained vision push back against these forms of idealism with practicality: despite having good intentions, early iterations of these systems are often naively designed and ignore the second or third-order effects of top-down incentive manipulation. In many cases, these policies could end up hurting those they purport to help by creating gamifiable or broken incentives that exacerbate existing inequalities.

Episode III: Governance

The meta-problem of open-source protocol governance has been a longstanding debate where a fault line can once again be identified along the constrained and unconstrained divide.

The constrained vision believes that optimal governance is achieved through a bottom-up approach that attempts to minimize subjectivity and maximize trustlessness, while the unconstrained vision believes optimal governance is achieved through a formalized on-chain approach that interfaces with existing, top-down legal frameworks.

Nick Szabo's mental model of wet code and dry further illustrates the nature of these conflicting visions. At the highest level, "wet code" is interpreted by humans, and "dry code" is interpreted by computers. Examples of wet code include law and traditional contracts. Examples of dry code include smart contracts, secure property titles, and the domain name system. Human language might be somewhere in between wet code and dry: if a computer program is able to translate text to multiple languages, for instance, human language may be considered dry.

The distinction between wet code and dry raises questions around the extent to which formalizing governance is possible without exposure to human subjectivity. If wet code is inherently human-readable and dry code computer-readable, the constrained vision would posit that transforming a wet code legal system into dry code would not only add additional complexity but also introduce elements of human subjectivity.

Because the specifics of law and governance are complex and unknowable, the constrained vision opposes fully formal on-chain governance: implementation of "law as code" becomes heavily subjective and unlikely to account for the unpredictable changes in the real world.

Since avoiding human subjectivity and maximizing a network's trustlessness is the constrained vision's top priority, "law as code" becomes unattractive. As Bitcoin Core developer Matt Corallo highlights, "trustlessness is the ability to use Bitcoin without trusting anything but the open-source software you run." The constrained vision posits that a formalized governance system, which adds unyielding subjectivity *to* the open-source software, would come at the cost of automated integrity and trustlessness.

Through formalized on chain governance, changes to dry code are completely arbitrary, a reality the constrained vision avoids by prioritizing and questioning the process first. As Sowell suggests:

To those with the vision of the anointed, it is simply a question of choosing the best solution, while to those with the tragic vision the more fundamental question is: Who is to choose? And by what process, and with what consequences for being wrong?

A software's formal governance system is created from a dry code implementation of something that is inherently wet code. As a result, the control and trust of the software transfers to humans. Under the unconstrained vision, humans *should* be able to change a network's implementation in an ongoing fashion, as humans are the final arbiters of truth. As such, the vision pushes back on the subjective claim that trust-minimization through software automation is optimal, refusing to accept such a claim as "law."

In practice, under the constrained vision, automated governance is limited to maintaining the set of verification rules, as seen in Bitcoin's governance model. In the case of a failure in a wet code process, such a system would resort to a fork, a change in the protocol influencing the validity of the set of rules. Since forks are seen as bugs to the unconstrained, the value proposition of an on-chain governance system is that it precisely avoi *ds* forks and encourages high upgradeability. However, by formalizing governance, the risks of undergoing a fork under what at the time would have been considered to be a perfect implementation may potentially speak to the

subjective nature of the implementation. For the long term sustainability of the protocol, the constrained vision posits this to be detrimental.

Episode IV: Proof-of-work vs. Proof-of-stake

Bitcoin's proof-of-work is an embodiment of the constrained vision, a mechanism to work around fundamental limitations rather than re-engineer them. First explained by Nick Szabo in *Money, blockchains, and social scalability*, Bitcoin's proof-of-work accommodates our cognitive limitations and behavior tendencies by making a necessary and intentional tradeoff: **greatly sacrificing computational scalability to improve social scalability.**

A feature to the constrained, a bug to the unconstrained.

The ability to participate in an "institutional technology" is predicated on the technology motivating participation and protecting the system and its participants from malicious activity. By improving social scalability, which proof-of-work does so effectively, the number of people who can beneficially participate in the system is maximized. Therefore, the constrained, "proof-of-work" vision posits that Bitcoin's success should not be determined by its computational efficiency but by its ability to increase social scalability through trust minimization.

What the unconstrained vision deems computationally inefficient and unscalable, the constrained vision not only deems an intended tradeoff, but a fundamental feature: specialized, dedicated hardware *should* perform a function whose sole output is to prove that the computer *did* indeed execute a costly computation. As Nick Szabo highlights, "prolific resource consumption and poor computational scalability unlocks the security necessary for independent, seamlessly global, and automated integrity."

While an implementation of both computational and social scalability is optimal, the constrained vision acknowledges that it cannot be done without compromising security. Embedded in computer science is a fundamental understanding of tradeoffs in security and performance where inevitably, automating integrity requires high resource utilization. Even with breakthroughs in computer science, the constrained vision recognizes that total integrity and absolute trustlessness is infeasible, making the delicacy of explicit and intentional tradeoffs all the more imperative. As such, the constrained vision fully accepts that such tradeoffs are unavoidable, and "it is probable no such big but integrity-preserving performance improvement is possible." [4]

To the unconstrained vision, the assumptions around proof-of-work are entirely different. Instead of asserting that proof-of-work sacrifices computational inefficiency

for social scalability, the unconstrained vision asserts that proof-of-work unjustifiably consumes significantly more resources than it creates, making it a wasteful and archaic system in dire need of improvement.

A commonly used statistic the unconstrained vision employs to illustrate proof-of-work's "wastefulness" is a measurement of the amount of energy the system expends as a proportion of the total transaction volume the system processes. By employing such a statistic, it becomes obvious why under the unconstrained view, proof-of-work is so scandalously inefficient: "Bitcoin consumes five Hiroshima's worth of energy per day" only to process "a mere fraction of what a payment service like Visa processes."

The use of this argument to illustrate proof-of-work's wastefulness implies that trust minimization is not viewed as a necessary feature in the unconstrained vision. If it were, comparing Bitcoin to Visa would be futile: **Visa does not provide the same improvements in social scalability through trust minimization *precisely because* it is more "computationally efficient".** Such a comparison not only dismisses the existence of limitations, but attempts to associate two completely unrelated variables (i.e. energy expenditure and transaction volume are not functions of each other). As Sowell highlights, wrongful association of these variables leads to "statistical extrapolation without any analysis of the actual processes from which these numbers were generated." [5]

A costless alternative?

Deeming proof-of-work wasteful suggests a cheaper, more prudent alternative exists. To the unconstrained vision, the reason proof-of-work has not fully succumbed to an alternative may come from a lack of care for the environment or a lack of imagination of technological advancements as Emin Gun Sirer suggests:

100 years from now, future generations will talk about the PoW craze with the same bemused view we hold for other mass manias. The absurdity of wasting energy to make chicken scratch marks on an electronic ledger is going to become more obvious. We are going to look back the same way we look at the use of CFCs and leaded gasoline. We should replace it with systems that can do better.

As previously highlighted, the unconstrained view is to remove specific negative features in the existing situation to create a solution. In the context of proof-of-work, the question posed by the unconstrained is then: "how can we ***remove*** the computational inefficiency and energy wastefulness of proof-of-work to create a better sybil-control mechanism and consensus algorithm?"

Attempting to answer this question, mechanisms like proof-of-stake have emerged as the most popular solution, as Ethereum's Vitalik Buterin highlights:

"The philosophy of proof-of-stake is not 'security comes from burning energy', but rather 'security comes from putting up economic value-at-loss'.

In a proof-of-stake system, a blockchain appends and agrees on new blocks through a process in which anyone who holds coins inside of the system can participate and the influence an agent has is proportional to the number of coins (or 'stake') it holds. **This is a vastly more efficient alternative to proof-of-work 'mining' and enables blockchains to operate without mining's high hardware and electricity costs."**

Under the unconstrained view, proof-of-work is classified solely as a sybil-control mechanism. As such, there is greater justification for removing energy spend on coin production. Emin Gun Sirer explains:

The energy spent on coin production is purely wasted, it provides no price floor for coins, it is value leaked out of the system. Much like how the high cost of printing Bahts doesn't guarantee value higher than USD. It's just the cost of competition between miners.

Thus, the goal in the unconstrained vision is to implement an inherently costless system without leakage. In proof-of-stake, network participants are not required to use inordinate amounts of energy to maintain ledger immutability, significantly reducing labor intensity. A reduction in labor intensity would be more fair and help encourage community participation due to lower barriers to entry. Specifically, the unconstrained vision claims that taking mining out of the hands of entities with access to excessive amounts of low cost energy would help redistribute the work evenly and lead to a more democratized system. By removing the feature that secures value in a proof-of-work system, security in turn is derived from the value stored *within* the system itself. As David Yakira notes, "in a sense, a PoS system is recursive, augmenting the value it stores implies better security which further allows the value to increase and so on."

Under the constrained vision, however, defining proof-of-work as merely a sybil-control mechanism is non-exhaustive and trivializes its purpose. Proof-of-work is also seen as essential for maintaining unforgeable costliness "giving digital blocks real-world weight" and enforcing a predictable, meritocratic distribution mechanism.

Because the constrained vision believes there to be "no solutions, only tradeoffs," a costless mechanism without leakage would also be definitionally impossible, as Paul Sztorc notes:

"Switching the payout-trigger to a social or political dimension would merely transpose the work-expenditures correspondingly to the realms of bribery and propaganda.

If an object has value, people will spend effort to chase it, up to whatever the object is worth (MC=MR). This effort is also "work". [Thus], a stable solution to these problems is ***definitionally impossible***, as there is always an incentive to work until marginal cost equals marginal revenue."

The Future Remains To Be Built

As we've highlighted, these divisions between cryptocurrency enthusiasts, investors, and builders can be seen across the "unconstrained" and "constrained" axes, two conflicting ideologies that transcend geography, professional associations, or backgrounds.

We believe that the most likely outcome after the full possible actualizations of these visions is convergence in some form. While the future remains uncertain, a conflict of *visions* persists because in reality, visions are all we have to focus on ahead of a multi-decade roadmap of adoption and integration.

The dominant visions of the constrained view are not mutually exclusive with the more abstract unconstrained view. While on the surface, inter-currency battles persist, the final boss (third party disintermediation)—which unites everyone alike—is shared. Though differences emerge upon squinting, high-level goals are not divergent. Privacy-aware cypherpunks want to see the destruction of ad-driven technology monopolies and Bitcoin remains a useful tool against tyrants independent of political, social, or religious affiliation. While cryptocurrency adoption appears zero-sum, experimentation is at the core of open-source and expands the size of the pie in the short-to-medium term by bringing new entrants to the market with disparate views while concurrently validating existing implementations.

It may be that for creating a global money, only a tightly constrained, focused view can prevail as launching a system mimicking a Swiss bank in your pocket requires this level of carefulness. If indeed blockchains represent a major evolution in computing, those systems may follow an evolving philosophy closer to a traditional software release cycle with constantly iterated release cycles.

These debates will be reminisced upon like early internet debates about the ideal protocol standard or intranets and the Internet (earlier generations' blockchains v. bitcoin) or debates even further back about the viability of inferior monetary metals to gold. Ultimately, winners will emerge out of today's conflicting visions invoking "how did we not see that coming?" commentary in the process.

For now, the future remains to be built.

Disclaimer:

THANK YOU, CREATORS.

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

This Journal does not contain reference to any of the investment products or services currently offered by members of the any specific business, that means any business I am associated with. Bitcoin, shitcoins, and related technologies can be volatile, Don't fuck around with this stuff because you might get burned.

Bitcoin has paved the way for some VERY radical technology AND it's very confusing. Read more. Ask questions. The purpose of this Journal is to provide archive and curate the best commentary and culture in the bitcoin space.

This Blog Post fairly represents the opinions and sentiments of its author at the date of publishing but it should be noted that such opinions and sentiments may be revised from time to time, for example in light of experience and further developments, and the blog post may not necessarily be updated to reflect the same.

Nothing within this Journal constitutes investment, legal, tax or other advice. This Journal should not be used as the basis for any investment decisions which a reader may be considering. Any potential investor in bitcoin or shitcoins, even if experienced and affluent, is strongly recommended to seek independent financial advice upon the merits of the same in the context of their own unique circumstances.

DYOR | BTFD | HOLD