

The background of the entire image is a close-up, macro shot of numerous red berries, likely raspberries or similar small fruits. The berries are in various stages of focus, with some in sharp foreground and others blurred in the background, creating a sense of depth. The lighting is soft, highlighting the texture and color of the berries.

CRYPTO WORDS

CY19 November

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

Contents

Goals and Scope.....	2
Support Crypto Words	3
The Real Wisdom behind Proof of Work	4
Tweetstorm: Circularity.....	6
Volatility as information.....	14
Why does hashing public keys not actually provide any quantum resistance?..	15
What Hath Satoshi Wrought.....	18
The Last Mortal Man.....	23
Tweetstorm: Bitcoin is a minimalist philosophy	28
Bitcoin, life and time.	30
Tweetstorm: Bitcoin Oxhearding.....	34
Tweetstorm: The Bitcoin Reformation	39
The Triumvirate of Liquidity.....	51
Op Ed: In China, It's Blockchain and Tyranny vs Bitcoin and Freedom.....	57
An Open Letter to Ray Dalio re: Bitcoin	61
Bitcoin Cannot be Banned.....	139
How I explain Bitcoin to normies.....	147
Johannes Trithemius, Archmage of Secrets.....	151
"The Sovereign Individual" Investment Thesis.....	155
Digital Money	162
Dissecting Bitcoin's Unrealised On-Chain Profit/Loss.....	166
Bitcoin is guerilla warfare.....	178
Bitcoin Is The Only Way To Opt-Out	179
Tweet: Bitcoin is the world's only independent central bank.....	189
Paxful is the Most Important Bitcoin Company You Aren't Paying Attention to.	190
Conclusion:.....	211
Disclaimer:.....	215



Goals and Scope

Crypto Words is a journal of Bitcoin commentary, established February 13, 2019. Its purpose is to document and advance commentary and research in disciplines of particular interest to the Bitcoin community. The journal is broad in scope, publishing content from original research, essays, blog posts, and tweetstorms from a wide variety of fields,

especially governance, technology, philosophy, politics, and economics, but also legal theory, history, criticism, and social or cultural analysis. Its broader mission is to capture the conversations and think pieces in the Bitcoin space for current and future researchers. *Crypto Words* hopes to continue and expand the tradition established by publications such as the *Journal of Libertarian Studies* and *Libertarian Papers*.

History

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

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

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

Support Crypto Words

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



Spread the word

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

Follow us on social media

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

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

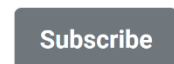


Subscribe to our newsletter

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

Our pledge

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



The Real Wisdom behind Proof of Work

By **Ferdous Bhai**

Posted October 29, 2019

My favorite thing about Bitcoin is “proof of work”.

It’s the idea that your odds of getting the rewards of a block depends on how much work you put in. It’s a simple idea. But it changed the world.

Prior to Bitcoin, the framework of fiat currencies (government-issued money) worked as follows:

There were two groups of humans:

- 1) Ordinary citizens, who have to work to get paid in the dollar. Once they earn the dollars, they must spend or invest these dollars as soon as possible. Because the dollar, sitting idle, loses value every day, as more and more dollars get created out of thin air.
- 2) The privileged class. Whenever new dollars are created, most of it goes to this privileged group of people via interest income, cronyism, and various rent-seeking mechanisms.

Over time, this distribution method ensures that all real wealth gets redistributed from group 1 to group 2.

At some point, inevitably, group 1 can no longer accept this perceived injustice. Battles ensue, unrests begin, civilizations collapse. We start over.

The average life expectancy of a fiat currency is only 27 years.

This beautiful image from Simpsons perfectly captures the moment when the ordinary citizens rise up to what they perceive as “unfair”.

Bitcoin fixed this.

In Bitcoin, the issuance of new coins is distributed via “proof of work”. All you have to do to earn new coins is to show “proof of work”.



“Proof of work” is not just about running the mining algorithm to keep the Bitcoin network secure. It’s deeper than that.

Are you a writer? Write. Those who value your work will pay you for it.

Are you a developer? Code.

Are you a chef? Cook.

Show proof of your work!

Unlike in fiat money, there’s no privileged class. Nobody earns bitcoins for free.

With this one simple idea: “proof of work”, Bitcoin leveled the field for humanity.

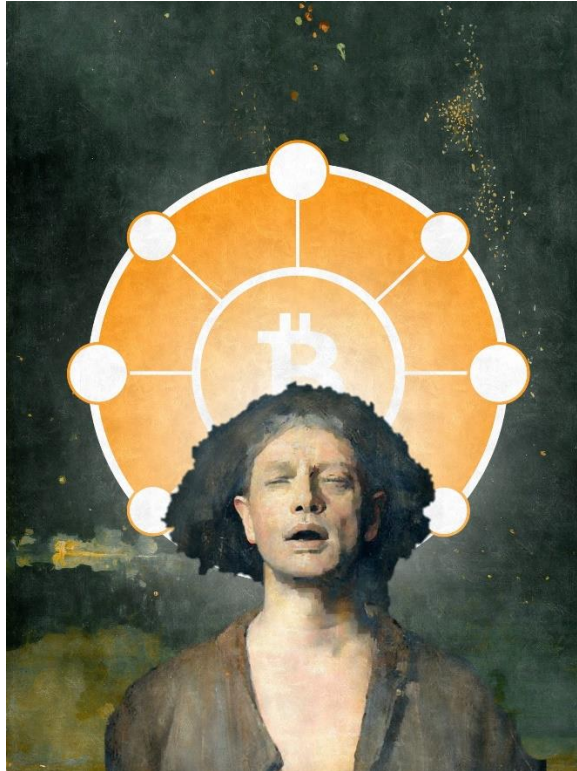
The world is a bit fairer when wealth gets distributed to those who do the work. 🙌

Tweetstorm: Circularity

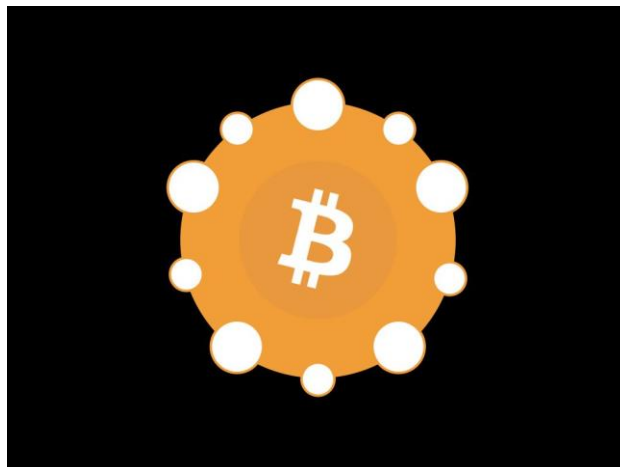
By Cigi

Posted October 30, 2019

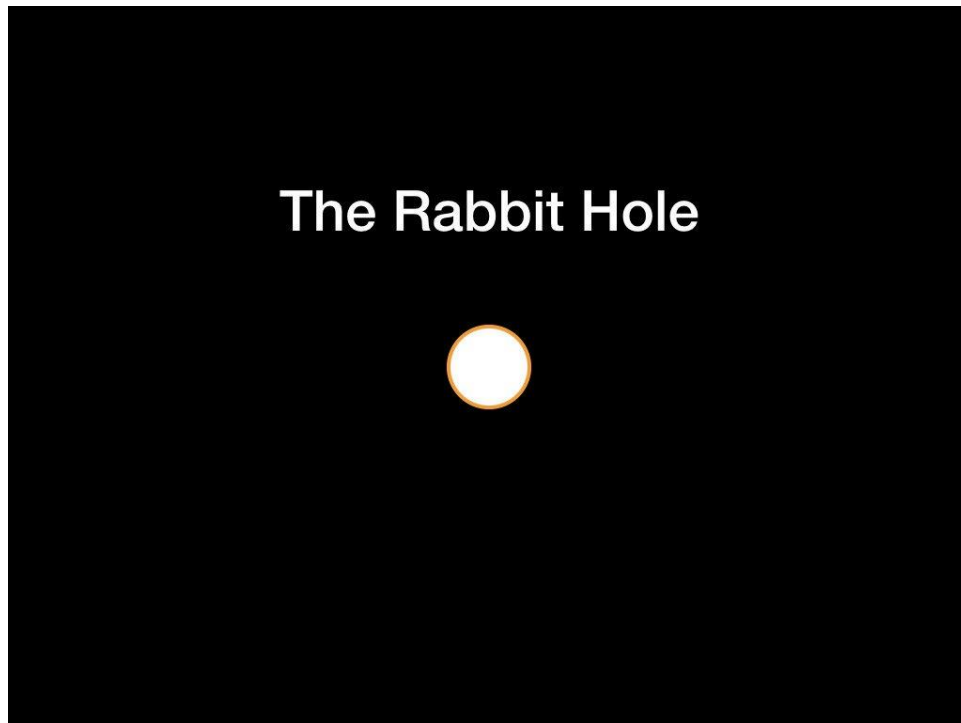
“Circularity” - A thread about Bitcoin, religion, mirrors, my rabbit hole journey, and where Bitcoin (and bitcoiners) might go in the next couple of years.



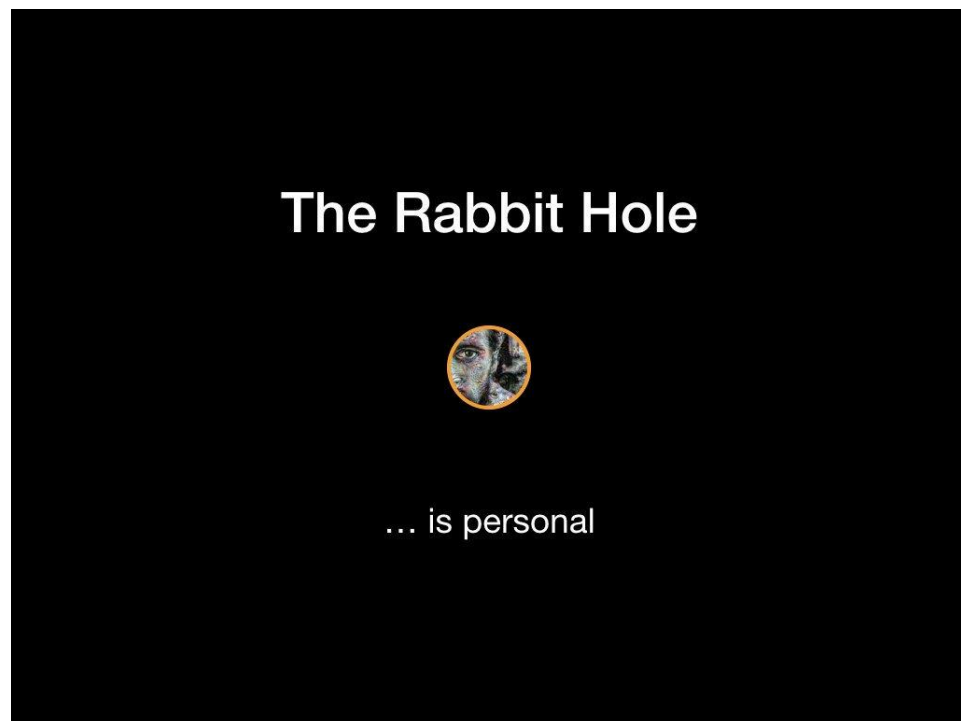
2/ I drew it in various forms, so the details (e.g. how many outside circles there are) aren't that important. The main idea is important - at least to me.



3/ The Bitcoin “rabbit hole” might look innocuous at first. After all, you’re just trying to answer a very simple question: “What is Bitcoin?”

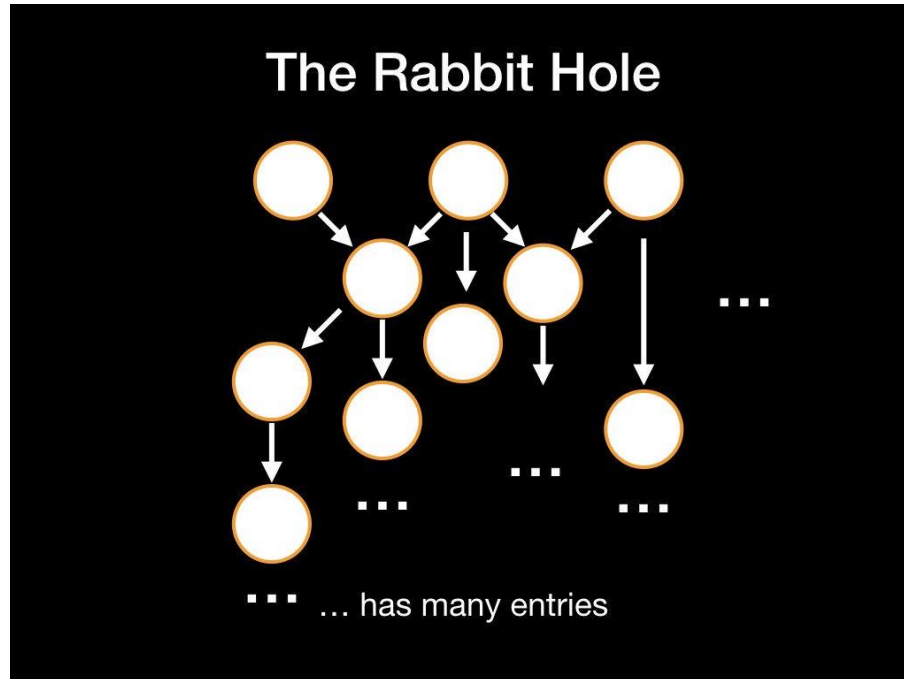


4/ First of all, I believe that falling down the Bitcoin rabbit hole is a deeply personal experience.

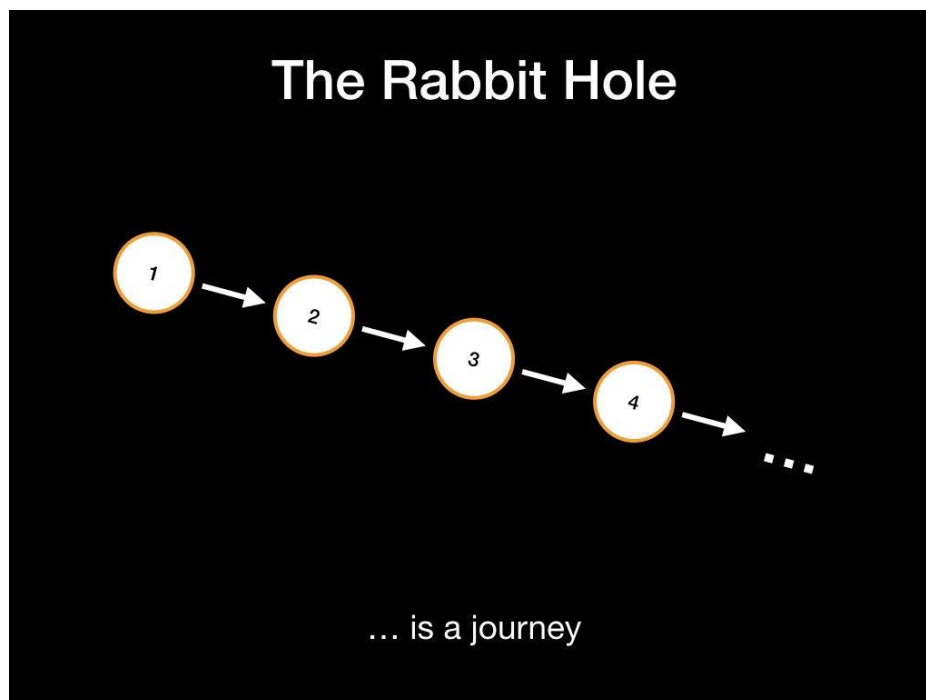


5/ The rabbit hole has many entries. Your particular entry point depends on circumstance, your background, and your previous experience.

Once you are inside, however, you will stumble upon things that are far removed from your particular point of entry.

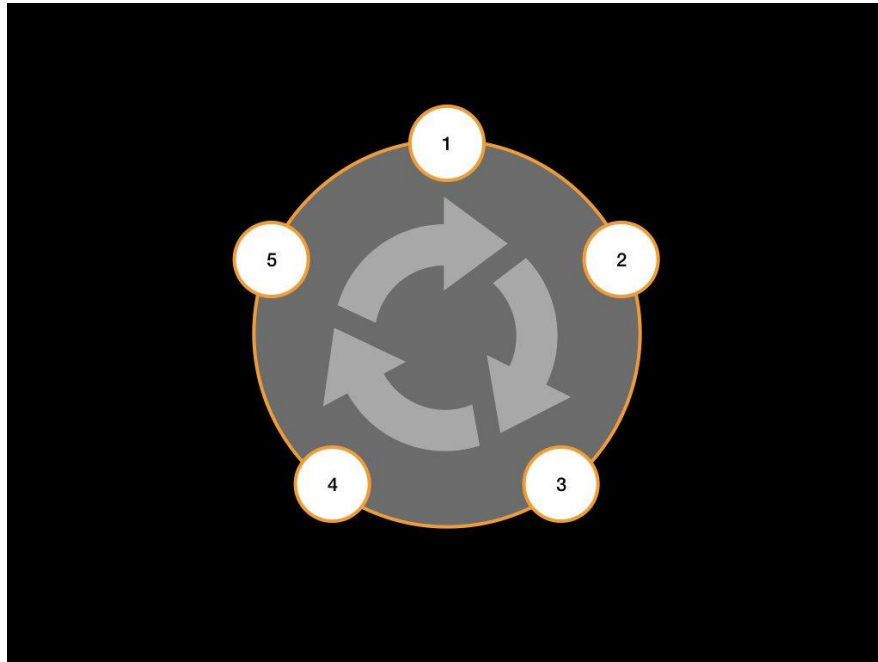


6/ Many say that the rabbit hole is bottomless, and I tend to agree. It certainly feels like a journey without end.



7/ However, I believe that Bitcoin - and the rabbit hole journey - is circular.

For whatever reason, this insight was of such profundity that it changed me, my view of the world, and my outlook in regards to the future.



8/ Bitcoin is profoundly circular. It is circular because it is anchored in nature, via the energy expended in proof-of-work. Some even go further and conclude the following:

“Bitcoin is Nature” – @FriarHass

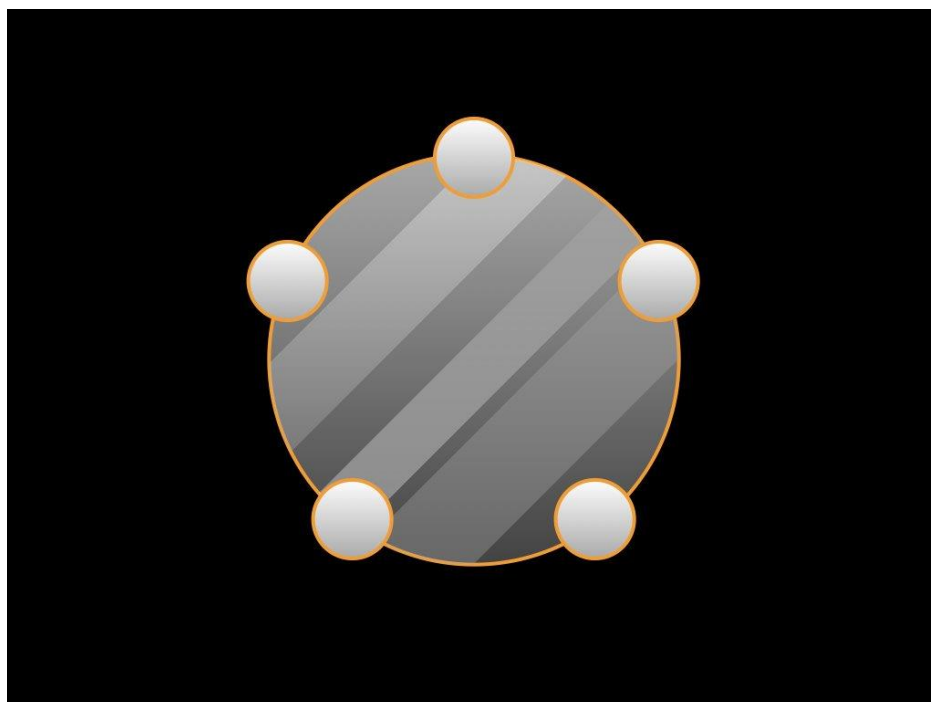


9/ You can get stuck in the smaller circles, which is partly why Bitcoin is so hard to understand. If you are a trader, you might get stuck trading. Others might get stuck on the whitepaper, or get stuck on implementation details.



10/ I sometimes drew this image as a mirror, because, well, I believe that Bitcoin is a mirror - it reflects who you are; it reflects your beliefs.

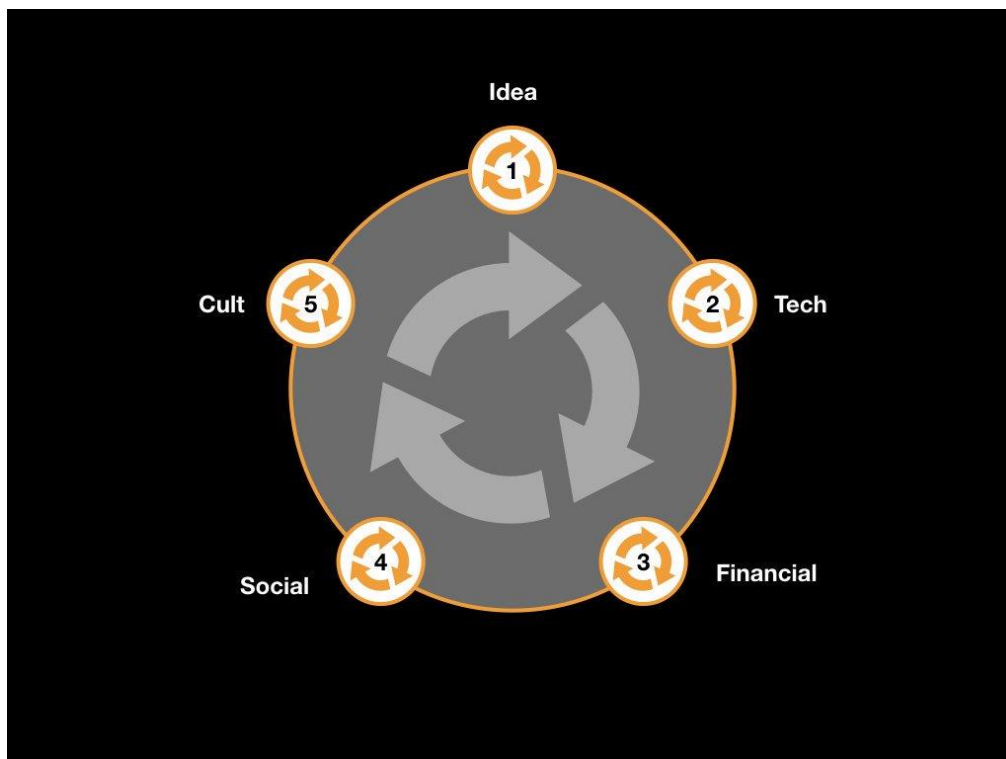
“Bitcoin is different things to different people.” “Bitcoin is whatever it needs to be...”



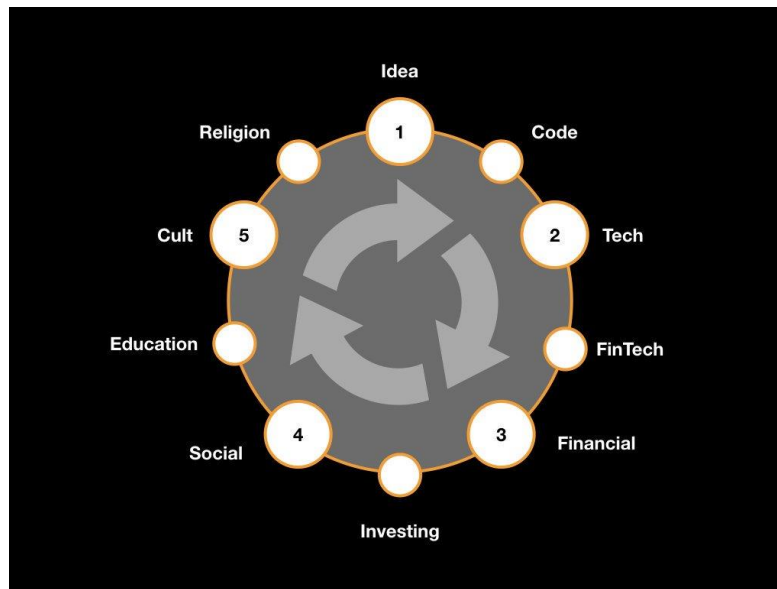
11/ "Knowledge is a mirror and for the first time in my life I was allowed to see who I was and who I might become."



12/ The main journey, as I see it now, is roughly as follows: Idea -> Tech -> Finance -> Social -> Cult -> Idea



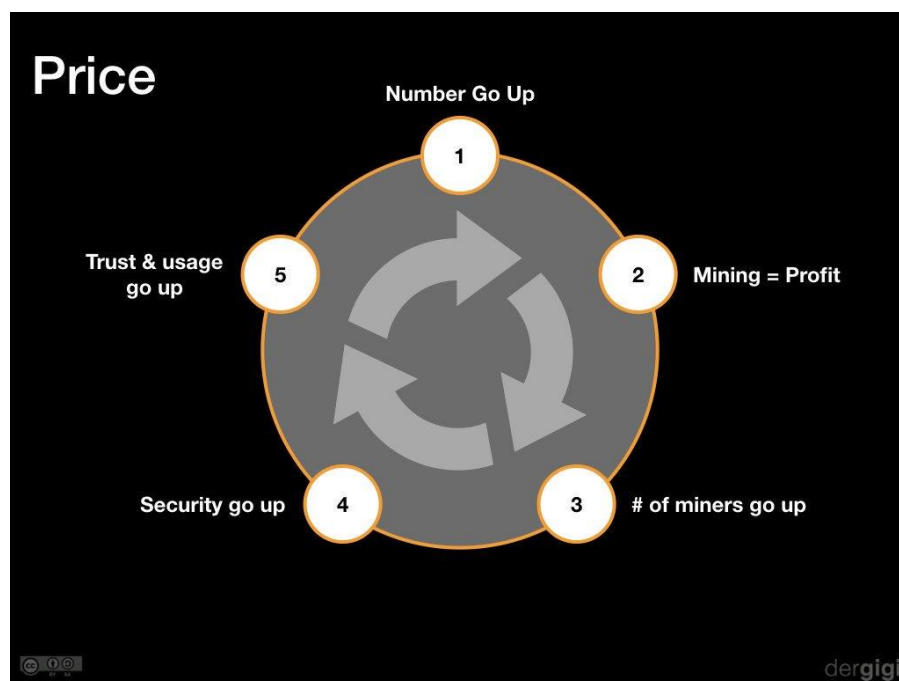
13/ There might be multiple stops in-between; that's not particularly important. What is important, is that a cult exists, and some people will take it to the next level. What is the next level? I think it's Religion.



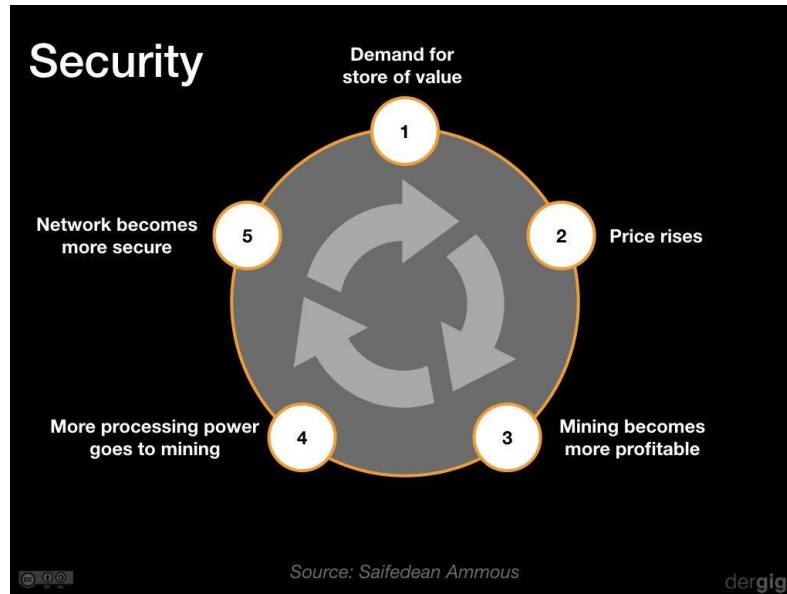
14/ Up to now, the most powerful ideas have been religious ideas.

Bitcoin fixes this. It combines financial incentives, economic realism, mathematics, and physics with fundamentalism and religious devotion. More powerful.

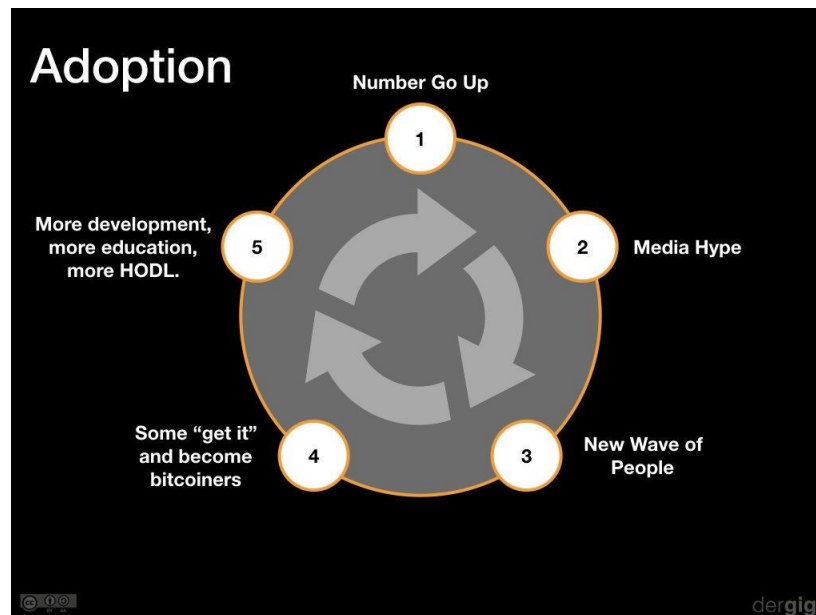
“Bitcoin religion” is real. It has already started.



15/ I believe that Bitcoin is the most powerful idea of our time. It is about to become one of the most powerful memes of our time. I believe that more and more people will be religious about Bitcoin, about the idea of separating money and state through absolute scarcity.



16/ Every cycle new bitcoiners are born. Some of these bitcoiners become maximalists, and some of these maximalists will have religious devotion.



17/ I'm prepared to be wrong about this.

But I ask you, dear skeptics: are you prepared to deal with tens of thousands of zealots, in case I'm right?

Volatility as information

By acrua

Posted October 31, 2019

There is this fascinating book by George Gilder named “Knowledge and power”.

In this book Gilder claims that knowledge acquired by entrepreneurs, and their freedom to share and use that knowledge, are the ignition to a prosperous economy. Whatever improves that knowledge sharing is, as a consequence, good for the economy.

On the other hand, Government’s “ability” to regulate and suppress knowledge, ideas and information manipulation prevent the economy from prospering.

Volatility is in my opinion information that has not yet been figured out

Entrepreneurs are actually agents that get into the unknown, and are rewarded by turning volatility into predictable outcomes. Indeed, volatile environments are steep learning curves and entrepreneurs are rewarded economically and through lots of learning by making things easier for others.

I feel this is exactly what is going on with Bitcoin’s price volatility. Its huge volatility is usually a symptom of something gigantic going on, on lots of information to be processed, huge rewards not only for the entrepreneurs (aka hodlers) willing to step in, but also for the entire world, once it manages to create a financial system where noise is mercilessly eliminated in order for information to flow freely and transformed into transparent code for those willing to learn to look into it. I think Bitcoin is what George Gilder calls a low entropy information carrier.

Its price volatility is the clear symptom that a massive amount of information still needs to be processed by millions. Entrepreneurs, speculators in a trader or hodler shape are helping to decrease it by absorbing way more information than others and profiting in the process.

If you are reading this, you are likely to be a “Bitcoin entrepreneur”, a hodler.

I have no doubt at this point that your learning efforts are very likely to be rewarded!

Why does hashing public keys not actually provide any quantum resistance?

By Andrew Chow

Posted October 16, 2019

In the discussions about taproot, it was mentioned that outputs will include the public key directly instead of hashing them. It is stated that, currently, hashing does not really provide quantum resistance. Why is that?

Answer:

Although hashing a public key by itself does provide quantum resistance, this is really only when it is considered by itself in a vacuum. Unfortunately, public key hashes do not exist in a vacuum and there are many other things in Bitcoin that need to be considered.

Firstly, if public keys were hashed, the funds are only protected before they are spent. As soon as a P2PKH or P2WPKH output is spent, the public key is exposed. Whilst the transaction is unconfirmed, an attacker with a fast enough quantum computer could compute the private key and create a conflicting transaction which sends the funds to himself instead of the intended recipient.

Furthermore, if that attacker is a miner, they could do this with every single transaction and simply refuse to mine transactions that don't send the coins to himself.

While this is a problem, people often argue that it's better than someone just spending the Bitcoin outright because they have the public key from the blockchain. While that is true, there are an extremely large number of outputs with exposed public keys.

Over 5.5 Million Bitcoin are in outputs with exposed public keys, either because they are P2PK outputs, or because users are reusing addresses and thus public keys are exposed in other transactions. So if a quantum computer existed that could produce the private key for a public key in a reasonable amount of time, the attacker would be able to steal so much Bitcoin that they would decimate the Bitcoin economy and Bitcoin would become worthless.

So while your particular outputs may be protected by hashes, the value of those outputs would be 0 as millions of Bitcoin are stolen. All that the hashes really do is provide a false sense of security.

Then there are issues with tooling and wallet software that simply expose public keys in other ways than just in transactions and in the blockchain. No existing tools treat public keys as private information; there's no reason they should.

Many wallets send the parent extended public keys to a server so that the server can watch for transactions and send that data back to the client. Anyone who uses such a wallet, even temporarily, exposes their parent public key to a service provider. That provider could then compute the private keys to the public keys they have, derive all of the child keys, and steal all of the Bitcoin associated with anyone who has used their wallet.

Additional issues exist with complex scripts and contracts involving public keys. These scripts, such as multisigs, do not hash the public keys. Furthermore, these contracts typically exist because not all parties necessarily trust each other; one of them could be malicious. In such cases, a malicious participant in the contract would know the public keys involved (by virtue of knowing the script) and be able to steal the Bitcoin associated with those outputs. Existing public key hashes do not protect against this.

So overall, there are tons of ways that public keys are already exposed outside of transactions. These all would allow different kinds of attackers to steal millions of Bitcoin thereby causing the value of Bitcoin to go to 0, which renders any Bitcoin protected by public key hashes to be worthless anyways. Furthermore, users are probably exposing their public keys in unintended ways due to the software that they are using. So using public key hashes only serves to provide a false sense of security, while also increasing the size of transactions. In general, it is not worth the extra size.

Lastly, it is possible to do a transition to post quantum cryptography if it is found that a QC exists which can break ECDLP. If detected in time but still too late to do a proper upgrade, all use of signature algorithms relying on ECDLP (i.e. ECDSA and Schnorr) could be soft forked out thereby locking all coins. The coins could then be spent by providing a Zero Knowledge Proof of some non-exposed or quantum resistant information that indicates ownership of the private keys for the public key.

For example, users could provide a proof that they have the BIP 32 seed that was used to derive the private key for the given public key. Since it is a Zero-Knowledge Proof, the seed itself is not exposed (note that the seed is not part of a public-private keypair so there is no public component that is shared). Since most wallets use BIP 32, this should be sufficient. There may be other

ways to prove ownership without risking coins that have not been thought of yet.

And of course, this all assumes that a quantum computer capable of computing the private key for a public key appears without the public being aware of the technology being close to existing. What is likely to happen is that the progression of quantum computers will be observed, and, at some point prior to them being powerful enough to break ECDLP, Bitcoin will soft fork in a Quantum resistant signature algorithm. Eventually, signatures relying on ECDLP will be removed. And all of that will occur before quantum computers truly becomes a threat. So in that scenario, hashing public keys provides no help anyways.

What Hath Satoshi Wrought

By Hashed Entropy

Posted November 2, 2019

.....

Letters from the Digital Saeculum:

The First Transmission

A **saeculum** is a length of time roughly equal to the potential lifetime of a person or, equivalently, of the complete renewal of a human population. The term was first used by the Etruscans. Originally it meant the period of time from the moment that something happened (for example the founding of a city) until the point in time that all people who had lived at the first moment had died. At that point a new saeculum would start. According to legend, the gods had allotted a certain number of saecula to every people or civilization; the Etruscans themselves, for example, had been given ten saecula.

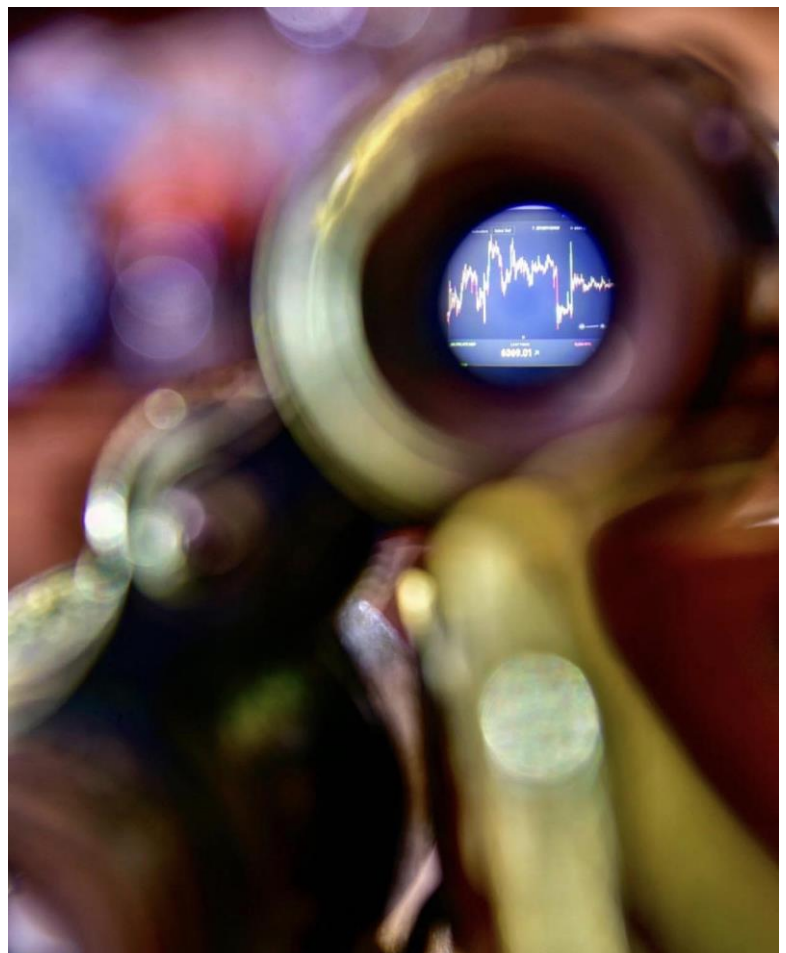
Wikipedia — Saeculum

Late Millennial Saeculum bitcoin chart (2018) viewed with Early Millennial Saeculum binoculars (1917)

What Hath Satoshi Wrought

I'll admit that I found the line to be a little sacrilegious. I guess not many are both students of History and Religion so I imagine that I was the only one on this side left with that impression. But I knew the sender and I knew the sender sent this message with the utmost respect to me as a homage to the honor provided by Annie Ellsworth exactly 200 years earlier.

I wondered if anyone noticed the slight encoding of history between the sender and receiver. I had



timed this very moment to coincide with “What Hath God Wrought” traveling along as a dot and a dash and a dash and a dot and a dot and a dot and a dot and a...well you can figure out the rest.

200 years to the moment.

The day was May 24th, 2044.

Now, it is May 9th, 38 EMS (Earth-Mars Synced time) and I have to proclaim once again What Hath Satoshi Wrought!

Today is the start of the Unraveling.

Digital Saeculum (82 years)				
Generation 8	Prophet (Idealist)	2023 - 2045 (22 years)	1st Turning: High: Hyperbitcoinization, Digital Identity Revolution Postgovernmentalism, The Great Space Leap	2025 - 2046 (21 years)
CyberX Generation	Nomad (Reactive)	2046 - 2063 (17 years)	2nd Turning: Awakening: Transhuman Movement, Fifth Great Awakening, Mars-Earth Quantum Fields	2047 - 2067 (20 years)
Deconstruct Generation	Hero (Civic)	2064 - 2083 (19 years)	3rd Turning: Unraveling: Posthumanism, Satoshi Inheritance Scandal Automarchy Dissolution, The Shallows War	2068 - 2085 (17 years)
Escape Generation	Artist (Adaptive)	2084 - 2105 (21 years)	4th Turning: Crisis: Digital Purge, Human Entropy Laws, The Galactic Migration Failure (Titan Settlement)	2086 - 2110 (24 years)

The Digital Saeculum – 2025–2110

The Unraveling

How can I describe to you all of the events over the last few years in such a short transmission? How do I explain in a few short words, the lifetime of moments that led up to you being asked to flee and leave behind a thousand generations of humanity in one place and to not even last one generation in a new place?

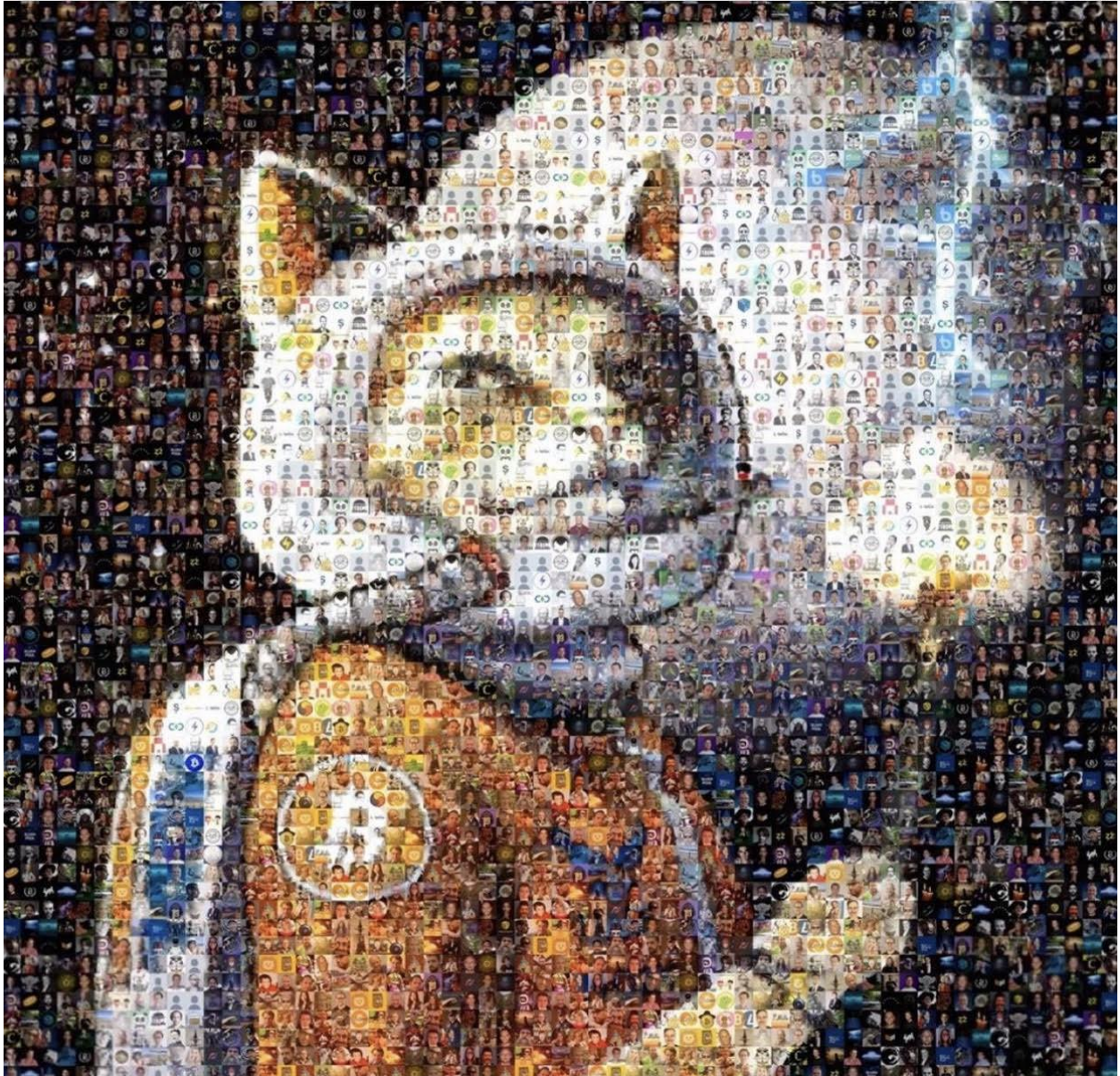
How do I explain this unraveling?

First, the moment of EMS was the most enlightened moment of our Digital Age. We: humanity, transhumans, and hubots brought our worlds: the Earth and Mars together in synchronicity. We enabled instantaneous communication, commerce, and cohabitation.

Geography has made us neighbors. History has made us friends. Economics has made us partners. And necessity has made us allies. Those whom nature hath so joined together, let no man put asunder.

John F. Kennedy

The strides in technology, science, and abstractionism reached the very peak in that moment.



*Pre-EMS Artwork Featuring Hodlonaut (May His Light Always Shine)
Comprised of Hodl'rs of Ancient Times*

For now, I'll focus on the economic tensions and leave the automarchy dissolution and the awakenings for another day.

Posthyperbitcoinization started with a simple point in time: I call it the moment that death commenced its 51% attack. This was the moment in which more than 50% of the early hodl'rs reached the end of their lives. The problem is that in their zeal for Self Sovereignty, too many failed to consider Family Sovereignty, Generational Sovereignty, Legacy Sovereignty, and with their deaths, Satoshi's burned from existence. This is now known as the Satoshi Inheritance Scandal.

We are a continuum. Just as we reach back to our ancestors for our fundamental values, so we, as guardians of that legacy, must reach ahead to our children and their children. And we do so with a sense of sacredness in that reaching.

Paul Tsongas

The inability to apply Low Time Preference to beyond one's self created a massive problem at the base layer of our economic system. This led to inequality as whole groups were unable to transact due to a lack of underlying bitcoin support. The Shallows War started as groups formed under the banner: "We are Left in the Shallows" claiming inequality and inability to access the Earth-Mars economic system.

A House Divided Against Itself Cannot Stand

Where did the first thread begin to separate? Where was the first point of weakness? Where was the first sign of anti-antifragility?

You must first understand the alliances that were created during the EMS. EMS initially created a foundation of fairness across Earth-Mars as for the first time bitcoin's foundational layer was synced, block rewards were distributed, and the risk of one alliance dispersing was finally fully addressed.

Surely there is no enchantment against Jacob, neither is there any divination against Israel: according to this time it shall be said of Jacob and of Israel, What hath God wrought! Behold, the people shall rise up as a great lion

Numbers 23:23-24

Now I will only speak in hushed tones here so understand that I can only say so much: this was also a moment that the inequalities (i.e. fairness) could be closed across humans and hubots.

But the unraveling started...

The first thread tore when a large number of hodl'rs died on Earth as a result of the "accidental" CitaHal destruction. [CitaHal was the second major Citadel built which was appropriately named in honor of Hal Finney] While the earliest banners proclaimed "Remember the CitaHal", the undermining of the supply of bitcoin on the Earth, quickly led to disappointment, disillusionment, dissolution, and finally "We are Left in the Shallows".

The Shallows Artwork – "We are Being Left Behind"

The string was pulled and when it unraveled:

The Last Mortal Man

By **HashedEntropy**

Posted November 13, 2019

Letters from the Digital Saeculum (Part 2):

The First Message

The First Transmission (Part 1) is located here:

<https://medium.com/@HashedEntropy/what-hath-satoshi-wrought-f7687b631d42>

*For they are like a breath of air;
their days are like a passing
shadow. Psalm 144:4*

Fragility

Humans were so fragile. I used to wonder if humans were preoccupied by the thought of their own mortality, though I now know that transformations can be very gradual.



If you drop a frog in a pot of boiling water, it will of course frantically try to clamber out. But if you place it gently in a pot of tepid water and turn the heat on low, it will float there quite placidly. As the water gradually heats up, the frog will sink into a tranquil stupor, exactly like one of us in a hot bath, and before long, with a smile on its face, it will unresistingly allow itself to be boiled to death.

Parable as described by Daniel Quinn

I now accept that mortality was an ever present reality for humans in which they were able to function without being crushed by an existential dread. Mortality was in the air they breathed, constantly floating and surrounding and flowing...it was their existence. They were vapor; there was no other way.

Oh, how wrong were we to think that immortality never meant dying

Our Lady of Sorrows by My Chemical Romance

As it is unknowable to ascertain when humans first became humans, it is as unknowable to fix the very moment when humans crossed the chasm into Homo Alium. Yet, we know for certain the identity and cause of **The Last Mortal Man**.

You have already read the words from **The Last Mortal Man** as shared in the The First Transmission.

Now I will share with you The First Message.

The First Message

Sacrifice was one of humanity's greatest gifts.

Human progress is neither automatic nor inevitable... Every step toward the goal of justice requires sacrifice, suffering, and struggle; the tireless exertions and passionate concern of dedicated individuals.

Martin Luther King Jr.

In 3 EMS, it was proven that **Satoshi** sacrificed wealth, power, and fame in order to allow bitcoin to survive its moment of greatest vulnerability. The question of **Satoshi's** mortality or intentional anonymity was finally answered.

*Photo of Book with Wings Sculpture
by Anselm Kiefer (1992-1994);
Material: lead, tin, and steel*

But, you know, sometimes you just gotta be drop-kicked out of the nest...It's the only thing that gets you to the next level, right?

Robert Downey Jr.

In letting go, **Satoshi** provided the conditions for bitcoin to grow its anti-fragility, survive, and eventually thrive.

This was **Satoshi's** sacrifice.

And **The Last Mortal Man** would someday make the last human sacrifice.



*The fleeting moment of a
bubble floating by the enduring
sun*

Like the dew on the mountain,
Like the foam on the river,
Like the bubble on the fountain,
Thou art gone, and for ever!
Coronach by Sir Walter Scott

The Crisis

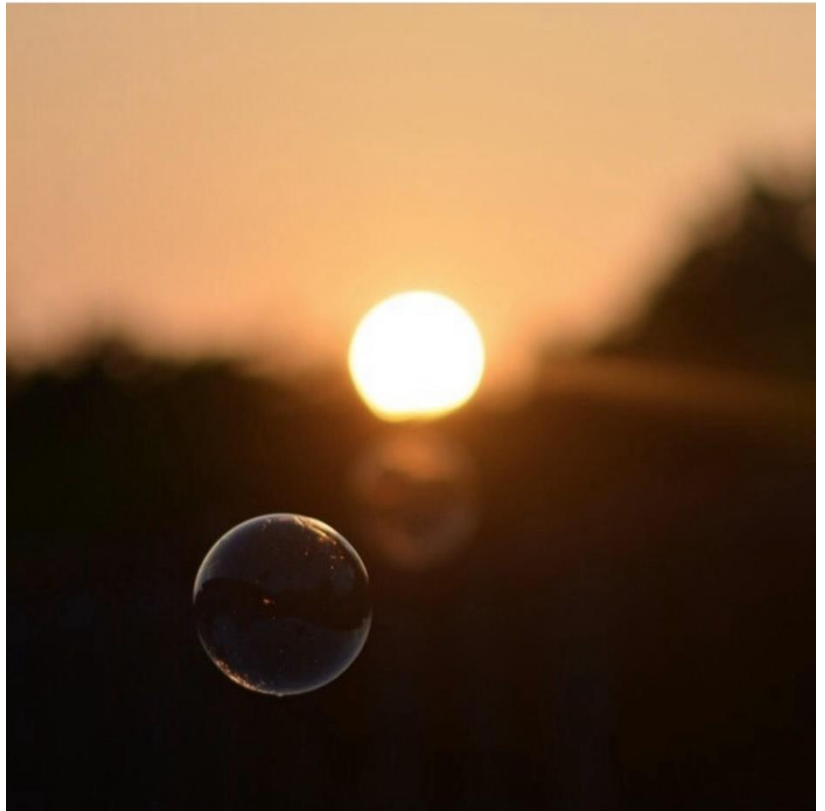
In the First Transmission, you read of the Unraveling. You read the words of The **Last Mortal Man**. Now, I will share with you the story of what was lost and what led to The **Last Mortal Man** to make the final sacrifice.

The Shallows War was beyond brutal. Earth against Mars and humans against hubots. The de-center could not hold and the protocol that automated laws and rules and society was undermined. The Automarchy Dissolution resulted in a existence with no binding connectors. Incentives (both economic and governance) were no longer aligned. This led to a crisis greater than you can even imagine.

Beyond the standard rules of engagement that one might expect in an all out conflict, humans were the first to enact the “nuclear option.” The Shallows War showed that humans could not win a war on equal footing given the hubot’s embedded AI, quantum processors, and synchronicity. Out of the ashes, humans launched a Digital Purge strategy. By going completely offline, they quickly separated from their dependence on technology. They then attacked the hubs that powered hubots and assaulted any forms of digital existence. The Digital Purge reached totality in Mars and was on the verge of fully erasing the digital world from the Earth.

We’re plugged in 24 hours a day now. We’re all part of one big machine, whether we are conscious of that or not. And if we can’t unplug from that machine, eventually we’re going to become mindless.

Alan Lightman



But the hubots responded. And fittingly, they responded with code. A code was developed that would become known as the Human Entropy Laws. The concept was simple but extremely effective. Human behavior maintained a certain level of disorder and unpredictability. Through fine tuning their own behaviors, hubots were able to detect these irregularities and could eliminate the source. The source being humans.

Humans were left with two options: cede their freewill and humanity to align with the order range of hubots (and hence “to get in line”) or face destruction.

My message to you is this: pretend that you have free will. It’s essential that you behave as if your decisions matter, even though you know they don’t. The reality isn’t important: what’s important is your belief, and believing the lie is the only way to avoid a waking coma. Civilization now depends on self-deception. Perhaps it always has.

Ted Chiang

The Moment

All seemed lost, yet there was one that found another way. **The Last Mortal Man** had found a way to preserve humanity (thus undermining the Human Entropy Laws), to preserve hubotics (thus undermining the Digital Purge), and to preserve a lasting peace.

*Monument to Earth Mars
Synchronicity; Damaged
during The Shallows War*

And it partly involved going back to the source: back to a protocol, back to a decentralized peer-to-peer solution. Back to the economics. Back to that ancient honey badger. Back to bitcoin.

We know the very act, though it is not yet time to share with you those details.

We call it The Moment, the moment in which **The Last Mortal Man** made the sacrifice.



And there was a catch...

It would cost him everything and yet the worst part is that after The Moment, he would live 21 more years.

Can you imagine the turmoil of knowing that you will be the last human to face mortality and to have to grapple with that reality for years?

Remember, the Story is not over and as he described in the First Transmission, you are the hope.

For now, you should know that the end of **The Last Mortal Man** would also be the last death knell of humanity as you know it.

Though, somewhere in the fog of the Crisis:

Homo Alium would arise.

Tweetstorm: Bitcoin is a minimalist philosophy

By Dan Held & Conner Brown

1/ Bitcoin is a minimalist philosophy.

Bitcoin Minimalism is a lifestyle that helps people question what things add value to their lives.

A joint thread mostly by @ConnerBrown and myself, with other Bitcoiners providing input:

2a/ Create more, consume less

Bitcoin reduces your time preference and enables you to look long-term at saving and investing. It's not about consuming, it's about saving and investing that makes our world a great place.

2b/ By consuming less, you allow others to access good and services more cheaply currently.

It's a way to escape the excesses of the world around us — the excesses of consumerism, material possessions, clutter, too much debt, too many distractions, too much noise.

3a/ Discover purpose in our lives

Bitcoin Minimalism is about finding truth in yourself and your beliefs rather than in material possessions. Freedom from the trappings of the consumer culture we've built our lives around which has been fueled by Keynesian economic policies

3b/ Bitcoin minimalism is about making decisions more consciously, more deliberately... a flight to quality. Clearing away all of the frivolous arguments and only focusing on what matters. In stark contrast to the ICO bubble in which consuming, waste, and fraud were prevalent.

3c/ Minimalists search for happiness not through things, but through life itself; thus, it's up to you to determine what is necessary and what is superfluous in your life. The pursuit of knowledge through Bitcoin Minimalism is about better understanding the world around you.

4a/ Minimal viable product

Building a product is about fighting the insidious disease of more. Bitcoin's community and core dev team have focused on being the most efficient, or minimal, they can be in regards to building Bitcoin.

4b/ Developers: Working with one chain reduces mental bandwidth for developers. Working with many is a near impossible task.

4c/ Security: Using just one Blockchain enhances the security of the ecosystem through more rigorous exploit analysis and PoW building the “largest” wall (instead of hundreds of little walls)

4d/ Code: Satoshi chose a non-turing complete language so that it can provide predictable outcomes and facilitate trust minimization.

Adding more complex loops creates unpredictable scenarios (DAO, parity) that requires you to trust the script without knowing the outcomes.

4e/ Scalability: Bitcoin is about being hyper-efficient with Layer 1 (Schnorr/Segwit) while also pushing innovation on Layer 2 (Lightning) which is an exponentially more scalable solution, thereby enabling Bitcoin to be more usable by the masses.

4f/ We want to maximize the value/byte transfer. While we could easily increase the block size, it would be the least efficient way to scale. And being efficient with our limited block size is of utmost importance as it enables us to become decentralized/censorship resistant.

4g/ Economics: By rebuilding the capital markets stack from a sound money base, we can then be confident that our foundation is structurally secure.

5a/ Bitcoin Minimalism is rooted in libertarian philosophy

Libertarian political philosophy follows the idea of minimal government intervention and respect for the sovereignty of the individual. As Thoreau said, “Government is best which governs least”

5b/ A government should be a minimalist system that protects individuals from threat of violence or coercion, enforces contract and property rights, and reasonably provides for the national defense.

5c/ By separating the monopoly on money from the state, we are guaranteed that any seizure of wealth must be through direct taxation rather than through silent inflation or deficit spending.

5d/ 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.

Bitcoin, life and time.

By zen B

Posted November 5, 2019

You have a limited lifespan.

The moment you are born to the moment you die. A limited and countable number of days and hours. This time is the scarcest and thus the most valuable thing you will ever have.



Photo by Aron Visuals on Unsplash

Every passing minute, every passing second takes away a bit from the whole, leaving every remaining second even more valuable. Time keeps on passing, with or without you acknowledging, exponentially increasing the value of every day, every second you are left with to live.

Every new morning is exponentially more valuable than the last.

Now, take a pause, look at where you are right now. The present moment, this very second is *the most valuable second you have ever had*, exponentially valuable than any time in your life until now.

Look around, look at yourself, ask, what have you traded this time for?



Photo by [Mink Mingle](#) on [Unsplash](#)

Knowing this, become aware that all your life you have been trading. Trading the most valuable, scarcest resource for fulfilling your desires.

All your decisions are but a trade in time.

Most of the humanity chooses some form of good, called money, to store the time they spent generating time efficiency (value) for others. You trade your working hours for money, saving it, expecting it to hold the value of your time into the future.

With that foundation, here's a thought experiment. One from personal experience. My mother spent most of her life teaching biology to high school students. She was paid \$8/month at the start of her career in 1980s. She traded 10hr/day for a month in exchange for \$8. At her retirement she was paid ~\$1000/month for almost the same job.

The 8\$ she was paid for a month is not even worth a day's expense today.

Where did her time go?

Isn't 30 days of her life back then(1980s) = 30 days of her life now? No? Think hard about it, think to the seconds that passed in that month and the seconds

that tick off her life now, count them. I bet they would be the same. Can those \$8 give her those days back?



If you understand the exponential nature of time's value as explained before, you'll see that those 30 days of her time then (if stored) should have been exponentially more valuable today because of the number of days she is left with in her life now.

So, what happened?

She's was ignorant of the importance of **scarcity**. Unaware of the fact that for a good to act a store of value, it needs to reflect the scarcity of the very thing whose value it is expected to store.

She traded her time (the scarcest good) for a good that was marketed to her as a store for value but was being produced in large quantities (\$). The easy printing of money diluted her life savings and robbed her of her own life.

Photo by [Tadeu Jnr](#) on [Unsplash](#)

I'd not disagree that she was a bad trader and could have traded the fiat(Government issued money) for something scarcer. But apparently the schools even today don't teach monetary history and markets.

This still goes on today. You will be robbed off your life.

Don't make the same mistake your parents made. Understand the value of your present moment, invest it properly(*it is the most valuable thing you'll ever have*).

So, what should you do?

Understand scarcity. Study money. Learn the difference between hard and easy money. Also learn about bitcoin, it is the scarcest good that is closest in reflecting the scarcity of your time.

To get started, pick a copy of [The Little Bitcoin Book](#) and Knut Svanholm's fantastic work [Bitcoin: Sovereignty through mathematics](#).

For a deeper dive check out [@saifedean's](#) book—[The Bitcoin Standard](#).

Follow [@dergigi](#) [@Breedlove22](#) [@bquitem](#) [@CitizenBitcoin](#) [@stephanlivera](#) [@heavilyarmedc](#) [@mrcoolbp](#) [@MartyBent](#) [@ManuelPolavieja](#) [@knutsvanholm](#)

@TheCryptoconomy @RawBTC @johnkvallis @matt_odell who inspired me to write this thread.

Ask questions and don't waste your life.

If you enjoyed and would like to support, drop me some satoshis:

<https://paynym.is/+darkfeather86b>



PM8TJbNS4T7Vz4NtWNaD2rfIrGKorjCPJ9FZjZ2qx3sGueDi26Ri8eZHDaU9ytbP
LFDYoEp9dkz4UY6Ra3guMmbc9rJ288fJkB1QGrn4frUpAFA344R

Tweetstorm: Bitcoin Oxhearding

By **Dennis Reimann**

Posted November 4, 2019

Some days ago [@dergigi](#) had a great thread about the idea of the Circular Rabbit Hole. This very much reminded me of the buddhist idea of the journey to enlightenment described with the ten Oxhearding pictures. Let's dive into that ...

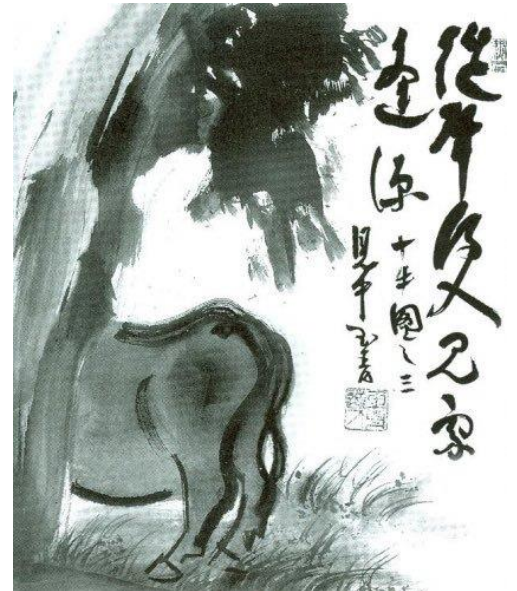
Searching: Going through life you feel something isn't quite right. You aren't satisfied and start to question things more fundamentally than before. You sense that you have been lied to – fake money, fake politics, fake chances.



Footprints: Challenging your tried and true beliefs you come to grips that trusting authorities and institutions all too much isn't a good idea. Fool me once, shame on you – fool me twice, shame on me.



Seeing: You find out about #Bitcoin, get a glimpse of its properties and potential. You read the white paper and you are excited how many ideas the space has to offer. This needs to be explored further ...



Catching: Excited by the many things you learn you become overwhelmed by the possibilities. You certainly want to be a part in all of this, start to trade and also dabble in shitcoins.



Tending: Sooner than later you get burned. You see there are scammers left and right – by no means this is as rosy as you thought. You get back to basics and become even more interested in Bitcoin as it stayed true to its ideals and promises real freedom instead of quick wins.



Riding Home: You see this will be a marathon rather than a sprint, become calmer and have gratitude for what you learned. You lower your time preference, start #stackingsats, gradually learn while you go and peacefully enjoy the ride.



Forgetting: Until now there was the idea there was something to do – this separation vanishes and there is nothing special anymore. Everything has become clearer: intentions, ideas and goals align.



Forgotten: „Bitcoin is. And that is enough.“ (h/t @Beautyon_)



Returning: You are where you were when you discovered the Rabbit Hole, but you are not the same anymore. You aren't as entangled as before, see things clearer and you have become more self-sovereign.



Entering the Marketplace with Helping Hands: Having experienced this fulfillment and kind of freedom you connect on a deeper level and help others. Still learning tons yourself you educate, develop, grow and nurture the world you want to live in. Onwards!



... that's it, hope you liked it. Special thanks go to [@dergigi](#) and [@citizenbitcoin](#) for the conversation they had on this episode, which inspired this thread: [Pod download](#)

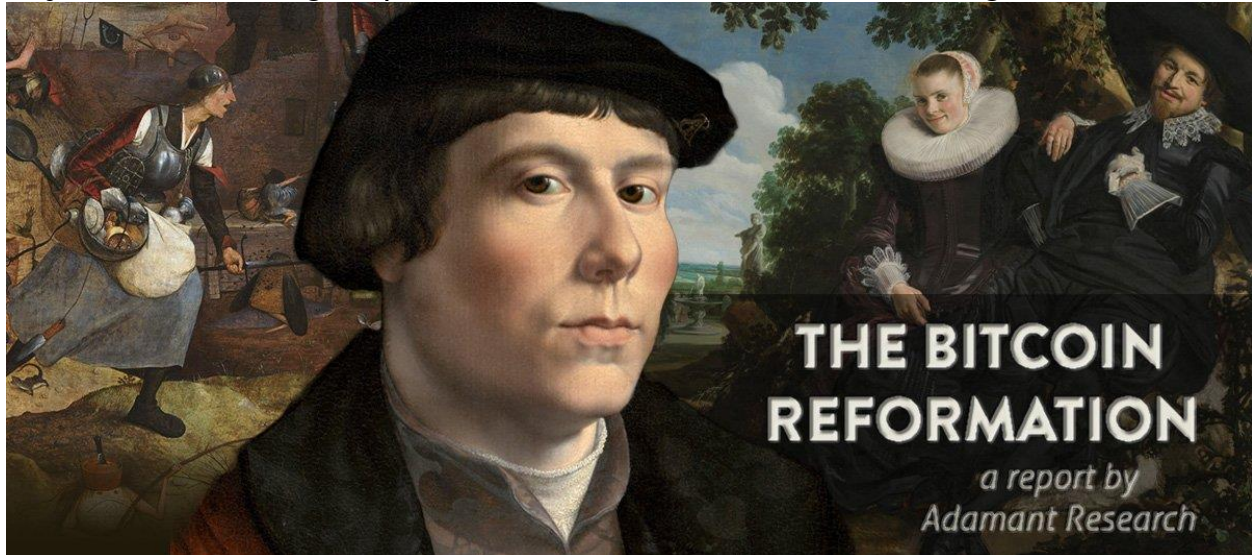
fyi: here's also the link to an article explaining the Oxherding path, which I tool the pictures from: [The Ten Oxherding Pictures](#)

Tweetstorm: The Bitcoin Reformation

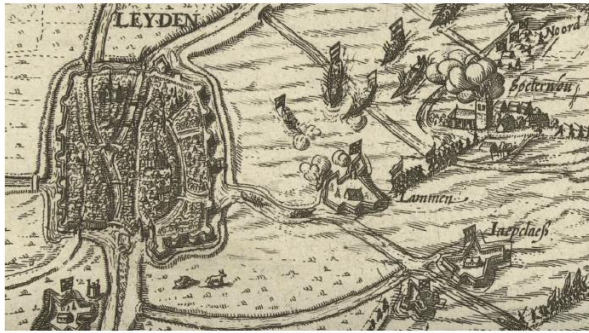
By Tuur Demeester

Posted November 7, 2019

1/ The main thesis of “The Bitcoin Reformation” is that there are four fundamental parallels between the Protestant Reformation and the present day, which could signal profound societal and economic changes ahead.



2/ This is the TL;DR version of a 13 page report. This tweetstorm shares the essence but strips away the little historical details that made it so fun to research and write. Check it out here: <https://docsend.com/view/ijd8qrs>



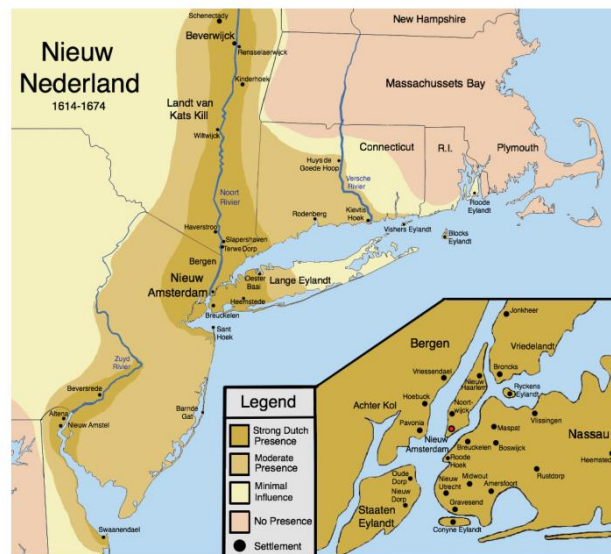
Relief of Leyden, 1574 (detail). Breaching the dikes to flood the countryside caused huge damage, but the flood weakened the Spanish army and allowed the Dutch militia to reach the city.



Cart used to transport gold coins at the Amsterdam Wisselbank



This etch from 1580 shows how threatened the Dutch felt by the Spanish invaders, here depicted as a pig infestation. The lion was a symbol associated with the Netherlands.¹



Map of New Netherlands - the Dutch presence was the greatest in the area currently known as New York City.

3/ The Protestant Reformation was a multi-generational conflict (16th-17th C.) that produced the separation of church and state, and which profoundly reshaped the economies of Europe and the New World. Today, bitcoin suggests that it's possible to separate *money* and state.

4/ Aside from the four general Reformation parallels, our report also suggests that there are significant similarities between the innovative economy of 17th century Netherlands and the bitcoin economy today. This may give us insight into what's coming for bitcoin.

5/ Here are a few of the conclusions:

Some suggested conclusions of this report:

- Bitcoin tolerance versus intolerance to become a major political fault line
- Bitcoin's primary drivers will be in saving, lending and underwriting
- Collaborative custody to become an industry standard
- Offshore banking may transform into bitcoin banking
- Bitcoin to mature quickly: bonds, annuities, loans, insurance
- Initial exchange offerings (IEOs) expected to stay and grow larger
- Bitcoin savers could accelerate a revolution in the history of thought

6/ So let's dig in. What are the four requirements of a reformation?

Four preconditions of a reformation:

- Rent-seeking monopolistic service provider
- Technological revolution: catalyst for change
- New economic class: people with something to fight for
- Credible strategies for defense and escape

7/ First, we need a painful status quo in the form of a rent-seeking monopolistic service provider. In the 16th century that was the Catholic Church, today that is the financial system of fiat money and central banking.



Christ and the Sheep Shed, 1524, Nuremberg. This popular woodcut propagandizes how believers by faith alone will be welcomed by Christ, while the Catholic church is shown as pillaging the shed and cashing in on indulgences.

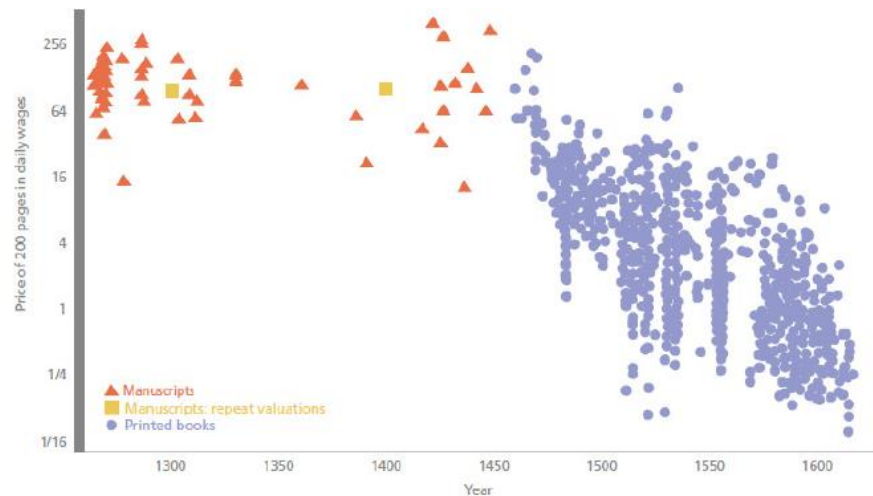


8/ The service provided by the Church was access into heaven (for which it charged money by selling indulgences). The service provided by the financial system today is access to “financial heaven” (for which it charges money in the form of inflation tax).

9/ The second requirement for a reformation is a technological revolution, which acts as a general accelerant in the battle of ideas: it lowers the cost of both information and travel.

10/ The most important 16th century innovations were in the area of maritime exploration, international business, and of course the printing press, which, in

one century, lowered the price of a book from a full year's wage to the equivalent of a chicken.



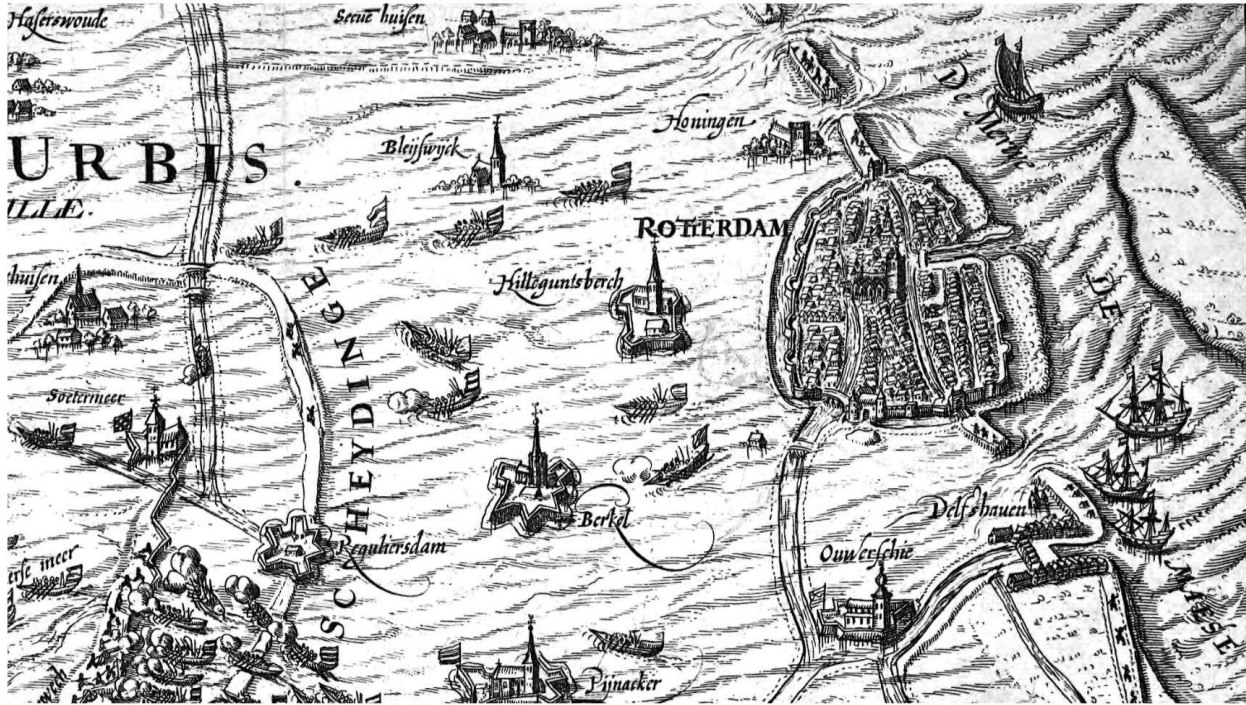
In 15th century Europe “the raw price of books fell by 2.4 per cent a year for over a hundred years,” while the share of university courses on scientific subjects rose from 25% to 40%. (Dittmar & Seabold)

11/ The current-day technological revolution is digital: telecommunications, computation, data storage, open source software, cryptography, and of course the internet. The cost of 1 Mb/s bandwidth dropped by 99% in 20 years, from \$100K to under \$10.

12/ Third, we need people who have something to fight for. In the 16th century that was the merchant class, today that is the millennial generation who don't trust the financial system and who are heavily invested in technology.



13/ And the final requirement for a reformation is for the rebels to have credible strategies of defense. The Dutch protestants mastered water as a defensive moat against invasions, the millennials have cryptography at their disposal.



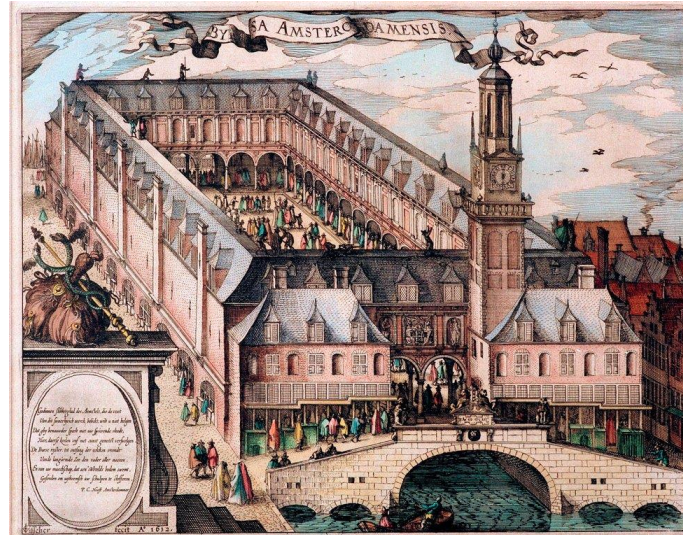
14/ Another parallel are the memes! The Protestants had slogans voicing their resolve to cut out the Church as a middle man:

- Sola Fide (faith alone is enough, no need for a priest), and
- Sola Scriptura (the bible is enough, you can now read it in your own language).

15/ Bitcoiners also have slogans which underscore their resolve to cut out trusted third parties:

- Vires in Numeris
- Don't Trust, Verify
- Not Your Keys, not Your Bitcoin
- HODL

16/ Over to the parallels between the financial economy of the Dutch Golden Age and that of Bitcoin today.



17/ The Dutch perfected deposit banking, with the world famous Amsterdam Wisselbank. We see echoes of heir staunch emphasis on security in bitcoin banking today, which is innovating with trust-minimized solutions such as collaborative custody.

Amsterdam City Hall, which also served as vault for the Amsterdam Wisselbank from 1609 to 1651.



18/16th-17th century maritime trade was risky but lucrative, which was the perfect breeding ground for the insurance sector. In the bitcoin economy we are seeing (proto-)insurance arrangements that resemble Dutch practices.



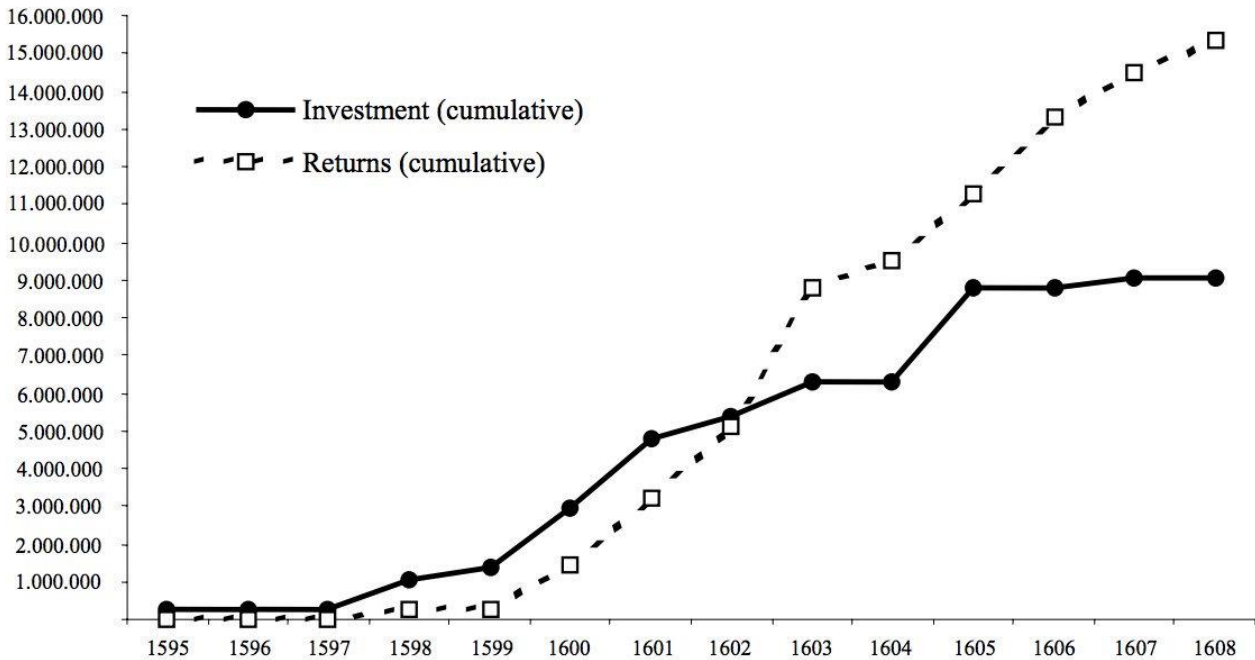


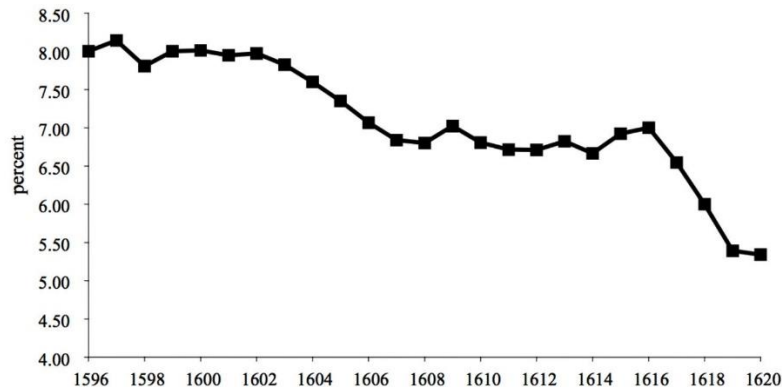
FIGURE 1

CUMULATIVE INVESTMENTS IN THE AMSTERDAM VOORCOMPAGNIEËN AND THE VOC CHAMBER AMSTERDAM, AND CUMULATIVE RETURNS FROM THE AMSTERDAM VOORCOMPAGNIEËN (1595–1608)



19/ The world's first IPO was the East India Trading Company (VOC). Its shares were so liquid and desirable that they were widely used as collateral. Bitcoin is showing similar characteristics, and so may form the base collateral for deep lending and derivatives markets.

HIGH GRADE COLLATERAL



"The drop in interest rates demonstrates the success of Amsterdam's secondary market, funneling a tidal wave of capital into productive purposes, notably short-term loans..."

20/ Finally there's a parallel between how the Dutch accessed capital via annuities, and IEO tokens today which give bitcoin exchanges access to capital. Our report predicts bitcoin based mutual life insurance, which is the next evolutionary step after annuities.

21/ The report's conclusion: "Once in a while, the puzzle of circumstance fits together in a peculiar way... allowing for a spectacle of chain reactions that profoundly reshapes society. This happened 500 years ago, and it may be

happening once more.”

But once in a while, the puzzle of circumstance fits together in a peculiar way, creating fertile ground for many ideas to be adopted at once, and allowing for a spectacle of chain reactions that profoundly reshapes society. The Protestant Reformation was such a time: ideas germinated, rebellion erupted, wounds healed, and a generation of radical entrepreneurs produced an unprecedented series of foundational economic and financial innovations. This happened 500 years ago, and it may be happening once more.

Today we see broad parts of society, millennials especially, acting increasingly critical of central bank interventionism. At the same time technologists, at an accelerating pace, are developing an array of tools that allow for disruption of the economic status quo. In a decade the millennial generation is projected to have the highest earning power of all generations, and this tech-savvy post 9/11 generation has encryption to its disposal as a defensive technology. Meanwhile the bitcoin ecosystem is maturing in all aspects of its economy, in particular in deposit banking, insurance, lending and derivatives, and early forms of life insurance. If this process persists, bitcoin’s layered protocol suite could become a global powerhouse and potential alternative to the IMFS.

Are you ready for the Bitcoin Reformation?

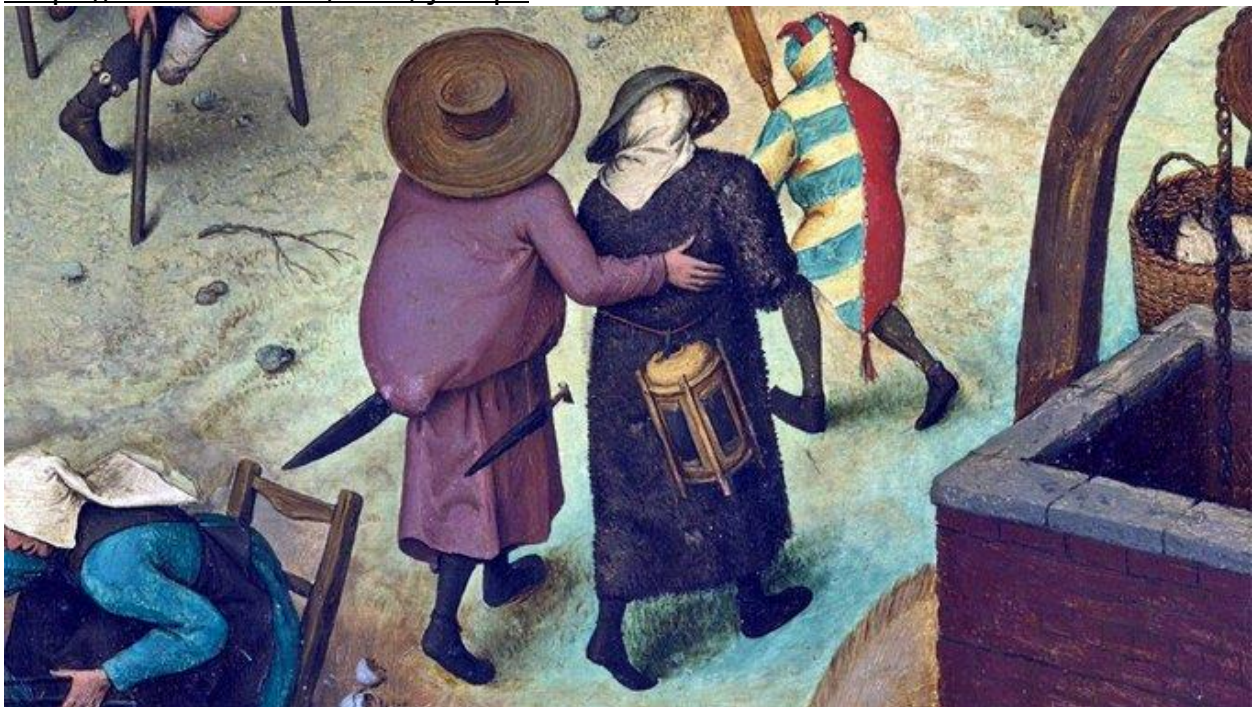
22/ We’ve added a four page chronology of the Protestant Reformation as an appendix. This should help better place the report’s analysis in its historical context.

Brief chronology of the Protestant Reformation, with focus on the Low Countries

ONE EARLY DISSENT

In **1511**, Erasmus of Rotterdam publishes the wildly popular "Praise of Folly," a bold satire of the Catholic church.³⁹ Six years later in **1517** Martin Luther goes public with his "Ninety-Five Theses," a scathing criticism of the rent-seeking practices of the Catholic Church.⁴⁰ Within months, thousands of copies circulate throughout Europe. In response to this perceived heresy against Catholicism, the first book burnings take place in **1521**.⁴¹ In **1522**, king Charles V institutes the Inquisition in the Low Countries for the suppression of heretics.⁴² In **1523** we see the first heretic executions by fire.⁴³ In

23/ Thank you! Once more, here is the link to read "The Bitcoin Reformation":
<https://docsend.com/view/ijd8qrs>



The Triumvirate of Liquidity

By **Nik Bhatia**

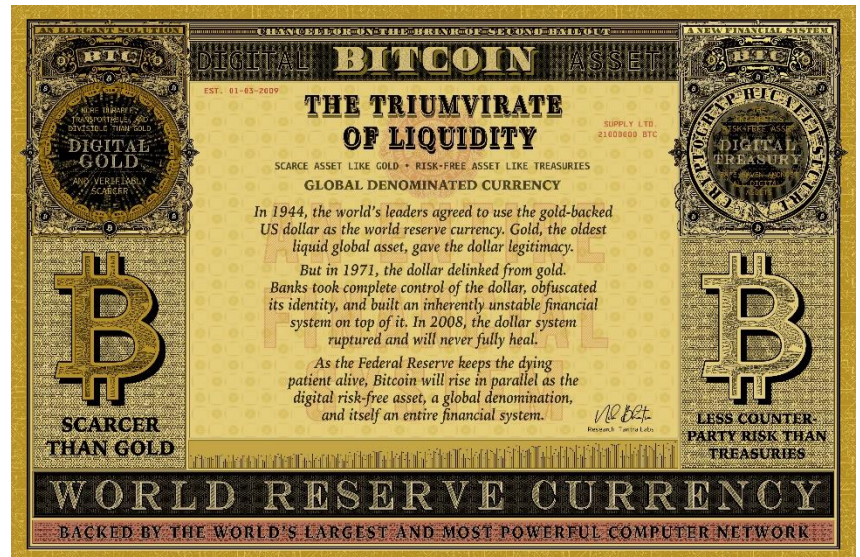
Posted November 6, 2019

Bitcoin is both digital gold and digital Treasuries, and has all the makings of the world's next risk-free asset.

Original artwork by **Lucho Poletti**

Introduction

US Treasuries, gold, and Bitcoin serve as a triumvirate of global liquidity, a powerful trio of safe haven assets that shelter their owners from the risks of our highly leveraged, credit-based monetary system. Of the \$300+ trillion in financial assets around the world, *only* \$32 trillion exist at this echelon of safety and liquidity.



Bitcoin captured an astonishing 1% of the trio's total market value after only eight years in existence, yet this was only a glimpse of the future. In its next chapter, Bitcoin will catapult toward gold's \$9 trillion size, fulfilling its destiny as digital gold. After that, Bitcoin will morph into digital Treasuries and replace them as the world's risk-free asset before eventually achieving world reserve currency status. Replacing the dollar as the world reserve currency is a lofty ambition, but it will occur only as a byproduct of Bitcoin embodying digital Treasuries.

Gold was the dollar's source of legitimacy

Gold is the original liquid global asset, a millennia-old money. The US dollar's gold-backing during the 20th century earned it legitimacy, culminating in the 1944 Bretton Woods agreement in which the world's leaders assigned the dollar as the world reserve currency. Even though gold no longer officially anchors global finance, central banks still hoard it as the world's safe haven asset, presumably as insurance against a dollar system failure. Today, global central bank gold holdings exceed \$1 trillion.



Bretton Woods, New Hampshire, 1944

Dollars, meet Eurodollars

In the 1950s, a new form of dollar emerged in Europe called the Eurodollar, a book-entry dollar to facilitate interbank settlement outside of the United States and outside the Federal Reserve banking system. As Eurodollar usage popularized, banks in London, Zurich, Montreal, and Tokyo gained the power to create the international settlement currency away from any regulatory purview. By 1971, excessive dollar redemptions for gold had depleted the United States' reserves. In order to protect its holdings of the world's safe haven asset, the US ceased all dollar-to-gold conversions, and the dollar officially lost backing. It still, however, had the confidence of global financial participants as their ultimate unit of account.

Treasuries, not dollars

Dollars weren't backed by risk-free assets anymore, so how did investors store dollar reserves safely? Bank deposits are essentially loans to banks and come with an inordinate amount of counterparty risk. Withdrawing truckloads of \$100 bills isn't feasible either, nor does it come with convertibility to an underlying asset. Deposits and cash simply aren't palatable investments for the risk-averse. The solution and capital market tendency is to purchase US Treasuries, a \$23 trillion market, in order to safely store dollars.

The dollar loses its identity

From 1971 to 2007, banks took complete control of the dollar, obfuscated its identity, and built an inherently unstable financial system on top of it.

Eurodollars grew both in supply and sophistication. Banks stopped funding themselves with deposits; instead, they used US Treasuries as collateral to borrow book-entry dollars from each other. A bank license and US Treasuries together wielded the power to create seemingly unlimited money, obscuring money's very definition. The dollar lost all of the identity it once had as a gold claim and became purely a banking liability, a loan to the overly-leveraged financial system. Instead of dollars, Treasuries became the most desirable global asset, not only because of the US government's counterparty superiority, but also because Treasuries possessed omnipotent collateral powers that enabled money creation. Banks use US Treasuries, not dollars, as their risk-free asset, collateral anchor, and primary leverage vehicle.

The dollar system breaks in 2007

In 2007, banks began facing funding pressure. The previous culture of strike-of-the-pen collateralized lending withered away, and banks were unable to roll forward their maturing debt. Banks relied on their ability to constantly issue new debt, and when confidence in them faltered, so did solvency.

For decades, the relationship between dollars and Eurodollars existed without much drama; Federal Funds and LIBOR, the interest rate of each dollar type, mostly mirrored each other. In August 2007, however, LIBOR drifted higher relative to the Federal Funds rate, a sign of acute credit risk in the Eurodollar system. In hindsight, the problem wasn't acute: banks began pulling back from each other as the global dollar system had reached an inflection point. This interest rate divergence foreshadowed the subsequent cascade of dollar-funding shortfalls and bank collapses. The multi-decade free run of money creation had cracked irrevocably.

In 2008, the Federal Reserve bailed out the world by liquifying the entire system. It chose not to discriminate between dollar liabilities and Eurodollar liabilities, and provided a lifeline to any bank or central bank in need by injecting reserves onshore and providing currency swaps offshore. Demand for the safety and liquidity of US Treasuries skyrocketed as they became the world's security blanket, trapping the world in a dollar denomination even though the dollar's long term viability as world reserve currency was irrefutably in question.

Permanent disrepair

The financial system is infected with a chronic disease that won't go away. The dollar is no longer solely the national currency for the United States issued by the Federal Reserve. Instead, the dollar is an international banking instrument without limits, form, or the ability to sustain itself. The system decays as contractions in interbank liabilities cause repeated liquidity shortages for leveraged asset holders. Banks choose not to provide collateralized liquidity to

other banks, even when the collateral is Treasuries themselves. This is the ultimate warning sign that banks don't trust each other anymore. Furthermore, the Federal Reserve always bails out the system as the lender of last resort, permanently eliminating any motivation whatsoever for banks to provide liquidity to each other. The Fed's default response is to create US dollar bank reserves, but this does not address the core problem of broken interbank trust. The Fed only provides a numbing mechanism, keeping the dying patient alive as long as they can.

Bitcoin is digital gold *and* digital Treasuries

What's the endgame? Bitcoin is. Its software is engraved with "Chancellor on the Brink of Second Bailout" to proclaim an elegant solution to our banking system nightmare. Bitcoin is a bearer asset like gold, a risk-free asset like Treasuries, and a currency denomination like the dollar, rising up in parallel over the next couple decades as the infrastructure for the next financial system.



The original newspaper article referenced in Bitcoin's genesis block

Gold and Bitcoin are both scarce assets without counterparty risk, yet Bitcoin's digital final settlement functionality gives it a massive advantage over gold in the coming decades. Bitcoin is not only digital gold though, it's also digital Treasuries. Bitcoin is the safe haven from all other digital assets, just as Treasuries are the safe haven from all other dollar assets. Bitcoin is used as collateral for derivatives agreements just like Treasuries are. But Bitcoin doesn't

have the counterparty risk or supply variability of Treasuries, positioning it perfectly for the forthcoming competition.

Bitcoin is the risk-free asset of the future.

The anti-Bretton Woods

The Bretton Woods monetary system established the dollar as the world's reserve currency in 1944, but the next monetary system will not be determined by agreement between nations. Bitcoin's path to world reserve currency status will occur one asset holder at a time. Thanks to the early-stage Lightning Network, Bitcoin's design now includes an instantly settling currency function in addition to its slower asset function, a characteristic neither Treasuries nor gold possess. But Bitcoin first needs to add *many* trillions in market value to truly compete with Treasuries and gold as an asset class.

Uncertainty demands liquidity

Investors demand risk-free assets when they face geopolitical and economic uncertainty. Securing the liquidity of these assets is paramount when other asset classes experience the brutal combination of increased performance risk and liquidity deterioration that is so common in today's financial world. In this era of dollar system fragility, the **Triumvirate of Liquidity** will reign supreme. Investors will scramble for financial safety, causing intense and persistent demand for US Treasuries, gold, and Bitcoin.

Start [here](#) and [here](#) for a dive down the Eurodollar rabbit hole.

Written by Nik Bhatia [@timevalueofbtc](#)

Original artwork by Lucho Poletti [@LuchoPoletti](#)

Author's opinion only. The views and opinions expressed in this article are those of the author and do not necessarily reflect the position of Tantra Labs SPC, ("Tantra") or any other company. Examples of analysis performed within this article are only examples. They should not be utilized in real-world investment decisions as they are based only on very limited information. Assumptions made within the analysis are not reflective of the position of Tantra or any company.

Non-reliance. The information set forth herein is for information purposes only and should not be relied on or construed as investment advice, counsel, or solicitation for investment in Tantra or any other company. Interested investors

should seek appropriate independent professional legal, investment, and tax advice prior to relying on any of the material contained in this article.

Forward-looking statements. Certain information set forth herein contains forward-looking statements that give a reader the opportunity to understand the author's beliefs and opinions with respect to the future. These statements are not guarantees of future performance of Tantra or any other company and undue reliance should not be placed on them, as they necessarily involve known and unknown risks and uncertainties.

Not a securities offer. This article does not constitute an offer of securities by Tantra or any other company.

Thank you for reading, and stay tuned as we present our ongoing research!

For more about Tantra Labs, check out our introductory post [here](#).

For more from Nik Bhatia, check out his other work on [Medium](#).

For more from Lucho Poletti , check out his [website](#).

For the latest updates, follow us on Twitter [@Tantra_Labs](#).

Op Ed: In China, It's Blockchain and Tyranny vs Bitcoin and Freedom

By Alex Gladstein

Posted November 5, 2019

On October 24, 2019, President Xi Jinping gave a major speech about how China is going to make blockchain technology a national priority. He said China would “take the leading position in the emerging field of blockchain” and explore its use “in people’s daily life.” China’s most-watched daily news show covered the speech in



primetime, and the next day, the *People's Daily* propaganda newspaper ran a front-page story on Xi and blockchain. Searches for “blockchain” on China’s most popular browser Baidu rose 200 percent.

What’s essential to note is that the “blockchain technology” that Xi and his cadre are pushing is a very different type than the one that helps power Bitcoin. The ledger in the Communist Party’s blockchain won’t be updated by proof-of-work and Nakamoto Consensus, but by proof-of-authority. Xi’s blockchains will be highly centralized for maximum control and are meant to be tools for improved surveillance and social engineering. They couldn’t be any farther from Bitcoin, which is open-source, decentralized, censorship-resistant and pseudonymous.

A Blockchain-Based Digital Yuan: ‘Lipstick for a Panoptical Pig’

Unlike the internet — which Beijing can easily manipulate and censor — Communist authorities can’t control the price of bitcoin, and they haven’t been able to effectively stop their citizens from buying and selling the currency. So instead of an outright ban — which would create a huge black market and likely make bitcoin even more intriguing — they have decided to create a competitor. China’s rulers have chosen to try and get out in front of bitcoin and libra by launching a new digital yuan, blockchain only in name and only for marketing purposes. They want to ride the hype of a new technology, and use it as lipstick for a panoptical pig.

According to leadership at the People's Bank of China (China's central bank, known as the PBOC), the goal of the digital yuan is to eventually replace the "MO" base money supply in China. Meaning: they want to replace all paper notes and coins with a digital version based on blockchain technology that's easily surveillable, freezable and confiscatable.

Cash is already an endangered species in China, with the majority of all daily transactions happening via apps like Tencent's WeChat and Alibaba's AliPay. The transformation in payments over the past decade from paper cash to social media platforms has been very helpful for China's police state, given that they can ask companies like Tencent for information on users any time. But a currency that, itself, is a surveillance platform – that would suit the state even better.

A Dictator's Dream: Eliminating Third-Party Cooperation for Surveillance

Today, the Communist Party is forced to work with third parties like commercial banks and technology companies to control and understand the flows of money. In a future scenario with a successful digital yuan, the Central Bank itself could have a real-time understanding of where all the nation's currency is and where it's going. This kind of omniscient financial surveillance is a dictator's dream.

The main goals of the digital yuan blockchain project are clear and have been stated publicly by various government officials repeatedly over the past two years:

1. to replace cash with a trackable digital currency
2. to popularize the Yuan around the world
3. to circumvent sanctions, U.S. and otherwise
4. to undermine SWIFT and the existing global payment network
5. to temper public hunger for bitcoin and other cryptocurrencies
6. to condense what is currently a huge patchwork of different banks and companies into a single, easily knowable ledger

From what has been publicly revealed so far, the digital yuan will be minted by the PBOC and then sold to banks and companies, including Tencent and Alibaba. According to statements from PBOC leadership, users would download a mobile wallet and exchange their existing money for the new digital yuan. Then they could start using that for their daily spending habits.

Every time a transaction happens, the government would know about it in real time, instead of having to ask a third party. Transactions would be protected with cryptography to reduce theft, with only the formal owners being able to

move assets. The exception, of course, would be Xi Jinping and the Communist Party, who would have a backdoor into anyone's wallet.

Economic Support for Political Oppression

At a time where the PBOC is running out of options to stimulate China's economy in the event of another recession, the digital yuan could give them new ways to fight a downturn. Consider: They could, with the click of a button, put a chunk of new digital yuan precisely into the personal account of every university student or every auto worker. In this way, Communist Party officials would be using blockchain technology to prolong the lifespan of a regime that is built on cruelty and fear. Remember: Xi Jinping is currently presiding over the internment of millions of Muslim-minority Uighurs in prison camps; the ongoing and nearly complete cultural genocide in Tibet; the crushing of democracy in Hong Kong; constant threats to "solve" the Taiwan problem; and the expansion of the Belt and Road, the largest infrastructure project in human history, which is installing surveillance technology and telecommunications across the developing world in a wave of digital colonialism. To move the digital yuan forward, the Communist Party is already educating Chinese citizens about blockchain technology in a variety of ways. Xuexi Qiangguo — the most popular app on China's Apple store — has added informational content on blockchains, just as state media and official government apps have popularized the subject. Just a few days after Xi's big speech, the Communist Party even launched a new phone app (called "Original Intentions Onchain") to encourage members to pledge their loyalty to the party "on a blockchain." Behind all of this is Beijing's overarching goal to strengthen control over its economy and exert financial sovereignty. Xi Jinping doesn't want the U.S. dollar or libra or bitcoin in the leading global position. He wants to win the new currency space race, and he's chosen to do it by putting the yuan on a centralized, digital ledger.

A Threat to Human Rights

Short term, this could be a big win for Xi and a big loss for human rights. If the technology works as planned, and can be rolled out fast enough, the digital yuan could soon be the financial backbone for not just all of China but for all of the dozens of "Belt and Road" countries from South Asia to Latin America. What's more, China moving forward aggressively to create a digital national currency will spark ripple effects of interest from governments and corporations who may follow in Beijing's footsteps and set up their own surveillance stablecoins.

We should have no doubts about their intentions or capabilities, and if we care about human rights and freedom, we should not cheer them on.

But long term, this could be a strategic blunder on a titanic scale. Bitcoin's ability to separate money from state by creating a parallel economy beyond government control represents one of the only things that could challenge Xi Jinping's totalitarian goals. And, unfortunately for him, it's hard to imagine that he can preside over a massive public blockchain education program for hundreds of millions of people, without more and more of them eventually waking up and learning about Bitcoin.

A Trojan Horse for Bitcoin and Freedom?

It's one thing to censor the internet. The regime can make mention of Tiananmen Square forbidden, and people by and large won't risk their livelihoods to learn about what happened on June 4, 1989, and gossip to their friends about taboo topics. But it's another thing entirely to keep people away from a well-performing financial asset with no barrier for entry. Governments can keep people off the internet, but it will be a lot harder to keep people off Bitcoin.

In "The Matrix," the protagonist Neo is given a choice by Morpheus to take the blue pill and stay in his known world of comfort and safety, or take the red pill and risk going down the rabbit hole. The digital yuan is the blue pill. And there are many people who are fine with the blue pill — perhaps even a large majority — who are happy to comply with the rules and who don't want to risk their comfortable, convenient situation by doing anything that could put their status quo in jeopardy.

But there are also plenty of Neos in the world, and there will be many people who want to take Bitcoin's red pill, especially when it's uncensorable, hard to track, and increasing in price year-by-year against a digital yuan whose value may struggle.

The Communist Party wants to ride the "blockchain" hype cycle and create a new currency of unprecedented surveillance and control. And they may succeed, at least in the short term. We should have no doubts about their intentions or capabilities, and if we care about human rights and freedom, we should not cheer them on. The only silver lining is that ultimately, the digital yuan may end up being one big Trojan Horse for Bitcoin, where Satoshi Nakamoto — not Xi Jinping — gets the last laugh.

An Open Letter to Ray Dalio re: Bitcoin

An open letter to hedge fund colossus Ray Dalio regarding his worldview, the forces of financial nature, and how Bitcoin is bound to reshape both.

By Robert Breedlove

Posted November 8, 2019

Introduction

Ray, your ability to penetrate the opaque realm of economics and share its secrets in an easy to understand language is one of your greatest gifts to humanity. With your videos, openly published research, and authorship, you have opened the eyes of many to a topic most consider too difficult to comprehend. The world needs more pioneers like yourself writing easy-to-read maps for the nearly incomprehensible territory of economics.

Macroeconomists, Academics and Central Bankers rely heavily on deceptive language and universal public ignorance to perpetrate their schemes; your work in converting this esoteric domain into a more exoteric form is therefore commendable.

Let me begin by saying that, like you Ray, I consider myself a “dumb shit” who is more focused on dealing with what I don’t know rather than relying on what I do know to navigate life and work – a mindset well accorded with ancient wisdom:

“All I know is that I know nothing.” – Socrates

Epistemic reach is finite, as knowledge cannot explain everything in the world and, often, it clouds the truth. So let us explore the territory of economics with a beginner’s mind, free of the accumulated clutter commonly called



“conventional wisdom”. It is from this frame of mind that I present to you this open letter regarding your perspective on Bitcoin through the lens of your stated principles on life and work (in this letter, I sometimes direct my comments at Ray, and sometimes at the audience, so please bear with these shifting perspectives).

We begin with an evaluation of Ray set in the idea-meritocratic style practiced at Ray’s firm, Bridgewater. The purpose of these evaluations is to grade your peers candidly, being brutally honest and holding no punches, to ensure that the best ideas rise to the surface – unimpeded by policy, politics, or hierarchy – so that they may be scrutinized and, if useful, acted upon. In Bridgewater’s culture, communication is both top-down and bottom-up, so that people feel empowered to share their honest perspectives. For Ray, it’s all about getting to the truth by any means necessary, and I appreciate his blunt approach. We will explore all of this more deeply below – so let’s dive in.

Evaluation of Ray’s Assessment of Bitcoin

Subject: Ray’s Assessment of Bitcoin

From: Robert Breedlove

To: Ray Dalio

Cc: Everyone

Attachments: Ray’s assessment of Bitcoin available here –

<https://www.youtube.com/watch?v=UyVluNI797w>

Ray,

You deserve an “F” for your assessment of Bitcoin’s significance and future prospects. Although there are very few of us, everyone who has the requisite depth of understanding in the fields of computer science, monetary history, game theory, economics, and mathematics, and has spent the time intensely studying Bitcoin (it takes a lot), agrees with this harsh evaluation of your short-sighted assessment of this momentous monetary innovation. As one of your biggest fans, I truly believe that if you take another look (a long, hard, thoughtful look), you will see the light. Specifically, your assessment fails for the following three reasons:

1. You claim that you are sold “blockchain technology”, despite the only proven use case for “blockchain technology” is as a component of Bitcoin. Contrary to “conventional wisdom”, the real breakthrough is Bitcoin, not blockchain.
2. You state that Bitcoin could be disrupted by another “cryptocurrency”, however this extremely unlikely: Bitcoin is a path-dependent, one-time invention; its critical breakthrough is the discovery of absolute scarcity – a

monetary property never before achieved by mankind. The emergence of Bitcoin cannot be reproduced because absolute irreproducibility is the discovery! The iPhone disrupting Blackberry analogy you cite is irrelevant; Bitcoin is a protocol, not a consumer product.

3. You state that price-stable, central bank issued currencies will be issued, which will likely be attempted, but such currencies would be antithetical to free markets. Further, price stability is an illusion: all economic goods move against one another in ratios of exchange, money is simply the most marketable good, hence the reason money-denominated exchange ratios (prices) tend to be more stable, but are still subject to supply and demand interaction. Since Bitcoin is absolutely scarce and cannot be stopped, it is likely to continue outcompeting all other monetary technologies on the free market. As an economic good monetizing in real time, the exchange ratios between Bitcoin and various fiat currencies is likely to remain volatile for some time, but this volatility will continue to subside as Bitcoin's market capitalization grows, thus making its use as a medium of exchange more practical, before reaching a point of sufficient network value where prices will come to be more commonly expressed in Bitcoin terms (similar to the evolutionary phases gold underwent during its monetization process).

Your assessment is especially disappointing for three reasons: 1) You have consistently exhibited a knack for comprehending, distilling, and communicating highly complex economic concepts in a manner palatable for general audiences, 2) The depth of knowledge you possess in history, economics, and free market dynamics presents you with a privileged position to best understand the emergence of and demand for this asset, and 3) Your virtually unparalleled reach and reputation as a macroeconomic thought leader, organizational engineer, and cultural innovator is an invaluable platform from which to trumpet to the dire circumstances faced by the prevailing economic order and how Bitcoin has the potential to alleviate them.

In the following open letter, I will show that the fundamental tenants of your worldview, as stated in your book Principles and other writings, are fully consistent with Bitcoin – even though you may not yet realize it. I'll begin with two primer sections: one on the nature of money and its history, and one on Bitcoin's general functionality and economic properties – either or both may be skipped by the reader who has “already fallen down the Bitcoin rabbit hole”, so to speak. After these primers, I will walk through many of Ray's most important Principles, one by one, and break them down to better understand their relationship to markets and Bitcoin. Let's begin.

Primer on Money

(this Primer on Money and the following Primer on Bitcoin may be skipped by the reader who understands the traits of money and Bitcoin's general functionality/economic properties)

Money is a tool for moving value across time and space (or spacetime, as Einstein explained, these are actually one in the same). Money is an emergent property of barter (or direct exchange) that purports to solve the three dimensions of its non-coincidence of wants problem; it evolves naturally in the free market as the most exchangeable good in an economy. Although he is silent as to its origins, Ray understands the technological functions of money, as stated in his video assessment of Bitcoin (see open letter attachment above) that the primary functions* of money are:

1. A store hold of wealth: also called a 'store of value' in regard to moving value across time (the first function and evolutionary phase of money)
2. A medium of exchange: in regard to moving value across space (the second function and evolutionary phase of money)

**We will ignore for now the third function and evolutionary phase of money, unit of account, as it isn't pertinent to our discussion here.*

Although the purpose of money always remains the same, to move value across spacetime, the technology fulfilling this purpose is constantly being subjected to market-driven evolutionary pressures. The greater a monetary technology's resistance to value dilution across time — whether by counterfeiting, supply inflation, or deterioration — the more effective it is as a store of value. Once a store of value accrues enough value, people begin to use it for trading purposes. The more widely accepted a form of money is, the higher its value as a medium of exchange, which makes this aspect of its value proportional to the number of its monetary network participants (aka users). When a specific monetary technology, in the form of an economic good, becomes widely accepted in interpersonal exchange (aka trade) it is called "money". Monetary technologies compete to become more widely adopted based on the following traits:

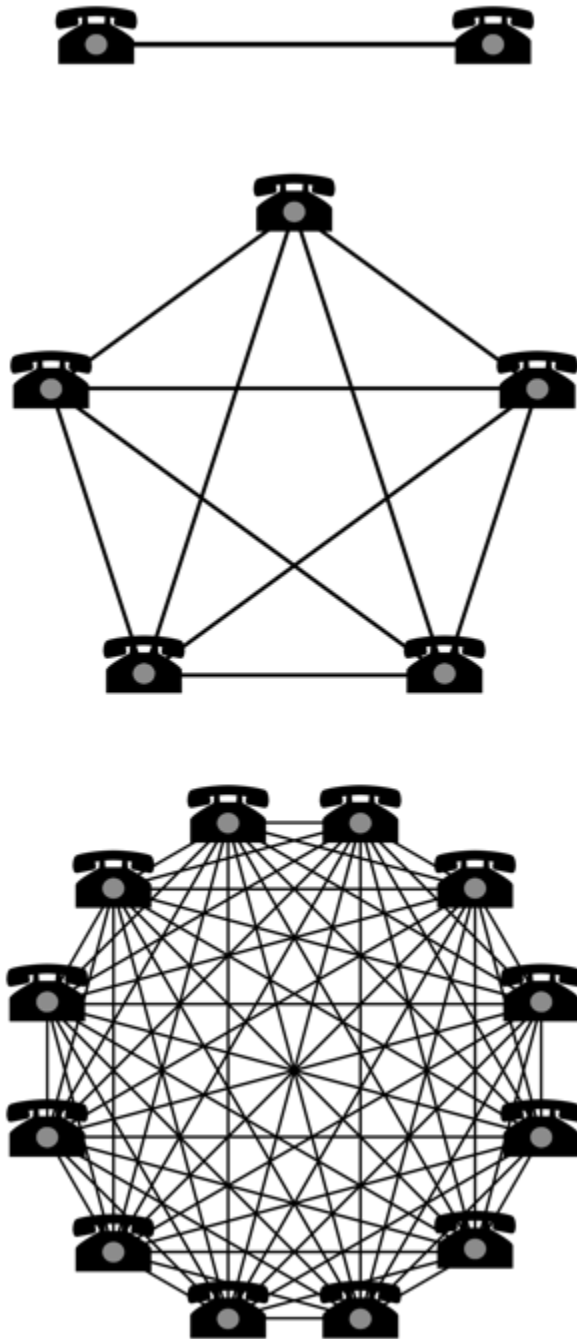
1. Scarcity: resistance to money supply manipulations and, thus, dilutions to its monetary unit value (difficult to produce)
2. Divisibility: ease of accounting and transacting at various scales (separable and combinable units)
3. Portability: ease of moving value across space (high value-to-weight ratio)
4. Durability: ease of moving value across time (resilient to deterioration)

5. Recognizability: ease of identifying and verifying the monetary value by other parties in a transaction (universally identifiable and verifiable)

Due to the relative advantages competing monetary technologies offer, the particular economic good being used as money can, and does, change over time. Throughout history, mankind has employed seashells, salt, cattle, precious metals, and government paper as money, to name a few. Similar to the price discovery process in a free market – where the collective actions of buyers and sellers are continuously compressed into a single actionable variable called the market price – competing monetary technologies undergo a market-driven discovery process. We can gain a better understanding of this dynamic through an analogy: monetary evolution is (roughly) comparable to the evolutionary process we see in communications technologies.

No matter what specific means is used to fulfill it, the purpose of communications technology remains the same: to move information across spacetime. Similar to the market for money, competition is at all times alive among different communications technologies, in which they are all subjected to a market-driven discovery process. As newer technologies are invented they are market-tested through competition; each survives or dies in terms of its relative speed, message fidelity, reliability, traceability, and mobility. Since these technologies have a singular purpose, people tend to adopt a common technology, a coalescent process that is propelled by network effects.

Network effects, defined as the incremental benefit attained by adding a new member to a network for all of its existing participants, drive people to adopt a primary form of communications technology. As more people migrate to the latest and greatest technology, it encourages others to do the same, as more network participation exponentially increases the number of possible connections. A simple example of this is the telephone: with two phones in existence, only 1 connection is possible; with five phones in the network, the number of connections jumps to 10; and with twelve networked phones, the number of connections increases exponentially again to 66, and so on. (see Metcalfe's Law for a directional explanation of this network effect dynamic):



Network values are based on the number of possible connections they enable; they grow exponentially with the addition of each new constituent (or node)—this property is called network effects.

Since the purpose of communications technology remains singular (moving information across spacetime) despite technological advances, whichever technology is best at fulfilling this purpose has a tendency to become dominant in the marketplace. This tendency, reinforced by network effects, has driven communications technology evolution from carrier pigeons to telegraphs, to the internet today. This is an expression of the winner-take-all (or, winner-take-most) dynamic inherent to many networks, including those of the communications and monetary technology varieties.

Similar to the purpose of communications technology, the purpose of monetary technology is singular: to move value across spacetime. The various monetary technologies used to fulfill this purpose, however, undergo market-driven discovery and, thus, evolve over time based on their respective monetary traits. In respect to the traits of money, the one that takes primacy in determining a specific monetary

technology's likelihood of success in the free market is its hardness (also called the scarcity or soundness of money). This trait is of primary importance because it determines a money's usefulness as a store of value, and a money that cannot adequately store value across time necessarily cannot transmit value effectively across space. The relative hardness, or scarcity, of a competing monetary technology is quantified by its stock-to-flow ratio, a valuation metric also common in precious metals markets such as gold:

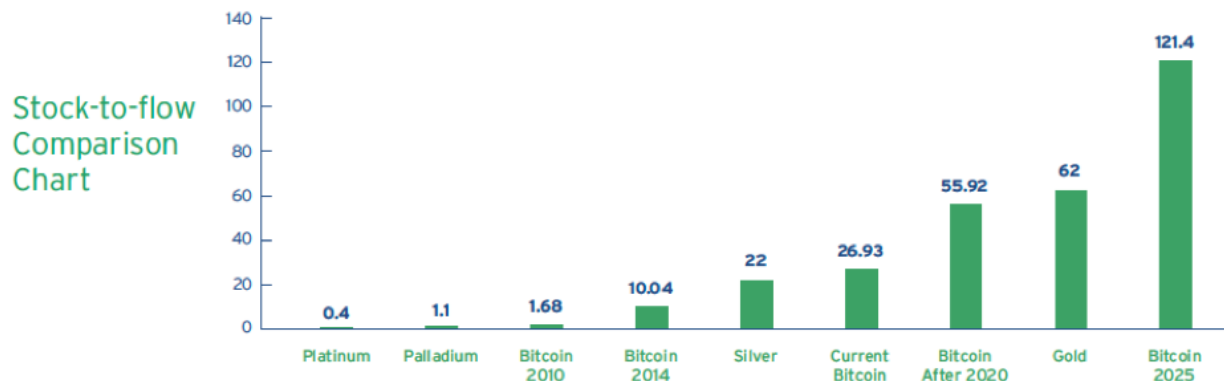
- Stock is the existing unit supply of monetary units (for example: ounces of gold, quantity of US Dollars, or quantity of Bitcoin)
- Flow is the newly created supply over a specific time span, usually one year
- The stock-to-flow ratio is calculated by dividing the stock of monetary units by its newly created supply flow (can be thought of as the inverse of inflation)
- The higher the stock-to-flow ratio, the greater the hardness (also called soundness or scarcity) of the monetary technology

We can think of monetary hardness as the difficulty (or cost) necessary to produce an incremental unit of a monetary technology. For instance, the capital and operational expenditure necessary to extract an ounce of gold from the ground is the basis of its monetary hardness. As producers of gold will always seek to extract it until their incremental cost per ounce is equal to their incremental revenue per ounce (in other words, until marginal cost equals marginal revenue), there is a perpetual financial incentive for producers to maximize new supply flows up to the point of economic breakeven. In comparison to communications technologies, money exhibits much stronger centripetal, winner-take-all network effects that drive users to adopt a single store of value. Those who fail to adopt the hardest money available to them face a debasement of their stored value by those who can produce it at an incremental profit (where $MC < MR$). Hard money, then, is simply the monetary technology freely selected in an unobstructed marketplace as the most sound store of value available. Historically, gold prevailed as hard money precisely because of its superior stock-to-flow ratio relative to other monetary metals:

Table comparing SF ratios for gold, silver, palladium and platinum

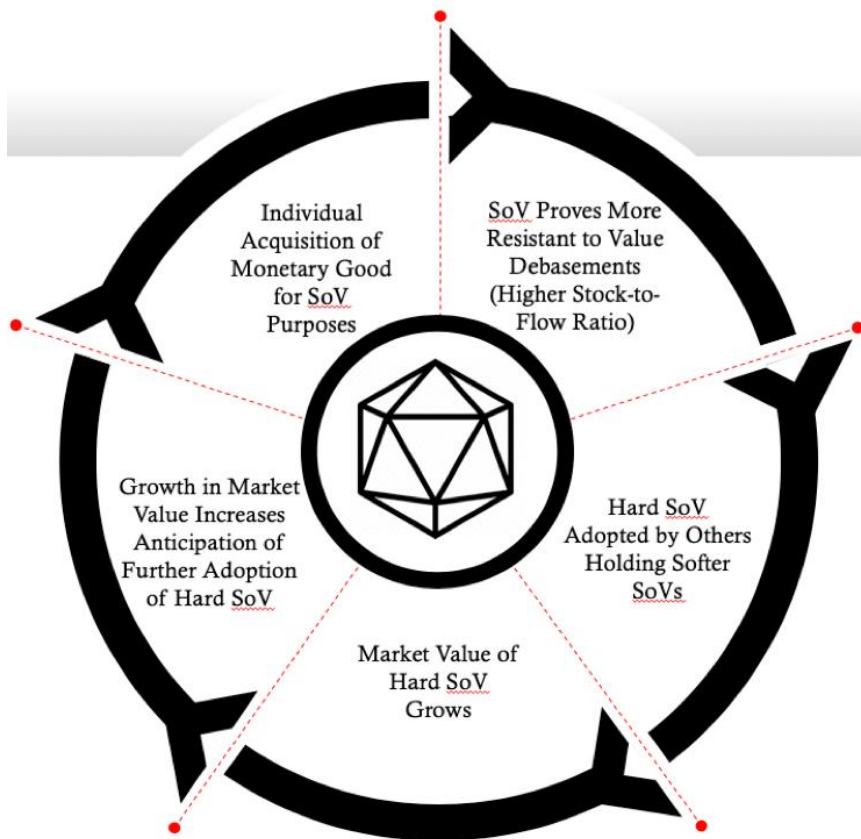
	Stock (tn)	Flow (tn)	SF	Price \$/Oz	Market Value
Gold	185,000	3,000	62	\$1300	\$8,417,500,000.000
Silver	550,000	25,000	22	\$10	\$308,000,000.000
Bitcoin (BTC)	15,200,000	656,250	23	\$11,500	\$174,800,000,000
Palladium	244	125	1.1	\$1400	\$11,956,000.000
Platinum	86	229	0.4	\$800	\$2,400,000.00

Gold has the greatest SF ratio. At the current flow rate, it will take 62 years to generate the same amount of stock that is currently available. Silver is second, it will take 22 years of silver production to generate the same amount of stock that is currently available. It is clear to see that as Market Value increases as SF ratio also increases.



Relative supply scarcity, as quantified by the stock-to-flow ratio, is a key driver of monetary value.

On the free market, people naturally and rationally choose to store the value created by their work in the monetary technology that is hardest to produce, since producing new units dilutes the value of existing units for all holders of said money. Since gold exhibits superior monetary hardness, it has outcompeted silver and other monetary metals several times throughout history. Gold outcompetes due to the game-theoretic aspects of an evolving store of value:



Propelled by network effects and relative supply scarcities, people coalesce around a single store of value.

Since gold is virtually indestructible, nearly every ounce mined throughout human history remains part of its extant supply; and since gold is relatively rare in the Earth's crust, its new supply flows are a small percentage of its existing stock each year. Taken together, these properties give gold the highest stock-to-flow ratio of

any monetary technology in the world (before Bitcoin), meaning that its supply inflates at a relatively low and predictable rate. Superior hardness is precisely why gold became the dominant monetary technology on the free market.

Game theory tells us, and market history proves, that anyone who can, for instance, profit from silver production by selling it at a higher price than it cost to produce, has a direct financial incentive (the protection of value across time) to store any profits generated in the hardest form of money available to them. As all market participants are subjected to this harsh economic reality, this persistent incentive triggers investment flows from silver (or any other softer monetary technology) to gold (or the hardest form of money available). In this way, free market competition causes people to converge on a single store of value and, therefore, perpetually promulgates hard money. This is not surprising, as free markets tend to zero in on the best possible technological solutions to problems, discarding the rest. And conceptually, in the same way that money is an emergent property of a direct exchange (barter) economy, hard money is an emergent property of an indirect exchange (monied) economy.

The physicality of gold gives it both advantages and disadvantages. Being a precious metal that achieved its monetary value on the free market, gold is a self-sovereign monetary technology, meaning that its value, trust factors, and

transactional permissibility as money are not subject to any counterparty risk whatsoever. In other words, gold is equity-based money or a bearer asset. If someone flips you a gold coin and you stick it in your pocket and walk away, then you have just participated in an irreversible transaction. The value of this coin is set by the market and whosoever is in physical possession of it is assumed to be its rightful owner. No bank or payment intermediary can censor or reverse this free market transaction. You have no need trust anyone else, whether you choose to hold or spend your gold. Self-sovereignty is a quality uniquely intrinsic to bearer assets such as gold, silver, or diamonds.

Contrarily, if someone hands you a US Dollar, you assume the counterparty risk of the US Government, who can dilute its value via supply inflation (as we see with all fiat currencies throughout history) or deauthorize its value altogether (as we saw when India deauthorized its 500 rupee bank note). Further, if you received this US Dollar through a payment intermediary, like Paypal or Venmo, you are also exposed to the risk of this payment being censored, reversed, or surveilled. Even when physically hoarding fiat currency, it is still vulnerable to supply inflation as its central bank backer can simply print more, stealing the value stored therein. By transacting in anything other than a bearer asset, which is valued solely based on free market dynamics, you forfeit your personal financial sovereignty to the currency issuer and/or other financial intermediaries.

Although gold's physicality gives it the property of self-sovereignty, it also comes with inherent disadvantages. Its primary drawback is its suboptimal divisibility. Since gold has such high value to weight, it is impractical to pay for coffee using gold coins, for instance. This drawback of gold is what gave silver some utility as a medium of exchange throughout history, as its value to weight was much lower making it more practical to use for everyday purchases (due to its higher divisibility and portability), whereas gold was typically reserved for settling large transactions.

Eventually, gold's divisibility problem was "solved" when central banks which began issuing paper currencies which were fully redeemable for gold. This provided users with a hybrid monetary technology that exhibited the hardness of gold, while offering an ease of transactability (high divisibility and portability) even greater than that of silver. With its marginal utility disrupted by paper currencies (and later, electronic abstractions of paper currencies), silver became completely demonetized and eventually the entire world market for money evolved to a paper-currency-enabled gold standard.

With transactions being executed in gold-backed paper currencies, the global gold standard led to the centralization of gold within bank vaults. These gold hoards became too tempting for governments and their central banks to resist expropriation of, thus catalyzing the fractional-reserve banking practices now ubiquitous in the modern world economy. As governments created more

currency units than they could support with their gold reserves, they started revoking currency redeemability for gold, which culminated in the 1971 unilateral decision by US President Nixon to permanently sever the peg to gold (deceivingly, it was declared to be a temporary measure):

<https://www.youtube.com/watch?v=iRzr1QU6K1o>

Since all other currencies in the world were pegged to the US Dollar, this final act of financial sovereignty usurpation officially abolished the gold standard worldwide. This death-stroke to monetary integrity brought us into the age of the “political debt-based money backed by the future cash flows of taxing authorities” we all are legally coerced into using today – fiat currency. With fiat currencies came the limitless inflation suffered episodically all over the world. Inflation comes to us from the Latin verb *inflare* meaning “to blow up”. This is an apt description since once it sets in, fiat currency inflation has only one possible outcome – dilution into worthlessness:



Central banking made many Zimbabweans the first broke-ass trillionaires, but certainly not the last.

Since breaking its peg to gold, the US dollar has lost over 97% of its relative value. The fiat currency printing press has proven to be the weapon of choice for political leaders to further their agendas and enrich themselves; it has also become the primary means for funding perpetual warfare. During the past century of central banking – which cunningly imposed its dominion over a large swath of the world’s gold supply through coercion and confiscation – there has been unprecedented per capita death in warfare, an ever-widening wealth disparity, and an incessant sequence of economic boom and busts fueled by the continual marginalization of paper currencies and, ultimately,

the instantiation of fiat currencies. Today, all semblance of monetary integrity and sanity has been destroyed with citizens left optionless, forced to transact in softest form of money in history.

In the wake of the latest (and arguably the greatest) fiat-currency-fueled economic bust, the 2008 Great Recession, when central banks all over the world were busy printing more fiat currencies to recapitalize their financial institutions via the shadow tax of inflation, Satoshi Nakamoto released an open-source software project into the world. He, she, or they called it Bitcoin.

Primer on Bitcoin

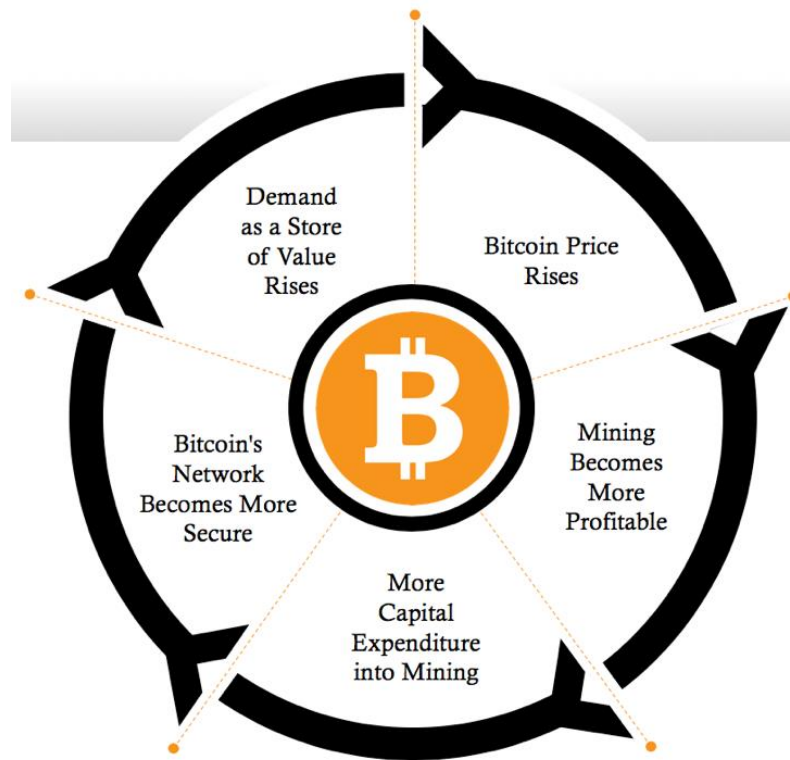
(again, this Primer on Bitcoin may be skipped by the reader who understands Bitcoin's general functionality/economic properties)

Bitcoin can be thought of as the first incarnation of self-sovereign money in digital form. Its transactions are irreversible, uncensorable, and unstoppable. In other words, Bitcoin is the world's first digital bearer asset. Possession of Bitcoin is achieved by holding its private key, which is an alphanumeric data string that can be stored in analog, computer, or even human memory. Its absolutely scarce money supply is anchored to the most fundamental commodity in the universe – energy.

Bitcoin's stock-to-flow ratio, the measure of its monetary hardness, increases (inevitably) every 4 years and will be about twice that of gold after its 2024 downward inflation rate adjustment (the halving); at this point, Bitcoin will definitively be the hardest form of money that has ever existed. Bitcoin's uncompromising, apolitical monetary policy is enforced by unbreakable cryptography, hence this inevitability (as sure as $1+1=2$). Its unrivaled hardness is made possible by an ever-rising production difficulty that requires expenditure of real world energy in a process called proof-of-work. This anchor to economic reality is also called mining – in an ode to the difficulty of gold production – and is the source of Bitcoin's monetary integrity.

Bitcoin is also the world's first asset with perfect supply inelasticity, as changes in its price have absolutely no impact on its supply flow. This means changes in demand for Bitcoin can only be expressed in its market price. If the price of gold increases, its new supply flow will increase as new miners enter the market and new methods of gold mining becoming economically feasible (since the gold miners can sell their product at a higher price), thereby applying downward pressure to its stock-to-flow ratio. With Bitcoin, no matter how much its price increases, it is absolutely impossible to create any new supply flow beyond its mathematically enforced and universally transparent issuance schedule. Also, a higher market price means a more secure Bitcoin network, as the resources allocated to mining are used to secure it. Like a vault with walls that thicken as more value is stored within it, Bitcoin adapts to

become a more secure monetary network as its market capitalization grows. Absolute obstinance of the algorithmically enforced Bitcoin monetary policy drives a virtuous cycle that perpetuates the expansion of its network:



An ingenious composite of unbreakable cryptography and economic incentives causes Bitcoin to grow relentlessly.

Bitcoin's money supply is absolutely scarce, meaning its monetary policy (or money supply) is fixed – only 21M units will ever exist. Before Bitcoin, only time itself exhibited the property of absolute scarcity. This means that its stock-to-flow ratio will continue to increase and eventually become infinite when the last Bitcoin is produced

sometime in the middle of the 22nd century. Bitcoin's monetary policy is becoming the most trusted in the world as it is fully transparent and unchangeable.

Bitcoin runs countervailing to government monetary policy which is uncertain, opaque, and subject to change based on the whim of bureaucrats. Essentially, we each must decide if we are to trust the whimsical nature of self-interested bureaucrats or the inviolable nature of mathematics to manage our money supply. Shockingly, whether we decide or not, the harsh economic reality of Bitcoin's superior hardness is likely to be imposed upon us all, as history teaches us the economic consequences of hard money cannot be ignored. As we saw earlier, the free market for money is winner-take-all. Critically, Bitcoin is open-source, like a spoken language, and it is transcendent of regulations and the legal insulations that preserve the monetary monopolies of central banks.

So we have Bitcoin, the hardest form of money in history, competing directly with government money, the softest form of money in history. So long as Bitcoin continues to exist, it will likely continue to outcompete gold and fiat currency in the free market, and its market capitalization will grow. Eventually, each and every holder of any softer form of money (whether its gold or fiat currency) will be faced with the grim reality of a gradually, then suddenly,

depreciating asset relative to Bitcoin's ever-constricting new supply flow. Imposition of this harsh economic reality will be applied persistently and each of us will be faced with the same mathematical and market-driven dynamic that has catalyzed the evolution of money throughout history.

Hard money, as selected on the free market, reigned for the first 4,900 out of 5,000 years of human commercial history and all signs indicate we are witnessing its reemergence in the rise of Bitcoin. Before government intervention, money supply was not a matter of policy, but instead was governed by game-theoretic principles, a "policy" rooted in natural law. Since governments have imposed monetary monopolies in the form of central banks, trust has steadily been eroded in their ability to prudently maintain money supplies. Said differently, Bitcoin is the most credible monetary policy in human history disrupting the most untrustworthy monetary policies in human history. A bet on Bitcoin is that the competitive dynamics inherent to the market for money will continue to play out in the same way they have throughout all of history, thus making money supply a matter to be determined once again by the free market instead of central planners.

Armed with these primers on money and Bitcoin, we will now dive deeper into the various principles that comprise Ray's worldview. Through this exploration, we will gain a more fundamental understanding of history, markets, and Bitcoin. We begin with Ray's most renowned cultural creation — the idea meritocracy.

Idea Meritocracy

(p.540) "Idea-meritocratic decision making is better than traditional autocratic or democratic decision making in almost all cases."

At the pinnacle of Ray's worldview is the cultural paradigm he originated at Bridgewater — the idea meritocracy. As a distinct organizational style, it's intended to eliminate all barriers to the free flow of information between people — including ego, hierarchy, and personal agendas. An idea meritocracy seeks to align itself with reason and become impervious to politics. As Ray puts it, (p.306) "Power should lie in the reasoning, not the position, of the individual. The best ideas win no matter who they come from." Essentially, an idea meritocracy is a free market for ideas — a way of filtering ideas via a (simulated) form of natural selection. Instead of charging ranked positions with the authority of decision-making, an idea meritocracy attempts to foster an environment in which the ideas compete freely based on their own merits:

The idea meritocracy: an open environment for the proliferation and combination of the most meritorious ideas, free from manmade impediments such as ego, policy, and hierarchy.

As a free market capitalist, it is unsurprising that Ray developed this approach to organizational culture, as it has proven to be the most effective system for the most people. It was (repeatedly) well established in the 20th century that free markets (capitalism) function better than centrally planned markets (socialism). At the heart of any economic system is the problem of properly adapting resource allocations to the circumstances faced by people at any particular point in spacetime. In other words, the core economic problem is how to best distribute current knowledge of relative value and scarcity. Knowledge is intrinsically superfluid: it resides within many minds and is constantly changing in accordance with the ceaseless interpersonal interactions among individuals and their assessments (and reassessments) of market realities. The challenge of an economic system is to enable quick, continuous, and effective assimilation and dissemination of this knowledge to properly guide entrepreneurial actions.

Naturally, individual entrepreneurs are always most familiar with the prevailing economic circumstances specific to their time, place, and industry. As they see, hear, and touch the productive factors and influences most pertinent to their domains on an almost daily basis, entrepreneurs gain and maintain an intimate understanding of the ever-changing conditions relevant to their chosen occupation. Said differently, knowledge has a localized dimension to it: it surfaces continuously at all points in spacetime where entrepreneurial actions (involving decisions and trade-offs) and economic realities (involving value and scarcity) interface. Therefore knowledge, by its very nature, is inherently distributed among the minds of many. And free markets, comprised of entrepreneurial actions guided by accurate price signals (more on these shortly) are the best assimilators and disseminators of these localized pools of knowledge within an economy. Simply, the free market is a nexus in which many minds effectively become one.

Capitalism is an economic system that deals with the distributed nature of knowledge in a true-to-life, bottom-up way. In a free market, each entrepreneur is unobstructed to operate in his own best interest in pursuit of profits. Contending with the ever-present realities of value and scarcity, the actions of entrepreneurs, like the actions of a pilot guiding his aircraft via his navigational instruments, are guided by the market prices relevant to his profession. This is free market capitalism: a seemingly chaotic bricolage of entrepreneurial decisions, price reconfigurations, and capital flows coming together in a unified orchestration that harmonizes individual and collective self-interests.

For instance, let's consider the case of Larry the lemon farmer. Being a farmer, Larry is primarily conscious of the cost of fertilizer, soil, and water; and keenly aware of his total cost structure relative to the expected market value of his lemon crop, as maintaining total revenues above total costs is necessary for

entrepreneurial survival. Should a drought strike and drive up the scarcity of water, Larry will become aware of this economic reality through the increased price of water which will, in turn, cause him to increase the selling price of his lemons or cut costs elsewhere to maintain his profit margin. Critically, Larry can respond effectively to this drought based purely on the increased price of water without any direct knowledge of the drought itself or its causes. As entrepreneurs choose to buy and sell the various productive factors related to their occupations, the knowledge in their minds becomes encapsulated in and distributed by the prices of these factors to everyone else in the world who interacts with them in the marketplace.

As new experiences provide feedback that change the state of knowledge, entrepreneurs must be left free to rationalize their own economic affairs, take risks in accordance with their rationalities, and operate in an environment free of coercion or violence that would otherwise disrupt their business dealings. Government is intended to be this protective force, which uses its monopoly on violence to prevent violence within society, thus preserving the rule of law and people's rights to private property. Unhampered, free market competition among entrepreneurs ensures that only those adding value to society can survive and thrive. This principle of non-interference and mutual respect form the essence of true free market capitalism. An excerpt from the masterful essay I, Pencil poetically explains the magic of free markets:

"I, Pencil, am a complex combination of miracles: a tree, zinc, copper, graphite, and so on. But to these miracles that manifest themselves in nature an even-more-extraordinary miracle has been added: the configuration of creative human energies — millions of tiny know-hows configuring naturally and spontaneously in response to human necessity and desire and in the absence of any human masterminding! Since only God can make a tree, I insist that only God could make me. Man can no more direct these millions of know-hows to bring me into being than he can put molecules together to create a tree...The above is what I meant when writing, "If you can become aware of the miraculousness that I symbolize, you can help save the freedom mankind is so unhappily losing." For, if one is aware that these know-hows will naturally, yes, automatically, arrange themselves into creative and productive patterns in response to human necessity and demand — that is, in the absence of governmental or any other coercive masterminding — then one will possess an absolutely essential ingredient for freedom: a faith in free people. Freedom is impossible without this faith...The lesson I have to teach is this: Leave all creative energies uninhibited. Merely organize society to act in harmony with this lesson. Let society's legal apparatus remove all obstacles the best it can. Permit these creative know-hows freely to flow. Have faith that free men and women will respond to the Invisible Hand. This faith will be confirmed. I, Pencil, seemingly simple though I am, offer the miracle of my creation as testimony

that this is a practical faith, as practical as the sun, the rain, a cedar tree, the good earth.”

Standing in stark contrast to the economic system of free market capitalism is central planning (socialism). Central planning, as the name implies, means directing an entire economy in accordance with a single unified plan in a top-down, authoritarian, and unnatural way. In a socialistic economic system, a central entity owns and operates all the productive factors (capital, land, and, ultimately, its people) within a society. As such, this centralized body (usually old, stale, and pale white guys) is arrogantly assumed to possess all the knowledge and feedback loops necessary to form a completely (and continuously) accurate representation of the ever-changing economic realities navigated by its society. Whereas the free market is a form of ideological competition (akin to the idea meritocracy) intended to guide entrepreneurial actions consistent with economic reality, central planning is more akin to the ideological totalitarianism (akin to bureaucratism) associated with a traditional organizational hierarchy, where the merits of ideas are given short shrift and underlings unquestionably carry out the orders of their “superiors”.

Being completely misaligned with reality, socialism failed because it is a poor information system: with all productive factors singularly owned and controlled, the price signals necessary for adapting to changing market realities are inhibited from developing. This inevitably leads to the shortages, mass starvation, and societal disintegration commonly associated with socialism. For an acute visualization of the differences in societal vibrancy between capitalism and socialism, take a look at this shot:



This image of North and South Korea at night vividly illuminates the stark differences between opaque central planning in the north, and vibrant free market capitalism in the south.

If we learned nothing else in the 20th century, it is that free markets are better than centrally planned ones in across almost every conceivable dimension. Left to function freely in their natural state, markets consistently generate innovation that increases productivity, lowers costs, and improves quality of life for everyone in society. Just consider for a moment how much innovations such as the automobile, smart phone, and internet services have increased our personal freedoms and enriched our lives. Now consider how un-innovative and un-adaptive government-run functions like the DMV, Post Office, and central banks are. So the elephant in the room, then, is why, in light of overwhelming evidence favoring a free market economic system, do we still tolerate central planning of the largest market of all – the market for money. Again, money is simply a technology for moving value across spacetime. Although it is an ancient (and somewhat, thanks largely to propagandists, enigmatic) social technology, it is hardly different than any of the other things we produce and distribute via free market mechanisms all over the world today.

Coming back to the congruence between the free market and the idea meritocracy, we arrive at two useful formulas. First, the idea meritocracy is comprised of three key elements: In Ray's words, (p.309):

"Idea Meritocracy = Radical Truth + Radical Transparency + Believability-Weighted Decision Making"

Now, let's translate this equation into its comparable free market format:

Free Markets = Truthful Price Signals + Transparent and Reliable Rule of Law, Private Property Rights, and Hard Money + "Skin in the Game"-Weighted Decision Making

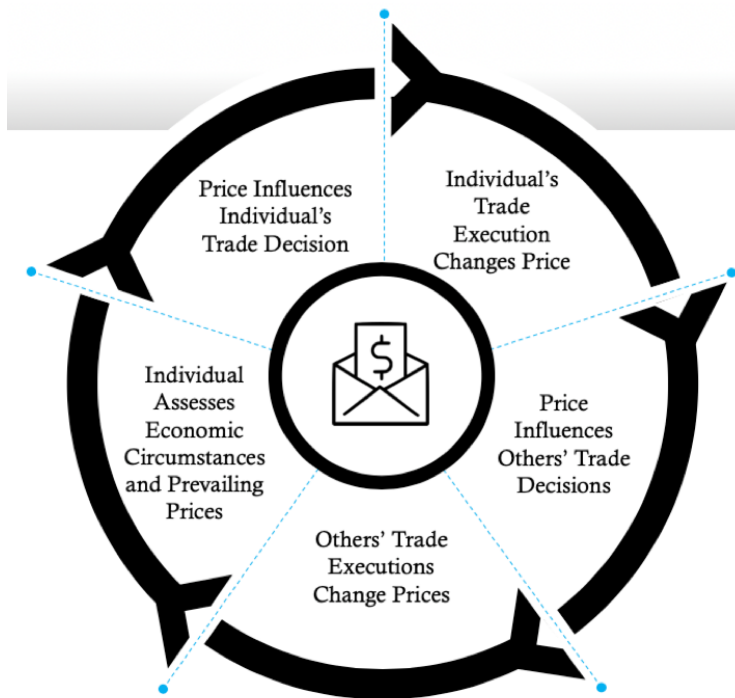
With these equations in mind, let's now dive into each of their elements to gain a clear understanding of Ray's idea meritocracy and its relationship to free markets. Once we fully unpack these concepts, we will go deeper into the other principles underpinning Ray's approach to life and work, using them as filters to more fully observe the potential impact of Bitcoin on all aspects of life.

We begin our journey from the greatest force of freedom in the universe – the truth.

Radical Truth

(p.135) "Truth – or, more precisely, an accurate understanding of reality – is the essential foundation for any good outcome."

The first element of Ray's idea meritocracy is Radical Truth, the idea that gaining a clear perception of reality is paramount to facing it head on and dealing with it. In markets, it's commonly said that "price is truth"; meaning that all known market realities are expressed in, and evaluated by, any particular asset's price at any given moment. You may remember from Economics 101 that the market price is the intersection of supply (an objective quality) and demand (an intersubjective or opinion-based quality). Put another way, prices are data packets that convey information about scarcity (which is objective) and value (which is intersubjective). Each entrepreneur's decision to buy or sell is influenced by prevailing prices and, in turn, communicates back into the market the state of economic conditions relevant to him which, in turn, influences the same decision-making of all other entrepreneurs within his market; this is intersubjective value. These decisions are based on actual availability of time, resources, and know-how; this is objective scarcity. This feedback loop is the means by which free markets dynamically adapt to express prices that accurately portray economic realities:



Price signals are the economic nervous signals of an economy. To remain healthy and honest, they must be expressed in an uncompromisable monetary medium.

Let's return to Larry the lemon farmer: say a storm wipes out a large crop of lemons in California; reduced supply levels of lemons intersecting with an unchanged level of consumer demand necessarily means an increase in lemon prices. Increased prices incentivize lemon growers like Larry to produce more as they now fetch higher prices in the

marketplace. On the other side of the lemon market, higher prices disincentivize consumers from buying as many of the sour yellow citrus fruit. As people respond to these ever-shifting incentives, which are a reflection of the endlessly shifting economic realities of supply and demand, free markets adapt to maximize output and minimize costs. In this way, price signals serve as a dynamic incentive system for equalizing supply and demand discrepancies in free markets. However, to maintain their truthfulness, these price signals must be freely expressed in a money that is undistorted by government interventionism.

A price signal converts countless economic complexities into simplicity; it compresses myriad market realities down into a single, actionable variable – the market price.

Accurate price signals only prevail if the market is freely competitive and not subject to government interventions such as price fixing, trade restriction, or legal monopoly insulation. In true free market capitalism, most markets are relatively unobstructed by such artifices and the price signals are, accordingly, mostly reliable conveyors of truth. Lemon prices, for instance, tend to reflect the actual underlying supply and demand (or scarcity and value) realities at any given point in time. The market for money, however, is quite different in the modern economy, and its differences have cascading effects across all other markets.

Money is economic water; in the same way water intermixes and intersperses organic chemicals throughout the circle of life, money

mediates the interchange of goods, services, and knowledge within markets.

Money, as one half of virtually every economic exchange, is the largest market in the world. This market is monopolized by central banks in every major economy worldwide; meaning that all forms of money competitive to fiat currency are prohibited (see eGold). As Ray aptly points out, (p.533) “Fiefdoms are counterproductive and contrary to the values of an idea meritocracy.” Yet, for some reason, the economic fiefdoms called nation-states, which are antithetical to the free market paradigm (and, therefore, the idea-meritocratic paradigm), are commonplace. Even in the US, where we pride ourselves on being free market capitalists, we maintain this socialistic market structure for money. In this market, the following elements impact price expression of money:

- Supply – the amount of money available to be loaned out (aka loanable funds)
- Demand – the amount of loanable funds desired for borrowing
- Interest Rate – the price paid for funds borrowed

Central banks “manage” the market for money by controlling the supply of loanable funds and setting the interest rate (the price) at which these funds can be lent out. These central bank privileges are preserved by state-enforced monopoly rights, which insulate their mass-produced fiat currencies from competition and eliminate their “skin in the game”. Skin in the game, a crucial Talebian concept, is a property based on symmetry, a balance of incentives and disincentives: in addition to upside exposure, people must also be penalized if something for which they are responsible for goes wrong or hurts others. Skin in the game is a central pillar for properly functioning systems, of both the organic and inorganic variety, 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. Central banks, through various schemes and machinations, eventually coopted the market for gold and developed an economic system that could create money without skin in the game; allowing them to privatize seigniorage profits and socialize any losses they incurred through inflation. Unless consequential decisions are made by people who are exposed to the results of their decisions, the system is vulnerable to total collapse; the frequent faltering of fiat currencies attests to the unfavorable asymmetry of this model for citizens.

Most commonly, as they have a direct financial incentive to do so, and with no downside to consider, central banks increase the supply of loanable funds and decrease the interest rate below its natural levels, thereby inducing an expansion of the money supply. Importantly, money supply expansion does

not create any new wealth, as “printing money” does not infuse an economy with any new productive factors such as tools, factories, equipment, or human time. Instead, expansionary monetary policy only redistributes claims on productive assets from their rightful owners to those who receive the newly printed money first — usually bankers, politicians, and the other politically-favored-few closest to the spigot of liquidity (due to the Cantillon Effect). As Charles Holt Carroll said:

“Inflation is the surest way to fertilize the rich man’s field with the sweat of the poor man’s brow.”

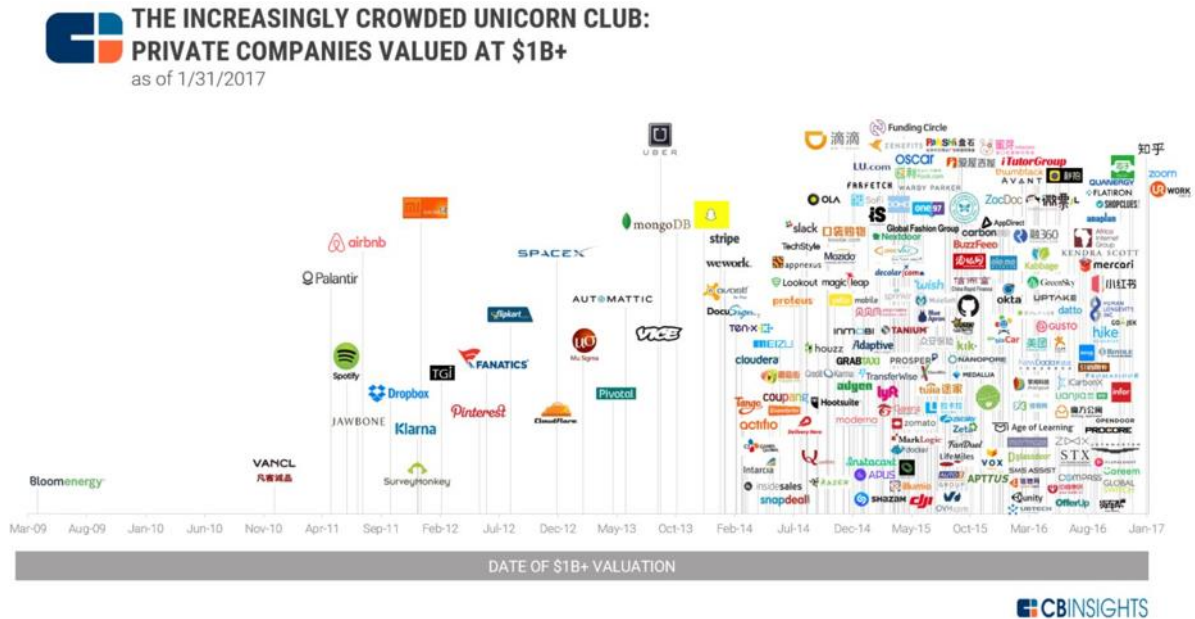
Inflation of the money supply is a violation of private property rights, as it reallocates wealth away from its original owners (the many) into the hands of those closest to the governors of the monetary system (the few). But confiscation of wealth, via the shadow tax of inflation, is not the only collateral damage inflicted by money supply expansion. Entrepreneurs operating in these soft money economies are easily misled by the distorted price signals that centrally planned fiat currency markets inevitably cause.

To understand this, let’s look at the world through the lens of Larry the lemon farmer: emboldened by the “cheap” loans proffered by his local banker, Larry decides to borrow money to expand his lemon farm. He figures that borrowing enough money at 3% will allow him to expand and increase output of his farm by 2.5X, while only increasing his cost structure (including the 3% loan interest payable to his banker each year) by 2.3X. This economy of scale (the positive 0.2X margin between revenue growth of 2.5X and cost increase of 2.3X), Larry calculates, will drop straight to his bottom-line profit. So, Larry visits his local banker to sign the loan documents and sets out to expand his operation. At first, everything seems to be going smoothly as Larry gradually begins buying the additional land, fertilizer, and equipment necessary to grow and sell more lemons. However, things get sideways when other lemon farmers, lured by similar prospects of economic gain, also borrow from their local bank to expand their farms. As more lemon producers borrow and bid for the same lemon-farming assets, inflation sets in and prices begin to rise, thus increasing the cost structure of lemon production. Shortly after investing all his loan capital into his farm expansion, Larry finds that his cost structure has actually increased 2.8X due to more dollars chasing the same amount of productive factors for lemon farming. Gradually, then suddenly, the money Larry borrowed to expand his profit margin begins to work against him, as his increased capacity has eaten up his original profits and is now generating a loss (the negative 0.3X margin between revenue growth of 2.5X and cost increase of 2.8X, net of any prior profit margin). At this point, Larry has no choice except to increase his prices, cut costs, refinance, sell the farm, or declare bankruptcy. Under the same circumstances, other projects in other industries, misled into overborrowing by artificially cheap money, begin suffering losses as well.

An economy-wide simultaneous failure of overleveraged projects like Larry's 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 manipulation in the market for money. It is substantively no different than the shortages that would result if the price of bread was fixed at an artificially low level (which caused the starvation of millions in Soviet Russia). Artificially low interest rates don't provide any benefit to the real economy, rather they simply disseminate distorted price signals that encourage entrepreneurs to embark on projects that cannot be profitably executed due to the (hard to foresee) impact of inflation on their cost structures. As with all well-functioning markets, the price of money must emerge through, and constantly reorient itself against, the natural interactions of supply and demand. Attempts to centrally plan this market only distort truth (price signals) and trigger overborrowing, recessions, and cause (or, at least, exacerbate) the boom-and-bust business cycle.

As money supplies become more opaque, so too do the critical price signals they carry back and forth between the minds of entrepreneurs.

The more opaque the present and future supplies of money, the more entrepreneurs suffer from this myopia, and the more stifled the economization of human action becomes. Price signal distortions like those faced by Larry result entirely from the opacity of central bank "managed" (read: manipulated) money supplies. Central banks are only able to perpetrate this scheme due to the legal monopolies (artificial barriers against free market competition) which shield their inferior monetary technologies (fiat currencies) from facing off with superior technologies (like gold) in the marketplace. Legal monopoly protections inhibit price discovery in the market for money (the natural interest rate). There is also ample evidence that central banks actively suppress the price of gold to preserve fiat currencies (see Gata.org). Further, if monetary technologies were freely selected and priced in the marketplace, as was the case when gold ascended to dominance, then everyone could more reliably use money as a store of value instead of being forced further out along the risk curve into stocks, real estate, and other scarce assets to protect their wealth from the ravages of inflation, which further distorts prices; the increasingly crowded unicorn club reflects just how distorted prices have become:



Money that cannot reliably hold its value across time forces people to make ever-riskier investments.

Simply put, price is truth; distorted money supplies distort the truthfulness of price signals and throw entrepreneurial action into disarray. At the heart of the cyclic booms and busts in the economy, then, is this distortion of the fundamental signaling which, in its current distorted state, misguides entrepreneurial action. Under these conditions of monetary socialism, trying to build a business is like trying to build a house in a jurisdiction that constantly changes the spatial values of its metric system; as Taleb puts it:

According to Wittgenstein's ruler: Unless you have confidence in the ruler's reliability, if you use a ruler to measure a table you may also be using the table to measure the ruler. The less you trust the ruler's reliability, the more information you are getting about the ruler and the less about the table.

With an absolutely fixed supply, Bitcoin will restore the clarity of these economic nerve signals that are so critical to proper capital allocation, risk assessment, and entrepreneurial planning. Universal units of measurement are critical in economics and industry — the seconds, meters, kilograms, and other units of measurement we use throughout the world are all immutable in value. Upon these foundations of standardized measurement, the machinery of global commerce is constructed: builders of skyscrapers, electronics, and myriad other goods rely on the constancy of these measurement units when sourcing components and materials from around the globe. Money, too, is most communicative when its supply is immutable. As a purely objective monetary medium, once it accretes enough value to incentivize its users to spend it, Bitcoin denominated price signals will carry more truth than any other money in history.

Bitcoin is a monetary channel free from the noise of unexpected supply fluctuations, which necessarily means it carries the clearest signals. In this way, Bitcoin is the perfect conveyor of the data packets on value and scarcity known as price signals.

In terms of the idea meritocracy equation, we see that fiat currency is antithetical to radical truth and, its free market corollary, truthful price signals. On the other hand, Bitcoin is the most honest money imaginable, as every component of it, including its money supply, is viewable by everyone. In a world filled with fake news, click bait, and data breaches – Bitcoin is one of the rare instances of honesty in modernity. Central banking is the reverse; it is shrouded in complexities intended to hide its truth. Bitcoin is both radically truthful and transparent.

If money is economic water, then fiat currency is inscrutably murky, and Bitcoin is crystal clear.

Bitcoin's transparency has already shed much light on the umbral industry of central banking and its shadowy tactics by sparking a renewed interest in Austrian economics and making an entire generation ask the question: "What is Money?". We stand to gain even more clarity around Bitcoin's impact on the world by diving into the second element of Ray's idea meritocracy – radical transparency.

Radical Transparency

(p.308) "By radical transparency, I mean giving most everyone the ability to see most everything."

Originally, capitalism was founded on the cornerstones of reliably consistent rule of law, private property rights, and hard money. Respectively, these cornerstones provided people non-violent dispute resolution, confiscation resistant assets, and a sound medium of exchange. With strong and reliable rules, entrepreneurs are then free to "play the game", accumulating capital for themselves and diffusing any innovations gleaned in the process into the whole of society. For entrepreneurs to execute effectively, they must know the rules of the game, and must be able to trust that they are not subject to change. Imagine a poker player sitting at a table where the hand-rankings changed at the whims of the casino every few hands; without sound rules on which build a strategy, no player would remain engaged for long, and would quickly exit the game. Stability in these areas is among the primary reasons why the United States is such an attractive environment for investing; for the most part, its courts function well and contract law is enforced without bias. The exception, of course, is the violation of private property rights which results from centrally manipulated money supplies – in other words, the softness of the US dollar.

According to you Ray, “The most painful lesson that was repeatedly hammered home is that you can never be sure of anything: There are always risks out there that can hurt you badly, even in the seemingly safest bets, so it’s always best to assume you’re missing something”. Considered by many to be among the safest bets in the world today is the US Dollar – it is issued by the largest economy in the world, is “backed” by the world’s most militant taxing authority, and is accepted almost everywhere as a medium of exchange. Further, by unilateral decree (and a veiled threat of force), the US Dollar exclusively denominates the lifeblood commodity of the modern industrial economy, oil. The problem with the perceived safety of the US Dollar is the opacity of the rules which govern its existence: How many are there in existence? How many will be issued in years to come? Who gets to decide? Who stands to profit from its production? Even though the US Dollar today is just an SQL database maintained by The Fed that could choose to open its records to audit, it refuses.

https://twitter.com/_justinmoon_/status/1159598647815917568?s=21

Instead, The Fed sets monetary policy in closed door meetings and (only vaguely) communicates its intentions using ambivalent speech. To counterbalance this opacity, an army of macroeconomists, analyst, and market commentators pour over every detail of the statements issued by central bankers including not only their words, but their tone, delivery, and even wardrobes.

Imagine a semi-governmental agency being put in charge of setting the price of, say, automobiles based on undisclosed criteria and decided in closed-door meetings. Ask any “free market capitalist” if this seems like a good idea and he will spew vitriol at you for even suggesting such a socialistic method of managing the production of automobiles. Then ask him whether it’s a good idea for this same agency to control the price of communications technologies like laptops and smart phones. You’ll be met with the same answer and (perhaps) a loud American battle cry in support of free market capitalism. Finally, very smoothly point out to him that The Fed sets the pricing of the US Dollar (the interest rate), which is the United States’ most valuable export market, and does so based on undisclosed criteria and closed-door discussions. Although Keynesians have done a great job convincing many of the enigmatic nature of money, it is quite simply just a tool for moving value across spacetime, and as such should be priced and technologically selected on the free market (just like everything else in a truly capitalist society).

Sunlight is the best disinfectant; when everyone can see the criteria and process behind a decision they are more likely to deem it trustworthy. With Bitcoin, the algorithm which sets its monetary policy is totally transparent, meaning people can universally agree that the system is fair and unbiased. As an open-source monetary protocol, Bitcoin is essentially the principle of radical

transparency in perpetual action. Similar to some of the management tools you've created Ray – such as the baseball cards, Dot Collector, Pain Button, etc. – Bitcoin can be thought of as a global monetary policy management tool. As a machine componentized by open-source software and entrepreneurial self-interest, it does the work facilitated by central banks today – maintaining monetary policy, reaching consensus as to account balances, and facilitating international value flows – without relying on the whims of bureaucrats who control state-backed monopolies on money. Bitcoin is the purely transparent alternative to the opacity of central banking; it is a beacon of light outcompeting an industry purposefully shrouded in darkness. Once properly understood, Bitcoin's superior visibility inescapably enhances its believability. And once you see it, it cannot be unseen.

Bitcoin's monetary policy (its new supply flow schedule) is becoming the most trusted in the world as it is fully transparent and unchangeable. Bitcoin runs countervailing to government monetary policy which is uncertain, opaque, and subject to change based on bureaucratic whim.

In terms of the idea meritocracy equation, Bitcoin restores the confiscation-resistance of money, which provides its users stronger property rights when compared to fiat currency. Importantly, Bitcoin also reestablishes the sorely lacking 3rd cornerstone of capitalism in an otherwise free world – hard money. As an economic good undergoing monetization on the free market, with a supply inelasticity destined to surpass that of gold, Bitcoin is resurrecting the free market capitalist triad. As it bears repeating: Bitcoin is both radically truthful and transparent.

As you've said Ray: (p.327) "Having nothing to hide relieves stress and builds trust." Transparency and reliability is the essence of Bitcoin's monetary policy. It is truly unique in that its supply is absolutely predictable and absolutely scarce. Bitcoin is the most credible monetary policy in history outcompeting the least trustworthy monetary policies in history; it is rapidly gaining a track-record superior to central banks across all dimensions – reliability, predictability, auditability, cost-effectiveness, and resistance to censorship or manipulation – thereby further eroding the believability of central bankers, which is in shorter supply with every dollar printed.

Believability-Weighted Decision Making

(p.284) "When you're responsible for a decision, compare the believability-weighted decision making of the crowd to what you believe."

When it comes to money, track records matter. People's trust tends to coalesce slowly around the most stable from an exchange ratio perspective – in other words, what best maintains or gains purchasing power across time. In this respect, gold is undoubtedly the king, as it sports a more than 5,000 year

history of remaining reliably scarce and, therefore, valuable. An ounce of gold has roughly equaled the price of a fine man's suit for the past century, whereas the same suit's price in dollars has skyrocketed. The best performing central bank fiat currency in history in the British pound, which has only lost 99.5% of its value in its 317 year existence. When it comes to value storage, gold has a believable track record, whereas fiat currencies could only barely be less believable. The hardness or soundness of money, as one of the three cornerstones of free market capitalism, has been almost completely compromised as a result of state-enforced monopolization.

For free markets to function optimally, its three cornerstones — rule of law, private property rights, and hard money — must be consistently applied across all market participants. While the rule of law and property rights are (mostly) sound in western society, centrally planned money supplies are quite the opposite. Without any reliable insight into the primary governance aspects of money (see Radical Transparency above), entrepreneurs are forced to rely on other means of protecting their wealth from theft or debasement. Simply, the implementation of fiat currency offers limited to no assurances to its users that their wealth will be protected from confiscation, censorship, inflation, or counterfeit.

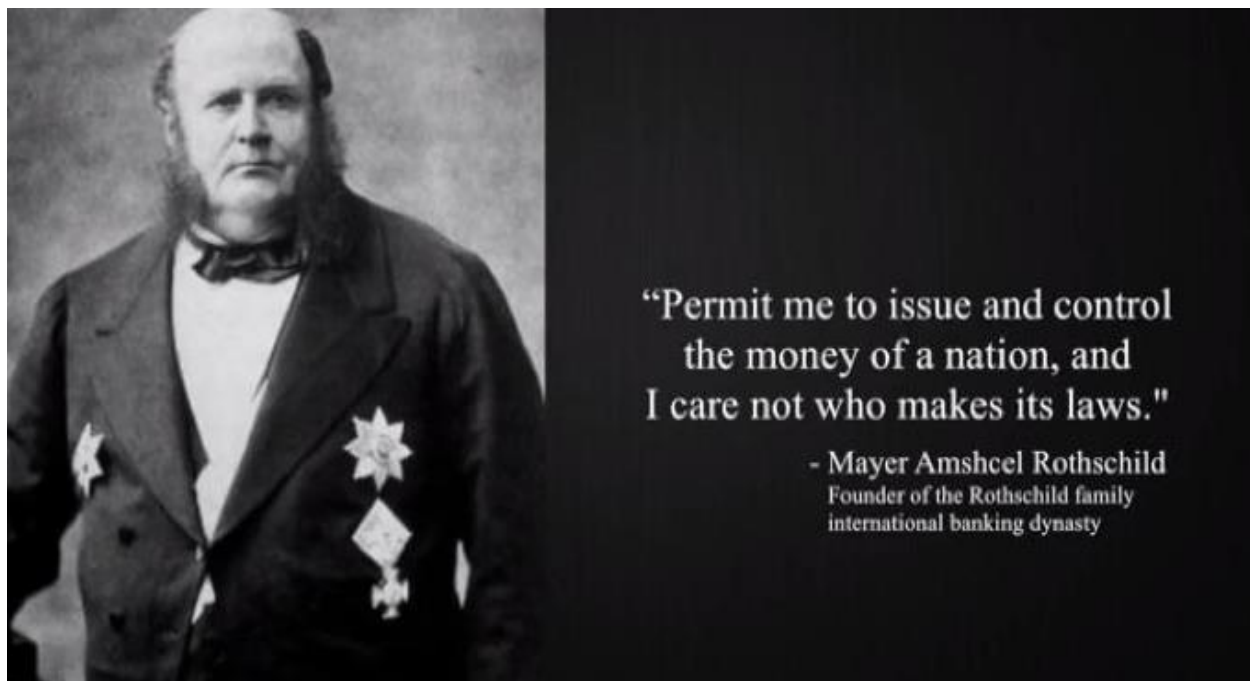
Fiat currencies, when stored in banks, are subject to confiscation or payment censorship by authorities. When stored physically (say, under your mattress), fiat currencies are still subject to value dilution via inflation (the legalized version of counterfeiting). Although fiat currencies offer some physical security measures against counterfeiting (the criminalized version of inflation), this has proven to be a cat and mouse game in which counterfeiters and authorities are constantly trying to outsmart one another in the domain of currency verification technologies.

Bitcoin, on the other hand, is a purely sound money and offers robust assurances to its users. It is resistant to confiscation, as only the possessor of a private key (an alphanumeric string of data) can produce the digital signature necessary to spend it. Bitcoin transactions cannot be censored due to the peer-to-peer and open-source nature of its software architecture. Complete immunity to unforeseen changes in its money supply is guaranteed by unbreakable cryptography and the economic self-interest of miners which secure its network. Finally, since the rules which govern Bitcoin can be verified by anyone, anywhere, and at any time — it is completely counterfeit resistant. Indeed, it is its radically transparent nature that makes Bitcoin the most believable monetary technology in history. Monetary opacity always leads to moral hazard on the part of policymakers.

With decades of experience seeing these hazards explode up close, Ray has said, (p.107) "The job of a policymaker is challenging under the best of circumstances, and it's almost impossible during a crisis. The politics are

horrendous and distortions and outright misinformation from the media make things worse.” So this begs the question: why should we permit policymakers to dictate monetary policy? As “free market capitalists”, we make no such concessions in any other market in the world. We don’t trust a board of governors to tell us how many automobiles to manufacture or at what price to sell laptops each year, so why should we trust central banks to set price and production targets the largest market in the world? As with all production decisions, the free market – representing the collective interests, intelligence, and wisdom of all economic actors – is always the best generator of (low) believable prices, new innovations, and consumer satisfaction.

Controlling monetary policy is like being crowned king of the world. As a fat-cat banker once said:



Money is an instrument of freedom; controlling its supply grants control over its users.

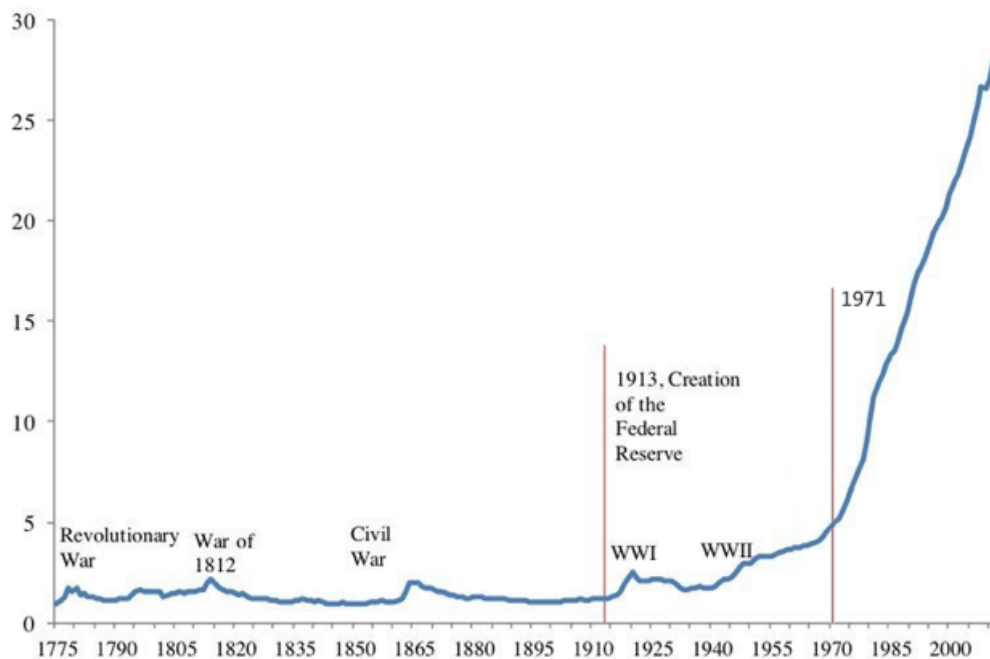
For this reason, most of the world’s wars have been waged in an attempt gain control over this contentious crown. And to control monetary policy, it is necessary to dominate the original monetary sovereignty layer of planet Earth – gold. For instance, during World War II, North America became a geographically-strategic safe haven for European gold hoards to protect them from Nazi plundering. At the conclusion of World War II, into which the United States ultimately intervened to destroy its war-wearied opponents and declare itself victorious, the Brettonwoods Conference was convened in which the rules of the global economic were rewritten by the newly self-proclaimed king – the United States. This conference cemented The Fed as the effective central bank of the world and the US dollar as the world reserve currency.

Even if you are a believer in monetary socialism, you would be hard pressed to defend the believability of central bankers. As you said Ray, “Think about people’s believability, which is a function of their capabilities and their willingness to say what they think. Keep their track records in mind.” In terms of capabilities, central banks have arrogated themselves virtually unlimited latitude to manipulate the supply and price of fiat currency. However, they have exercised these privileges based on (largely) undisclosed criteria and are notorious for their veiled communication styles. In other words, central bankers seem quite unwilling to say what they think (which violates the first thing necessary for an idea meritocracy) and their decision-making criteria is shrouded in falsehood. As Michel de Montaigne once wrote:

“If falsehood had, like truth, but one face only, we should be upon better terms; for we should then take for certain the contrary to what the liar says: but the reverse of truth has a hundred thousand forms, and a field indefinite, without bound or limit.”

In regards to track records, central bankers likely hold the world record for the most abysmal performance history. Since reputation cannot be printed, and must be earned through a lifetime of honesty, it is unsurprising that central banks have struggled in this respect. Historically, every fiat currency has trended towards worthlessness, which has only dragged the believability of this monetary model ever-downward. Mandated with price stabilization and employment maximization, The Fed has failed miserably at both, especially since severing the peg to gold in 1971; here, we show the US dollar’s loss of purchasing power since 1775:

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



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

The softer money becomes, the more it trends towards absolute worthlessness.

Central banker opinion-driven money supplies are proportionately reliable to the value storage functionalities of the ever-softening fiat currencies they mass produce. Bitcoin's fact-driven money supply is as reliable as the mathematics and thermodynamics which sanctify its inviolable ledger. Opinions are like soft money, in that they can easily be diluted and distorted. Facts are like hard money, in that they are rooted in scientific realities. Said simply: do we believe the largest market in the world is best governed by opinion or fact? Buying Bitcoin is buying a put option on central banker malfeasance. As Travis Kling says:

https://twitter.com/Travis_Kling/status/1181647574861832193

More fundamentally: how can we possibly believe that central bankers will perform well when they completely lack skin in the game? As Taleb puts it:

"Systems don't learn because people learn individually -that's the myth of modernity. Systems learn at the collective level by the mechanism of selection: by eliminating those elements that reduce the fitness of the whole, provided these have skin in the game. Food in New York improves from bankruptcy to bankruptcy, rather than the chefs individual learning curves -compare the food

quality in mortal restaurants to that in an immortal governmental cafeteria. And in the absence of the filtering of skin in the game, the mechanisms of evolution fail: if someone else dies in your stead, the build up of asymmetric risks and misfitness will cause the system to eventually blow-up.”

Totally disconnected from the consequences of their policy actions, which are instead born by citizens, central bankers are incentivized to maintain the status quo to preserve their jobs and “prestige”. Money, the largest and most critical market in the world, simply cannot evolve without practitioners who are subjected to real world consequences and tradeoffs, in real time. Simply, if you lack skin in the game then you lack believability. This explains why ancient Roman architects were required by law to stand beneath their monolithic arches when the scaffolding was removed. This (deadly) disincentive to malperformance worked wonders, as some of the oldest arches constructed in this way are still standing at over 2,000 years of age. If only central bankers were subjected to the devastation they inflict on centrally planned economies should their decision-making not work out, then perhaps the world would still be on a gold standard and the dire need for Bitcoin would be lessened.

Parading themselves as the healers of economic crises, central bankers are actually the creators of these calamities. QE, TARP, NIRP, and other interventions inflict a heavy iatrogenic cost on society; and the harm done is further compounded by the agency problem (central bankers have no skin in the game, and therefore have conflicted interests when it comes to managing money supplies).

So, in terms of the idea meritocracy formula, it is clear that central banking fails to satisfy its third element of Believability-Weighted Decision Making, instead, the prevailing economic order seems to promote the least believable people into the driver’s seat of the world economy. Translated into the free market formula terms, this is an expectant result as these policymakers suffer from the agency problem and are rendered impotent without “Skin in the Game”-Weighted Decision Making. In this sense, Bitcoin is the reverse; its node operators and miners govern the system, all of whom have skin in the game and, therefore, possess more believable decision-making capabilities – just like the ancient architects who stood beneath their newly un-scaffolded arches.

To put it all together in terms of our original equations; we began with:

“Idea Meritocracy = Radical Truth + Radical Transparency + Believability-Weighted Decision Making”

Which translates to this free market format:

Free Markets = Truthful Price Signals + Transparent and Reliable Rule of Law, Private Property Rights, and Hard Money + ‘Skin in the Game’-Weighted Decision Making

Based on what we've learned so far, we can translate these equations once again into central banking and Bitcoin versions:

Central Banking = Untruthful Price Signals + Transparent and Reliable Rule of Law, Marginalized Private Property Rights (due to violations via inflation), and Soft Money + "Agency Problem"-Weighted Decision Making

Bitcoin = (Absolutely) Truthful Price Signals + Transparent and Reliable Rule of Law, Private Property Rights, and (Absolutely) Hard Money + "Skin in the Game"-Weighted Decision Making

Clearly, only Bitcoin is 100% consistent with the equation for free markets; whereas fiat currency is almost entirely inconsistent. Since this free market equation is equivalent to the idea-meritocratic equation, we may deduce: Bitcoin is completely consistent with Ray's formulation of the idea meritocracy, and fiat currency is not.

Therefore, because math, Bitcoin is both a free market and an idea meritocracy.

So, Ray, assuming your Principles are stated forthrightly, how can you possibly be a non-believer in Bitcoin? As you said Ray, (p.379) "When someone says 'I believe X,' ask them: What data are you looking at? What reasoning are you using to draw your conclusion?" So let me ask you Ray: after Bitcoin's impeccable performance for over a decade (over 99.98% uptime, never been hacked, evolution into the most secure computing network in the world, roughly \$200B in market capitalization, and over \$1T of transactions cleared in total), what data and reasoning are you using to draw your conclusion about Bitcoin?

My guess is that like many smart people, you may have disregarded Bitcoin at the outset. In accordance with one of your favorite principles, I implore you to keep an open mind about Bitcoin and, perhaps, you will come to see it as an embodiment of open-mindedness itself. In that spirit, let's dive deeper.

Open-Mindedness

(p. 187) "If you can recognize that you have blind spots and open-mindedly consider the possibility that others might see something better than you – and that the threats and opportunities they are trying to point out really exist – you are more likely to make good decisions."

Open-mindedness is a key aspect of both an idea meritocracy and evolution. It is a concept closely related with filtering and optionality: a form of non-cognitive intelligence intrinsic to natural systems in which exposure to multiple potentialities is employed, allowing the system to "learn" by adopting what works and discarding what doesn't. An interesting paradox is discovered

in that this openness is the source of Mother Nature's opaque logic — as Taleb puts it:

“Evolution proceeds by undirected, convex bricolage or tinkering, inherently robust, i.e., with the achievement of potential stochastic gains thanks to continuous, repetitive, small, localized mistakes. What men have done with top-down, command-and-control science has been exactly the reverse: interventions with negative convexity effects, i.e., the achievement of small certain gains through exposure to massive potential mistakes...Simply, humans should not be given explosive toys (like atomic bombs, financial derivatives, or tools to create life)”

Close-mindedness, on the other hand, represents a rigid fixity on an existing knowledge framework that excludes the possibility of learning, innovation, and evolution. Without a culture of open-mindedness, organizations fail to learn and adapt well, and begin to suffer losses at the hands of more fit competitors. Sheltered from market discipline by their legally fortified monopoly positions, central bankers become feeble minded while, at the same time, their monetary technologies become brittle and maladapted to shifts in user demand.

Open-mindedness is an ever-present state of mind, a keen awareness of optionality and the freedom to filter; to change one's mental or organizational model, to reform one's prior assessment of conditions based on new information or a new vantage on old information (Bayesian inference).

Here, we see another perspective on the ineffectiveness of central planning — by moving in accordance with a single, rigid plan of action, the economy gets locked into a non-opportunistic course of action; it becomes blind to optionality and, thus, close-minded. For institutions, innovations, and individuals, close-mindedness is fatal. As legendary physicist Richard Feynman said, “we can never be sure we're right, we can only be sure we're wrong” — this is why open-mindedness matters across all spheres of human action.

Open-mindedness in the technological realm is manifests in the form of open-source technologies; tools sporting schematics that anyone can inspect, modify, or enhance. Ray incorporates this principle into his culture at Bridgewater and in the “management tools” his team uses to make organizational and investment decisions. Bridgewater's management tools are open-source by design so that they can consistently adapt to offer the highest utility to its workforce. As Ray says, (p.527) “Because the thinking behind the algorithms is available to everyone, anyone can assess the quality of the logic and its fairness, and have a hand in shaping it.” By applying the principle of radical transparency to his management toolset, Ray encourages a culture of open-mindedness by making their tools open to critique and change, in the

same way ideas are assessed openly based on their merits alone within his cultural paradigm. This approach ensures that everyone maintains a perspective of “why are we doing it this way” and “is the tool helping us achieve our objectives as an organization”.

Essentially, by practicing open-mindedness, the team at Bridgewater supports their effort to operate as an idea meritocracy. In effect, Bridgewater has structured itself as an open-source organization in which its team learns and grows by, (p. 67) “Wrestling with the markets, thinking independently and creatively about how to make our bets, making mistakes, bringing those mistakes to the surface, diagnosing them to get at their root causes, designing new and better ways of doing things, systematically implementing the changes, making new mistakes, and so on.” Whether you realize it or not Ray, you have been cultivating a culture based on the ethos of open-source technology.

Open-source technology is readily inspectable and, therefore, trust-minimized. Openness lets it absorb feedback from many sources to adapt in response changing market conditions and user demand. These technologies are absolutely transparent and auditable, which minimizes the need to trust other people when using these tools to interact. Trust-minimization is one of the primary benefits of that ancient open-source monetary technology – gold. Since trading partners couldn’t necessarily trust each other, they could instead rely on the natural laws restricting the supply of gold and use time-honored techniques for assaying its authenticity (until coinage fulfilled, then repeatedly violated, this trust function), thus minimizing the need to trust counterparties to a transaction.

Closed-source technology is the reverse and thus requires users to trust in its purveyor; it is unauditable and, therefore, maladapted to market conditions and user demand. In the case of fiat currency, this purveyor is a monopolist and, as many of us learned in Economics 101, profit maximization for a monopolist comes at great expense to everyone else. Fiat currency is closed-source technology that is legally protected from audits and competing monetary technologies. Such opacity and market insulation not only slows the rate of monetary technology innovation, it also erodes the trustworthiness of fiat currency, and fattens its monopolists:



Agustin Carstens, head of the Bank of International Settlements, the central bank of central banks. Just a soft guy, slinging soft money.

As you've said, "Adaptation through rapid trial and error is invaluable" — this is the ethos of open-source. Bitcoin, being open-source, is like a language, as 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). Further, 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 improved functionality and network growth. The work of these open-source programmers closely mirrors Ray's approach to organization building, in which he creates systems that encourage others to (p.64) "Put honest thoughts on the table, have thoughtful disagreements in which people are willing to shift their opinions as they learn, and have agreed-upon ways of deciding if disagreements remains so that we can move beyond them without resentments". Again Ray, your approach to culture and management style mirrors the philosophy of open-source technology.

Ray, is there any reason you believe Bridgewater should benefit from open-source tools while society should suffer under closed-source fiat currency? Shouldn't citizens everywhere have access to the most open and highest

quality feature-set for the most important technology in their lives – money?

Bitcoin's openness is key to its competitive superiority as money. Over the past decade, its global army of volunteer programmers has greatly enhanced the utility of the Bitcoin network. However, and this is critical, these programmers are unable to change the rules of Bitcoin due to its ingenious social contract implementation. Further, since everyone (every node) is "in charge" of the Bitcoin network, it adheres well to Ray's advice to, "Make sure that those in charge are open-minded about the questions and comments of others." This constant scrutiny and feedback from users, each of whom has skin in the game and is "in charge", ensures that Bitcoin is always functioning at or near its optimum. Contrarily, fiat currency has undergone essentially no innovation since its inception.

Due to its open-source nature, Bitcoin is sometimes referred to as "the internet of value". In the same way the internet is a set of open-source protocols for exchanging data (called the internet protocol suite), Bitcoin is an open-source protocol for exchanging value. Such openness ensures that Bitcoin's code cannot be manipulated to benefit anyone at the expense of anyone else. Fiat currency is the opposite; its central planners are, at their own discretion and at near-zero cost, able to siphon value from its monetary network by inflating its supply (such "technology backdoors" are only possible with fiat currency). In regards to how to kill Bitcoin, the "internet of value" analogy also gives us the useful comparative question: How would one turn off the entire internet worldwide, permanently? Governments have proven adept at eliminating centralized entities, however the decentralized nature of the internet and Bitcoin in many ways transcend the coercive and compulsory powers of governments (which is why America can't regulate Bitcoin).

The openness of Bitcoin also makes it antifragile, meaning it becomes hardened by hostility. As you've said, "The key to success lies in knowing how to both strive for a lot and fail well." Open-source, decentralized, digital tools like Bitcoin are uniquely capable of organizing human efforts without a central coordinator at unprecedented scales (strive for a lot) and also become enhanced in the face of technical failings (fail well). Stressors to Bitcoin may come in the form of an external attack on its network or an attempt to fork its blockchain. After 11 years of nearly flawless operation within a relentlessly adversarial environment, Bitcoin has earned its fair share of battle scars (Bitcoin cash, Segwit, etc). Each time Bitcoin withstands an attack, its reputation for network security, reliability, and immutability is strengthened.

Bitcoin is a technology that has accrued value on the free market based on its credibility as money. Unlike fiat currency which persists only because of a government-enforced refugium from competing technologies, Bitcoin persists based on its own merits. Indeed, Bitcoin is a free market for converting

electricity into digital gold – it is outcompeting (literal) monopoly monies worldwide and, by doing so, making the market for money free once again (as we saw in the Gilded Age). Similar to the internet outcompeting intranets, Bitcoin is outcompeting fiat currencies because of its superior openness and monetary traits:

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.

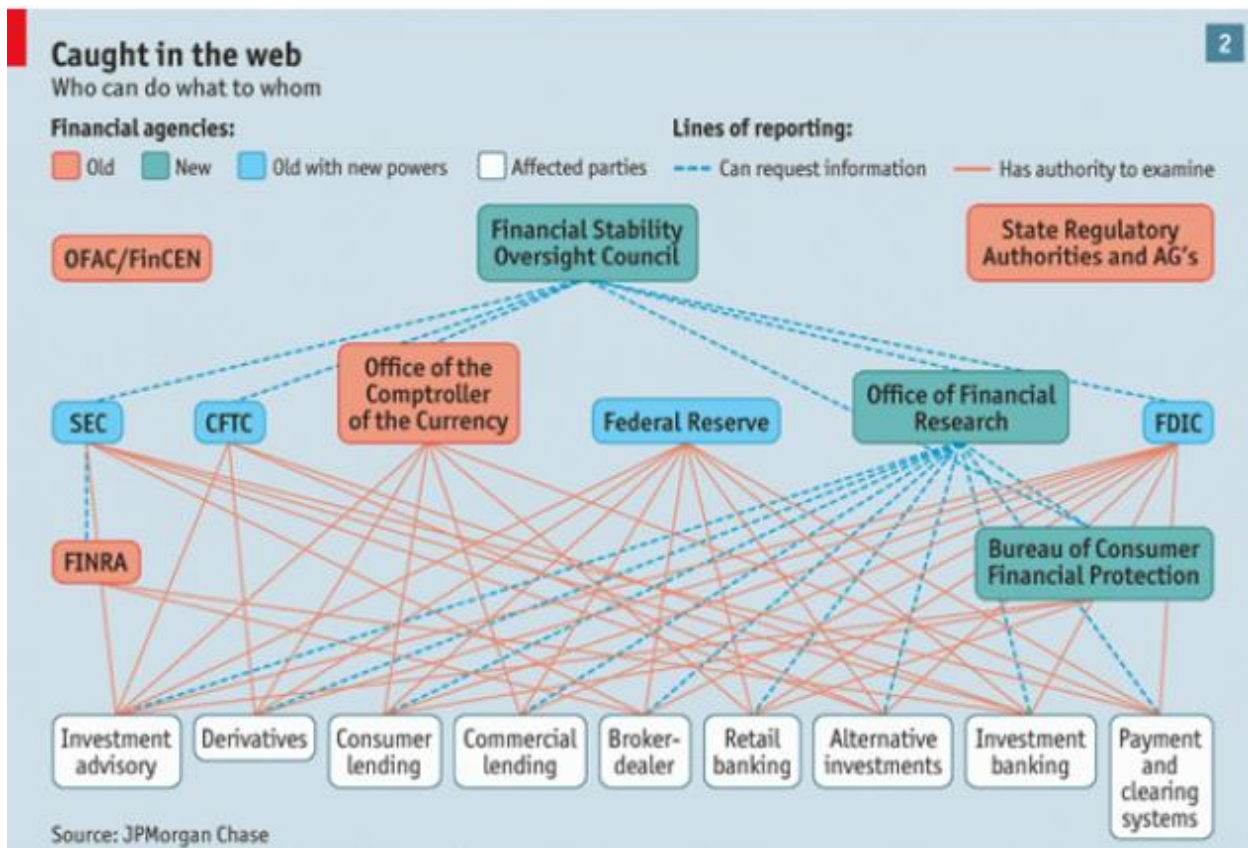
Traits of Money	Gold	Government Money	Bitcoin
Fungibility (interchangeable units)	High	Medium	High
Hardness (stock-to-flow ratio)	Medium	Low	High
Portability	Medium	High	High
Durability	High	Medium	High
Divisibility	Low	Medium	High
Security (cannot be counterfeited)	Medium	Medium	High
Easily Transactable	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

In the monetary ocean, Bitcoin is a blue whale feasting on large swarms of soft money plankton.

As you've said Ray, (p.189) "To be radically open-minded, you need to be so open to the possibility that you could be wrong that you encourage others to tell you so." Unhampered competition incentivizes others to prove you wrong in the marketplace by discovering better or cheaper ways of producing or doing things – this is the very essence of free market capitalism. In truly free markets individuals are maximally sovereign and ruthlessly pursue satisfaction of their wants, which keeps entrepreneurs ever-vigilant in their quest to deliver high quality at a fair price. This unabated pursuit makes free markets generators of quality, innovation, and cost-effectiveness. The reverse is true in monopolized markets – which maximize profits for monopolists at the expense of customers in the form of lower quality (low innovation) and higher prices (market distortions, egregious fees, and value confiscation via inflation).

As you've said in regard to open-source technology Ray, (p.528) "Though the system won't be perfect, it is much less arbitrary – and can much more easily

be examined for bias – than the much less specified and much less open decision making of individuals with authority.” Here you are describing the value of Bitcoin’s immutable monetary policy, which is totally free of arbitrariness, and its incentive-oriented design (people are incentivized to use Bitcoin, see feedback loop in Primer on Bitcoin) over central bank’s arbitrary monetary policy and disincentive-oriented design (people who attempt to compete with or refuse to use fiat currencies are punished). Further, the institutional web surrounding central bank interests is so complicated and holistically unfathomable, it is more prone to arbitrages by insiders, accumulation of systemic risks, and blow ups:



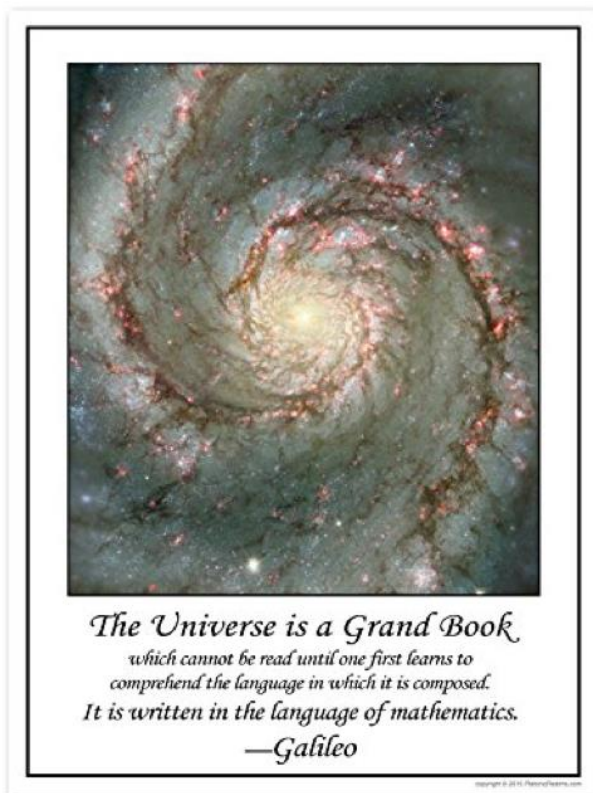
Clear as mud, and twice as dirty.

This messy, closed-source system is bureaucratic, inefficient, and fragile. The main point: open-mindedness is the key to the adaptivity and, thus, the longevity of natural systems. As open-source money, Bitcoin excels in this respect. And money, a long time before government, arose as a natural market phenomenon.

Faith in Nature

(p.140): “Whenever I observe something in nature that I (or mankind) think is wrong, I assume that I’m wrong and try to figure out why what nature is doing makes sense.”

Ray's introductory observation here is consistent with the wisdom of Taleb, who said, "what Mother Nature does is rigorous until proven otherwise; what human and science do is flawed until proven otherwise." Clearly, this is a damning indictment of fiat currencies, which are unnatural monies born of unnatural laws. Gold and silver, on the other hand, rose to become natural monies precisely because of natural laws, which are beyond the reach of mankind's prying hands, and which bestowed them with the traits of good money. Similar to the (mostly) uncompromising rules governing gold, the rules governing Bitcoin are founded in the (absolutely) uncompromising laws of mathematics – nature's fundamental language:



*Bitcoin is the fusion of
two universal languages:
money and
mathematics.*

As you've said Ray, (p.141)
"nature optimizes for the
whole, not for the
individual, but most
people judge good and
bad based only on how it
affects them." This is
what's wrong with
putting individuals in
charge of money supplies
— they are directly
incentivized to produce
ever-more money and use
it to acquire hard assets
(like land, gold, and
businesses) and pass on
the costs of production

(monetary value dilution via supply inflation) to all other market participants, who are legally coerced into using increasingly value-compromised fiat currencies.

As a social technology so fundamental to human cooperation, like spoken language itself, money, to offer the highest utility to the most people, must be governed by rules that cannot be manipulated to benefit one person over another. Somewhat counterintuitively, for money to benefit the most people, governance over its supply must be beyond the reach of everyone. This is why gold ascended to become money on the free market and why it remains the sole instrument for final settlement among central banks today. As the hardest natural money in the world, gold remains the prime monetary sovereignty

layer on Earth. From an accounting perspective, where $\text{Assets} = \text{Equity} + \text{Liabilities}$, gold is purely equity-based, as physically possessing a gold asset is 100% equity and 0% liability; whereas fiat currency is debt-based, as it requires trust in the issuer, its taxing authority, and any payment intermediary associated with its use at any given time.

Simply, gold is the king of natural money; it arose to the role of money as a result of free market processes which, themselves, are operations of nature. Fiat currencies, on the other hand, are artificial; they can only exist in economies where people are coerced into using them via artifices like legal tender laws, capital controls, confiscatory actions, and other anticompetitive restrictions on the market for money. The impetus for fiat currencies existence arises from egoic desires of man like greed, control, and protectionism.

Whereas central banking converts human greed into a race to debase fiat currencies, which inevitably destabilizes economies over time, Bitcoin converts greed into network resiliency and reliability. Bitcoin ingeniously combines the self-interestedness inherent to human nature with electricity and converts them into indisputable records and expansion of its monetary network. The Bitcoin network is itself an embodiment of a free market, where any entrepreneur with access to sufficiently cheap electricity and the necessary hardware can freely enter the market as a miner, that is disrupting the monopolization over the market for money worldwide.

In this sense, Bitcoin is a fractalized free market; its network of miners compete freely to forge an absolutely scarce money that exists outside the scope of monopoly-preserving artifice, thus impressing its free market characteristics onto the world market for money and giving people an alternative to monetary socialism.

Free markets represent a natural organizing principle for humanity that converts the pursuit of individual self-interests into improvement of its collective interests (in Talebian lingo: anti-iatrogenics). This spontaneous order generated by free markets has persisted, to a greater or lesser extent, ever since mankind started trading. Free markets, as an organizing principle, are among the most important in the world as they transmute greed into higher productivity, lower prices, and a stream of new, innovative ideas. What excuse is there, then, to tolerate an unfree market for money? As you've said Ray, (p.281) "Remember that most people will pretend to operate in your interest while operating in their own." This is exactly what the private owners of central banks have been doing for over a century — operating in their own self-interest, under the aegis of government-enforced monopolies, at the expense of everyone else. In this sense, central banking could be the most successful con artistry at scale ever perpetrated.

In nature, energy expenditure is required prior to eating. Plants harvest sunlight into sugar, herbivores spend much of their lives standing and eating plants, and carnivores push themselves to full exertion episodically to hunt. As the 1st Law of Thermodynamics teaches, there is no free lunch in this universe. If there appears to be, you can be sure that hidden risks are accumulating as nature inevitably optimizes for the whole and will eventually restore balance — suddenly and violently if a state of sufficient disequilibrium is reached. Central banks, via the printing press, have spent over a century enjoying a perpetual “free lunch” where control over assets is continuously reallocated from the many to the few; Bitcoin is a (relatively) sudden monetary phenomenon and an economically violent force against banking cartels that is restoring equilibrium to the global economic order.

Bitcoin mining, although often demonized for being tremendously wasteful, may actually have a profoundly positive impact on the world environment. Although this has not been conclusively proven yet, there is research which supports this claim and deductive reasoning suggests it to be true. Consider the following excerpts from a report on this matter:

“Because bitcoin mining is highly mobile compared to overall power demand, it might actually be a boon for global stranded renewables...Whereas traditional industrial and residential power demand is largely geographically captive — be it by proximity to cities, resources, transport links or whatever other factors determine the location of such entities — bitcoin mining can be undertaken pretty much anywhere...This means that some of our most promising sources of renewable energy remain untapped due to their remote locations...Bitcoin mining is a relentless race to the lowest electricity costs and therefore — as explored by Dan Held and Nic Carter — acts as an electricity buyer of last resort...In this manner, bitcoin mining — which offers the possibility of immediate electricity monetization independent of grid connection — can play a vital part in the renewables development cycle.”

What is an energy buyer of last resort? Nic Carter gives us a useful visualization:

“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.”

Nic Carter is really smart.

In this sense, Bitcoin mining is as natural as the free market processes of which it is composed. Instead of boiling the oceans, Bitcoin mining may actually help us to clean them up. Ray, as a thalassophile, I am sure this prospect must excite you, maybe you just haven't looked deeply enough at the nature of this new money to understand its potential environmental impact yet? After all, Bitcoin mining is among the most efficient uses of energy in the world, and increasing mankind's collective energy efficiency (aka productivity) is the entire purpose of the world economy in the first place:

	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

Life is all about energy efficiency; it's why we tinker, trade, and enjoy laying down.

In a profound sense, as Friar Hass says, Bitcoin is nature; a new form of life — a digital organism. 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.

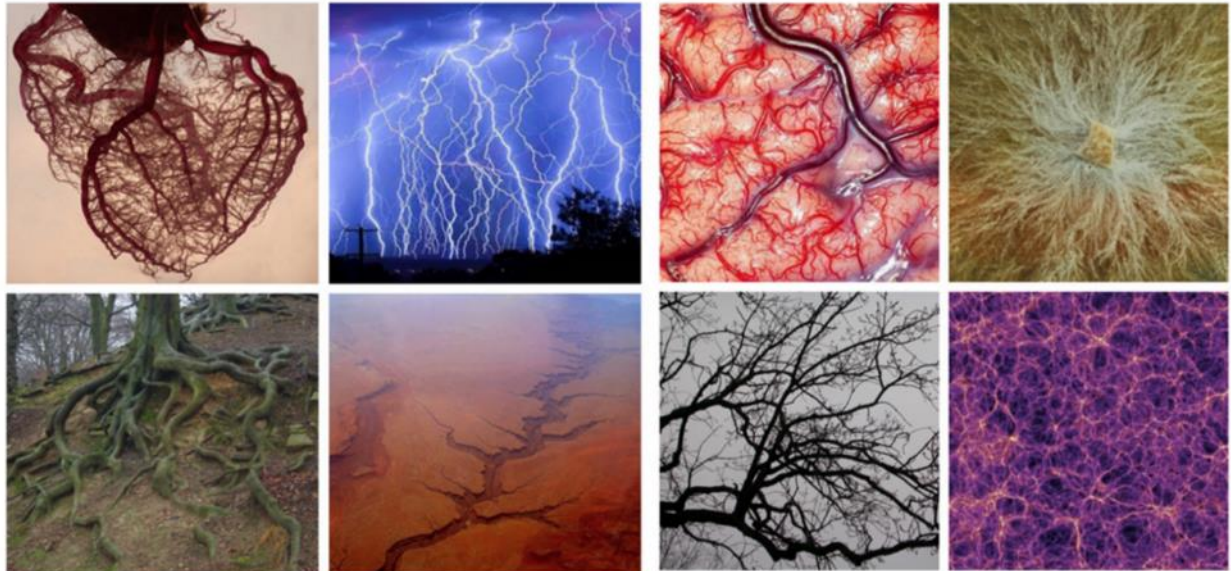
If nuclear war destroyed half of our planet, it would continue to live, uncorrupted. It would continue to offer its services. It would continue to pay people to keep it alive.

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:



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 (the largest observable structure known at over 1 billion lightyears across).

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.

Although fiat currency is commonly held as the “natural order of things” in modernity (a fallacious form of monetary uniformitarianism), it is precisely the opposite. As you’ve said Ray, (p.280) “to be great, one can’t compromise the uncompromisable.” What excuse was there to compromise the redeemability of dollars for natural money or to so heavily dilute the value of fiat currencies over time? These machinations were solely designed to enhance the expropriative abilities of bankers, bureaucrats, and politicians throughout history; letting them effectively default on their debts and pass on the real costs to citizenries. Far from being a natural form of money, fiat currency

became dominant in the world at the end of a long chain of causality — a chain rooted in a flawed system that incentivizes people to operate with smaller time horizons and a zero-sum mentality.

Chains of Cause and Effect

(p.127) "I believe that everything that happens comes about because of cause-effect relationships that repeat and evolve over time."

Different institutional structures and incentive systems produce different human behaviors. Fiat currency is the most recent, and most extreme, act of money supply manipulation — a practice engaged in by all those who gained the ability to do so throughout history. Interestingly, it was a drawback of monetary metals, the difficulty of assaying their value and authenticity, which gave rise to coinage. The "public stamp" emblazoned on the face of coins (usually with a smug emperor's face) served as the veracity that entrepreneurs of old relied upon, thus converting the need to verify (or assay) money used in each transaction into the need to trust a state-stamped corroboration of monetary value. Almost every time coinage arose, it was not long before rulers engaged in the act of "coin clipping" in which they would periodically gather the coins from the 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 themselves. People, of course, were outraged, as the expression of their preference for hard money was stifled; but this is an unsurprising effect of central planning.

When it comes to economic systems, free markets make customer preferences irrefutable; central planning causes them to become irrelevant.

Similar to modern day inflation, coin clipping was a way of surreptitiously taxing the population by debasing its currency. Nero, the infamous emperor of the Roman Republic, was the first to engage in this deceptive practice. In doing so, he set a malicious precedent that would be emulated by many successive emperors (and later, central bankers) across many different eras and empires. Each time the value-storage integrity of money was compromised by coin clipping or supply inflation, it was only a matter of time before the society which it bound together started to unravel. Centralizing control over a money supply always has, and always will, lead to expanded wealth disparity as those few (rulers, politicians, central bankers) who can extract value from the many (citizens) have always given in to this temptation. Eventually, this parasitism leads to social unrest and, ultimately, revolt.

Interestingly, as the problem of assaying monetary metals shifted the monetary trust function unto the state-backed coinage, this gave demagogues the means to violate the trust placed in their "public stamps" to enrich themselves. Had a monetary technology existed historically that was

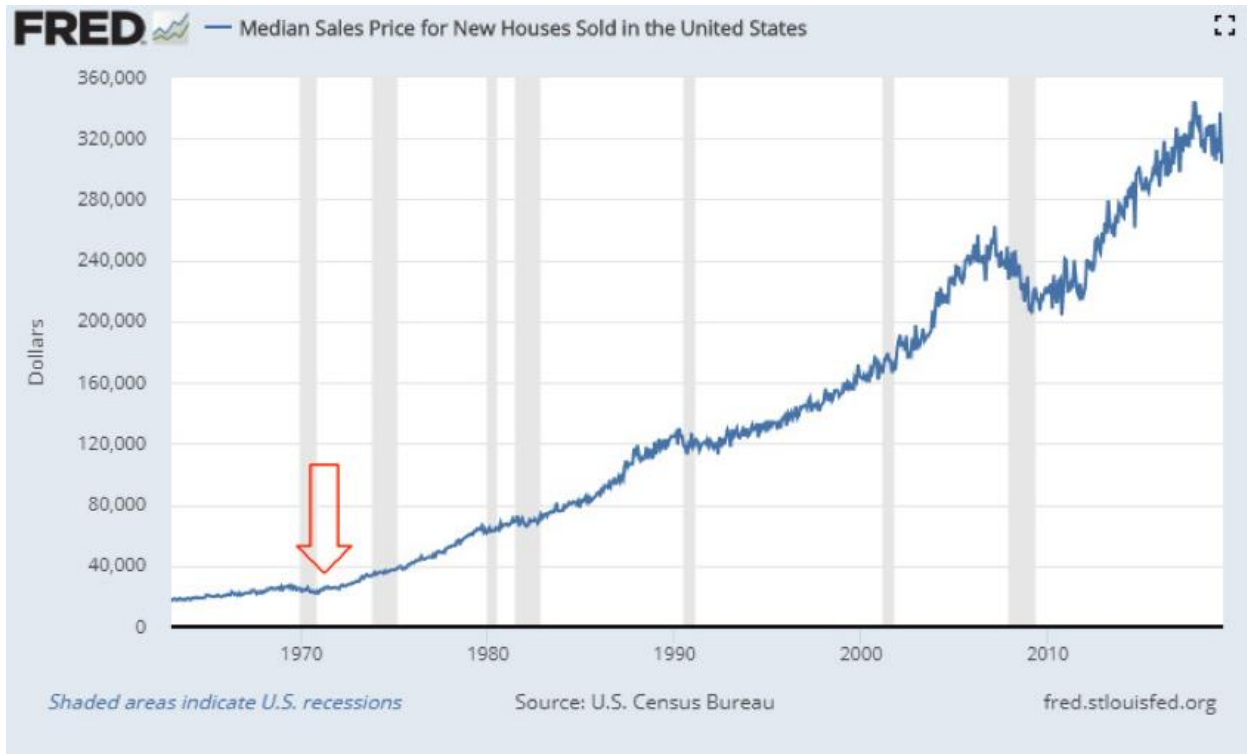
sufficiently counterfeit and confiscation resistant (like Bitcoin), government may have never grown to become such a significant institution in human affairs. Hard to believe perhaps, but true. Lack of trustworthy money caused the state to flourish; over time, the invention of perfectly credible money may, as a side effect, render the nation-state model anachronistic.

Money is the mechanism through which people market-price and exchange their time; it is the trust fabric through which people weigh opportunity costs and decide where to invest their finite energies and capital. When this cooperative mechanism is manipulated by rulers, the societies which run on the softening money begin to disintegrate as trust in the currency deteriorates, thus inhibiting trade and reversing the division of labor. This causes prices to rise and economic crisis to take hold. Unproperly channeled into a centrally planned economic system instead of a free market, greed becomes inherently self-annihilating.

Greed destroys fiat currencies, but greed secures the Bitcoin network.

Instead of learning these lessons of history, central banks pushed this monetary parasitism to unprecedented extremes. According to you Ray, “From 1950 until 1980, debt, inflation, and growth moved up and down together in steadily larger waves, with each bigger than the one before, especially after the dollar’s link to gold was broken in 1971.” The unitary motion of these economic forces was no coincidence. By breaking the peg to gold in 1971, Nixon set the world on an irreversible course that would be marked by successively larger recessions and (attempted) compensatory rounds of quantitative easing. This death-stroke to the gold standard moved the world into uncharted monetary territory, and became the cause of myriad economic and social problems. Here, we will highlight a few of them (for more on this, check out www.wtfhappenedin1971.com)

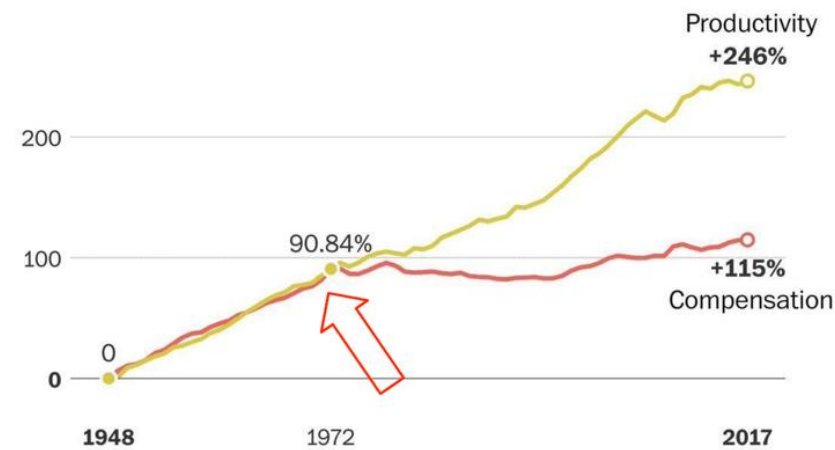
With the store of value functionality of money broken, people began using their homes as savings vehicles, which inflated a housing bubble that bursts in 2008 with disastrous consequences:



The above housing bubble tells another tale of fiat disease: when people use residential real estate as a store of value, whether it's their residence or not, they needlessly drive up the price of shelter, a basic human need. In this way, central banking generates homelessness.

By breaking money's anchor to reality, control over productive assets was steadily shifted into fewer hands with each economic recession and round of money printing (via the Cantillon effect). This caused an unprecedented decoupling of productivity and wage growth:

Growth in productivity and hourly compensation since 1948



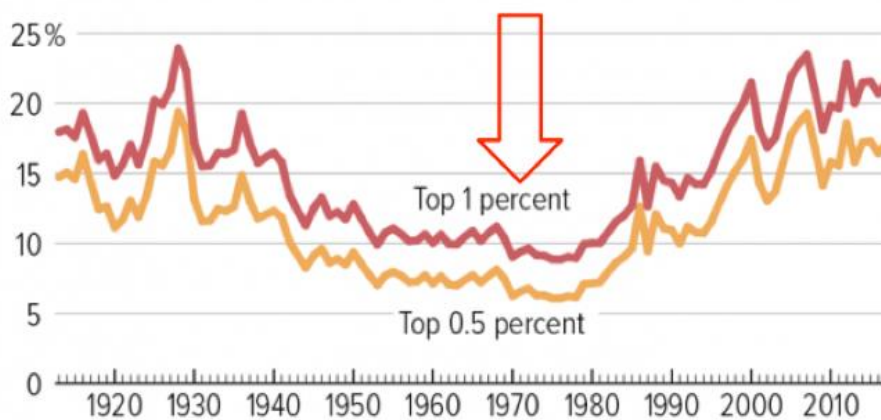
Note: Compensation includes wages and benefits for production and non-supervisory workers

Source: Economic Policy Institute

This divergence between productivity and compensation meant that more value was being captured by the most wealthy at the expense of the poorest:

Income Concentration at the Top Has Risen Sharply Since the 1970s

Share of total before-tax income flowing to the highest income households (including capital gains), 1913-2017



Source: Emmanuel Saez, based on IRS data

Such distortions and wealth redistributions are the inescapable effects of monetary central planning. By manipulating the price of money (the interest rate) central banks spur over-borrowing, capital misallocation, and market distortions. By holding the interest rate below its naturally determined value (at the intersection of the supply and demand curves for loanable funds), central

banks interrupt the natural chains of cause and effect which maintain dynamic market equilibria. This, in turn, causes market price movements to become more a function of monetary policy than of actual supply and demand curves. Ray observed this firsthand: “In 1978–80 (as in 1970–1971 and in 1974–75) different markets began to move in unison because they were more influenced by swings in money and credit growth than by changes in their individual supply-demand balances.” This causality still holds and becomes abundantly clear when seen from the right perspective:



A correlation as spurious as umbrella ownership in Seattle.

These market distortions would not exist in a world with a free market for money. Free markets are ruthlessly efficient and trimming excesses and encouraging optimal allocation of resources; which is why they are so ruthlessly effective at promulgating hard money, because people will naturally select the most liquid asset that best holds its value across time as money first and foremost. Hard money eliminates market distortions because its supply remains rooted in economic reality and beyond the reach of self-interested central planners. Simply, by transitioning to a free market money like Bitcoin, we can eliminate the prime driver of wealth disparity — money supply inflation.

To better understand the root cause of wealth disparity, we use an approach advocated by you Ray: as you've said, (p.489) "Root causes are described in adjectives, not verbs, so keep asking 'why' to get at them." Let's begin our analysis:

Root cause discovery process:

A primary cause of social unrest and societal disintegration is wealth disparity. Alarming, this has been on the rise in advanced economies all over the world.

Why is wealth disparity growing?

Disparity in wealth holdings is rooted deep in the monarchical history of mankind. Although some economic inequality is natural, as people are born with unequal skills and predispositions, the (growing) levels seen in modernity are anomalous. Today, few people own most of the productive assets. Under a system of monetary central planning, these few have privileged access to newly printed fiat currency, which represents a redistribution of productive assets to those who receive the newly printed money first at the expense of those who receive it later (via the Cantillon effect).

Why do few people have privileged access to newly printed money?

Those with the most control over productive assets have leveraged their position to monopolize the market for money. These positions are reinforced via the lobbying mechanism, a system of institutionalized bribery, that heavily influences public policy in favor of its financiers' private interests. Once a monopoly position is firmly established, they employ monetary policy as a means for implicitly taxing entire populations to further enrich themselves (again, via the Cantillon effect).

Why is there a legal monopoly on money?

Again, the few who own the most productive assets within a society are able to (heavily) influence the legal frameworks they operate under. Naturally, these few favor laws which benefit their interests. Primary among these interests is the ability to confiscate wealth via inflation. This privileged position is protected via the government monopoly on violence. Inflation allows early accessors of new liquidity to perpetually extract wealth from all the market participants coerced into using the fiat currency – those who resist face incarceration or violent retaliation.

Why is violence used to insulate the legal monopoly on money?

The root cause of violent coercion such as this is the fearfulness inherent to egoic human behavior. People naturally seek to secure themselves against the uncertainties inherent to the future. To this end money, a tool of pure optionality in the marketplace, is the ultimate hedge against the future. Using

the government monopoly on violence, private interests gradually were able to monopolize the market for money, thus obstructing its natural course. Simply, central banks have acquired absolute power, which as we all know, corrupts absolutely. Fiat currency is the ultimate expression of unfree market dynamics.

Per this root cause analysis: the “why” of a growing wealth disparity is causally rooted in the adjective “unfree”. The root cause of a growing wealth disparity, then, is an unfree market for money. Fiat currency is a tool for restricting freedom and confiscating wealth. Bitcoin, like its predecessor gold, is a purely free market money – a tool for maximizing freedom and preserving wealth.

Monetary inflation, a property unique to centrally planned money, is purely a means of wealth confiscation – it does not offer a single equitable benefit to the people. Not one. The virtually limitless power control over the fiat currency printing press affords is the very cause for its existence and monopolization; it is both the means and the ends of monetary socialism. Fiat currency is a governmental tool for taxing, controlling, and manipulating people. As Thomas Jefferson once warned:

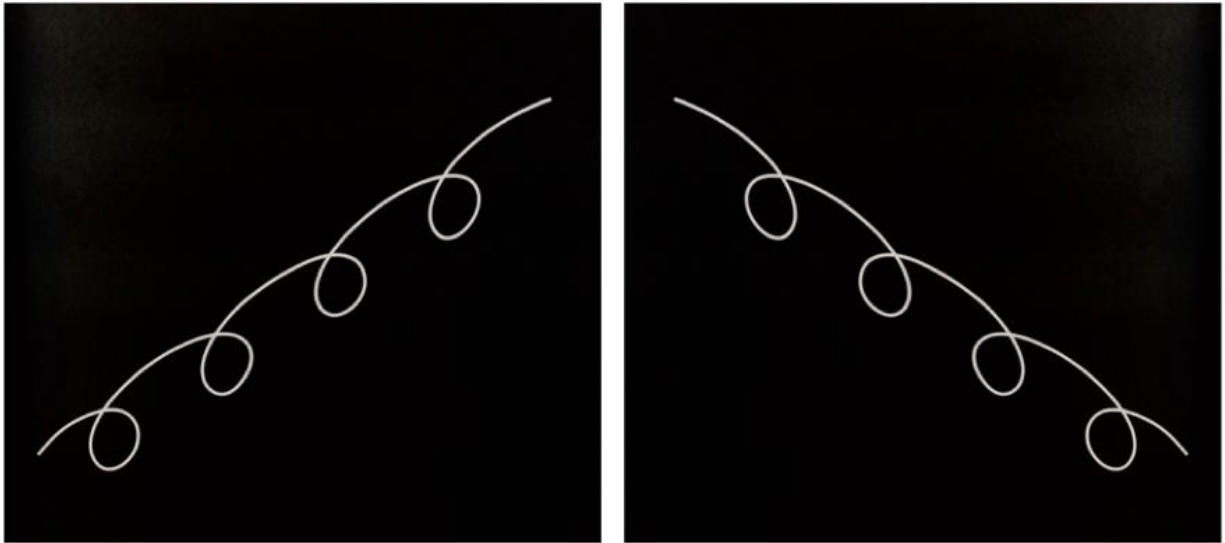
“If the American people ever allow private banks to control the issue of their currency, first by inflation, then by deflation, the banks and corporations that will grow up around them will deprive the people of all property until their children wake up homeless on the continent their Fathers conquered....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

By attempting to centrally plan money, mankind marginalizes his own potential. Although Bitcoin has demonstrated its disregard for the legal restrictions which insulate fiat currencies, it's impossible to know what monetary technology the market would naturally select absent government interventionism. Monopolization increases costs and stifles innovation, the exact opposite of the effects generated by free markets. Devolution is the inevitable and disastrous effect of monopolization, whereas free markets cause the reverse – evolution.

Evolution

(p.142) “Evolution is the single greatest force in the universe; it is the only thing that is permanent and it drives everything.”

Change is the only thing that never changes. And when something is finished changing, it is finished. As such, all things exist in either a state of evolution or devolution:



For better or worse, change never changes.

Whether improving or declining, all things exist in flux. As you've said Ray, (p.142) "As I thought about evolution, I realized that it exists in other forms than life and is carried out through other transmission mechanism than DNA. Technologies, languages, and everything else evolves." Money, like a spoken language, is an informational protocol. Unlike language, money has evolved to inhabit many different forms. Seashells, salt, cattle, beads, stones, precious metals and government paper have all functioned as money at one or more points in history. 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.

Historically, the hardest monetary technology to produce which exhibits otherwise comparable monetary traits (durability, divisibility, portability, recognizability) outcompetes more easily produced forms to become dominant on the free market – an asset that succeeds in this way is called hard money; a technology that is discovered through market-driven natural selection.

As we have learned, the rise of fiat currency was the result of governments coopting gold – which had risen to global dominance on the free market because of its superior scarcity relative to other monetary metals, which themselves exhibited superior monetary characteristics compared to other monetary technologies (like seashells, salt, cattle, etc.). By issuing paper money redeemable in gold, governments were able to resolve its one drawback – suboptimal divisibility. However, governments eventually eliminated

redeemability of paper money for gold, thus ushering in the age of fiat currency. Lack of scarcity would have resulted in the extinction of fiat currency long ago if it weren't for the anticompetitive efforts of governments in the gold markets (if you haven't yet, check out Gata.org). In this sense, gold is the last freely chosen money in the marketplace and fiat currency is but an apparition of this multi-millennia-old monetary metal; a deception that has been haunting human progress since its inception in 1971. As Taleb describes it:

"...institutions block evolution with bailouts and statism. Note that, in the long term, social and economic evolution nastily takes place by surprises, discontinuities, and jumps."

In free markets, competition generates the information that vitalizes innovation — the man-made type of evolution. Completely isolated from the discipline of the market by legal monopoly, central bank issued fiat currencies have softened tremendously, in both value and functionality. This is unsurprising: any complex system — whether it be a technology, an economy, or an organism — that is isolated from the shaping of competitive forces will naturally devolve over time. As you've observed Ray, (p. 147) "One of the great marvels of nature is how the whole system, which is full of individual organisms acting in their own self-interest and without understanding of guiding what's going on, can create a beautifully operating and evolving whole. While I'm not an expert at this, it seems that it's because evolution has produced a) incentives and interactions that lead to individuals pursuing their own interest and resulting in the advancement of the whole, b) the natural selection process, and c) rapid experimentation and adaptation." This marvelous dynamic is at the heart of free market competition, open-source adaptation, and Bitcoin which, as we have seen, is both a free market in and unto itself and an open-source instance of digital hard money.

Bitcoin is an evolutionary leap forward for money: it combines the divisibility, durability, portability, and recognizability of pure information with the absolute scarcity of time to form the most impeccable monetary technology the world has ever known.

As you've said in regards to evolution, (p. 124) "I realized that passing on knowledge is like passing on DNA — it is more important than the individual, because it lives way beyond the individual's life." Ray, isn't it time for humanity to transition to a form of money that exists beyond the schemes, machinations, and manipulations of those who are able to wrest control of its controlling mechanisms? By centering an evolved monetary social contract on an immutable ruleset, we can eliminate the incentives to fight over gold or international reserve currency status and therefore enhance mankind's cooperative capacity, which in turn will accentuate the division of labor, enhance productivity, and increase aggregate wealth creation worldwide. It's time for money to be governed by rules instead of rulers, and Bitcoin gives us

the opportunity to make this transition once and for all. Imagine how much human ingenuity could be freed up worldwide if we eliminated the need for monetary policymakers, the army of analysts who watch them under a microscope, and the heavily distorted price signals caused by soft money.

Each of us are nodes of information – biological machines expressing our genetics, experiences, and ideas – that are collectively best served by successfully minimizing impediments to expression like policies, hierarchies, and illegitimate institutions. As Noam Chomsky said:

“Institutional structures are legitimate insofar as they enhance the opportunity to freely inquire and create, out of inner need; otherwise, they are not.”

Modes of organization which favor merit-based competition and rely on natural selection to determine which ideas flourish help us flourish. This is the free market (and idea meritocratic) paradigm: unobstructed exchange is always superior to that which is centrally intermediated, regulated, or manipulated. Dissimilar to cognitive learning, evolution does not distinguish between the observer and the observed, enabling it to “learn at the edges” by absorbing the successes and failures of its constituents (cells, individuals, exchanges, or businesses) through a filter of natural selection and incorporating them into its own form (a body, society, market, or economy).

Global free markets, coordinated via truthful price signals, can be thought of as a human hive-mind constituted of innumerable interpersonal exchanges; an organic, bottom-up system in which resources, risks, and human time are priced and allocated according to the prevailing economic realities faced by society. This collective mind is the macrocosm of our individual mind microcosms, which have naturally evolved in a bottom-up way. Existing as illegitimate, closed-source economic fiefdoms, central bank money monopolies inhibit natural selection and diminish the evolutionary potential of our global collective mind.

<https://twitter.com/Breedlove22/status/1155304556164571137?s=20>

As you’ve observed Ray, (p.213) “This *universal brain* has evolved from the bottom up, meaning that its lower parts are evolutionarily the oldest and top parts are the newest.” Why should we expect the amalgamation of human economic actions to evolve any differently? Free markets enable price and technology discovery from the bottom up, as they completely lack any centralized governing body. Hard money has always evolved on the free market and is the norm of human history; only over the past century has it been so explicitly coopted by a few at the expense of everyone else. Using a Darwinian analogy: what natural selection is to gold, artificial selection is to fiat currency. In the same way mankind created designer dogs from wolves, or

Monsanto self-terminating seeds from naturally-occurring seeds, so did he create fiat currency from gold. Bitcoin, as an unstoppable free market money being naturally selected for favorably in the marketplace, may in this sense be considered the reemergence of hard money in the modern world; a natural reversion to the free market foundations of money through an evolved (and evolving) monetary technology.

As a hard money that is monetizing in real time, Bitcoin outcompetes other forms of money in market-driven natural selection, whereas fiat currencies exist exclusively due to monopoly-driven artificial selection. As Bitcoin transcends the artifices that preserve the monopolistic position of fiat currencies, it forces these monetary technologies to compete based on their own (inferior) merits, and promises to push them into extinction.

<https://twitter.com/Breedlove22/status/1179117506696376320?s=20>

One would be hard pressed to find a worse technology from both a functional and societal value-add standpoint. As you've said Ray, (p.272) "To be good, something must operate consistently with the laws of reality and contribute to the evolution of the whole; that is what is most rewarded." In this sense, fiat currencies are bad — really bad. Not only do they give politicians a lever by which to control people, they also erode societal cohesion as their primary function — the storage of value across time — is repeatedly compromised in favor of multifarious political agendas all over the world. As Taleb says:

"...it is downright irrational if one holds onto an old technology that is not naturalistic at all yet visibly harmful, or when the switch to a new technology... is obviously free of possible side effects that did not exist with the previous one. And resisting removal is downright incompetent and criminal (as I keep saying, the removal of something non-natural does not carry long-term side effects; it is typically iatrogenics free)."

Viewed on a grander scale, Bitcoin seems to be a natural evolutionary step towards freer society:

- Gutenberg's Printing Press gave us decentralized analog knowledge (which separated Church and State)
- Democracy gave us decentralized government
- The internet gave us decentralized digital knowledge
- Bitcoin gave us decentralized digital money (which may one day separate Money and State)

Indeed, it is amazing that a lone, anonymous programmer released an open-source protocol that is now a viable contender for the world reserve currency whereas Facebook, one of the most flush corporations in the world, has been unable to move forward with its currency project due to regulatory roadblocks.

Digital technology reshapes reality, and decentralization enables us to create leaderless organizational structures based more so on rules than rulers. Bitcoin is the latest and greatest expression of this overarching trend away from centrality and towards a more natural ordering of things.

<https://twitter.com/perbylund/status/1177589207491063812?s=21>

Like you Ray, I consider myself a shaper who experiences “the gap between what is and what could be as both a tragedy and a source of unending motivation.” I see a world shackled in financial slavery, with central bankers and their inner circles as the great parasites of wealth created by working people all over the world. Centrally planned money is straight out of the socialist playbook and, aside from a brief period in the late 19th century when the world was mostly on a gold standard, we have never seen a truly free market for money. An economy is like life itself; in life, we do not expect to understand events as they occur, at least with total causality and clarity in mind, but looking back on them we gain a better understanding. Bitcoin is alive; while it is impossible to say where it is heading with certainty, it is monetizing and evolving in real time, and its proponents all have skin in the game.

Evolution can only happen if the risk of extinction is present. Only systems with skin in the game are capable of evolution; absent this, devolution becomes inevitable. Systems learn and evolve through the death of their components; the biological manifestation of this via negativa process is called apoptosis. Any institution that cannot glean lessons from its undying components loses touch with reality as it grows until nature ultimately overrules its energetic imbalance in a mighty swing of the universal pendulum — whether by way of renaissance or revolution.

Therefore, we evolve best by sharpening our organizing principles against the palpable feedback gathered from falsifiable entrepreneurial experiments conducted at the front lines of our understanding, where each failure edifies the economic ensemble as to what does not work so that its next individual efforts will be emboldened by the greater experience gained. In this way, we are better served by the free market, with its bricolage of tactile sensory inputs from its entrepreneur-led, optionality-rich explorations of economic realities instead of the unwavering unidirectionality of a centralized plan. The choice of the technology we use as money is best arrived at in an uninhibited marketplace in the same way other technologies are invented, shaped by competitive forces, and tinkered with over time; in accordance with the timeless principle behind both innovation and evolution.

Timelessness

(p.121) "With time and experience, I came to see each encounter as "another one of those" that I could approach more calmly and analytically, like a biologist might approach an encounter with a threatening creature in the jungle: first identifying its species and then, drawing on his prior knowledge about its expected behaviors, reacting appropriately."

History doesn't repeat, but it does rhyme. Every moment and person are unique, but they tend to conform to some prior pattern or archetype. Personality types can be characterized and filtered by a variety of metrics including Meyers-Briggs and management tools like the Baseball Cards Bridgewater uses. Modern-day events are often foreshadowed by historical happenings. By thoughtfully studying these archetypal forms of characters and events, we are better equipped to deal with the uncertainties inherent to life and work. As the axiom says, "Those who do not learn history are doomed to repeat it."

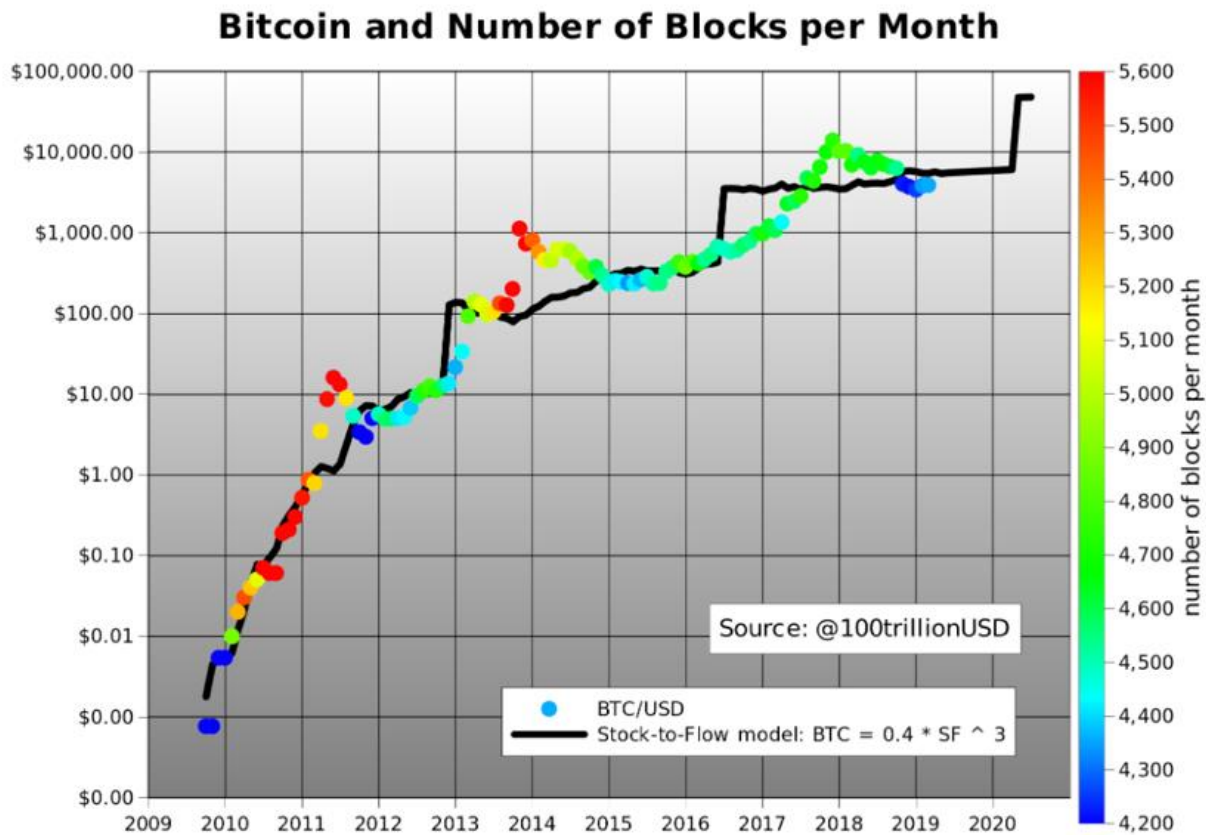
Bitcoin is often called digital gold for a good reason; the best analogy for its emergence is the monetization of gold. Money is a market pricing and coordination mechanism for human time; it reflects the present value of the (liquid) time savings generated by subdivided labor and denominates prices. The relative inelasticity of gold's supply to other monetary metals is the reason it outcompeted them to become dominant in the free market before central banking commandeered it (seriously, check out Gata.org). Its ascent as money is based on timeless economic principles from the Austrian school. Despite the justifications for schemes like fiat currency in 1971 (revoking dollar redeemability for gold was said to be a "temporary" measure) and MMT today, the minds of prominent historical figures agreed universally that only monetary metals were actual money:

- JP Morgan said in his 1912 testimony to congress: "Money is gold, and nothing else."

- Thomas Jefferson is quoted as saying: "Paper is poverty, it is only the ghost of money, and not the money itself."

Even you Ray once said: "If you don't own gold, you know neither history nor economics." In the free market, fiat currency has never existed. Only through state intervention has money come under the monopoly control; the state had no more of a hand in the development of money than it did language. So, to understand the ascent of Bitcoin from a quantitative perspective, we must first understand how gold came to dominate the market for money. In his masterful work The Bitcoin Standard, Saifedean Ammous sheds light on how Bitcoin can be perceived as "another one of those" in the sense that it is following a similar monetization path as that followed by gold. In short,

throughout history societies have naturally coalesced around the monetary technology exhibiting the highest “stock-to-flow” ratio. When we look at the stock-to-flow quantitative model put together by PlanB, we see that the Bitcoin price has an extremely high correlation to this key valuation metric:



Ignoring the lessons of history is a great strategy for being naturally selected out of the gene pool.

Said simply, the attribute of money that causes it to retain its value is its scarcity. As a former commodities trader Ray, I am sure you will understand the value of this model. In free market monetary competition, the scarcest money wins, as it is superior at protecting wealth across time. Bitcoin is on an inevitable path to become the highest stock-to-flow asset in human history, overtaking gold by a factor of two in the year 2024. Bitcoin’s ever-constricting new supply flow as a percentage of existing stock is encouraging its adoption first as a store of value before it begins fulfilling the other functions of money more adequately. This is consistent with the monetization path taken by gold – as the classical economist William Stanley Jevons remarked:

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.

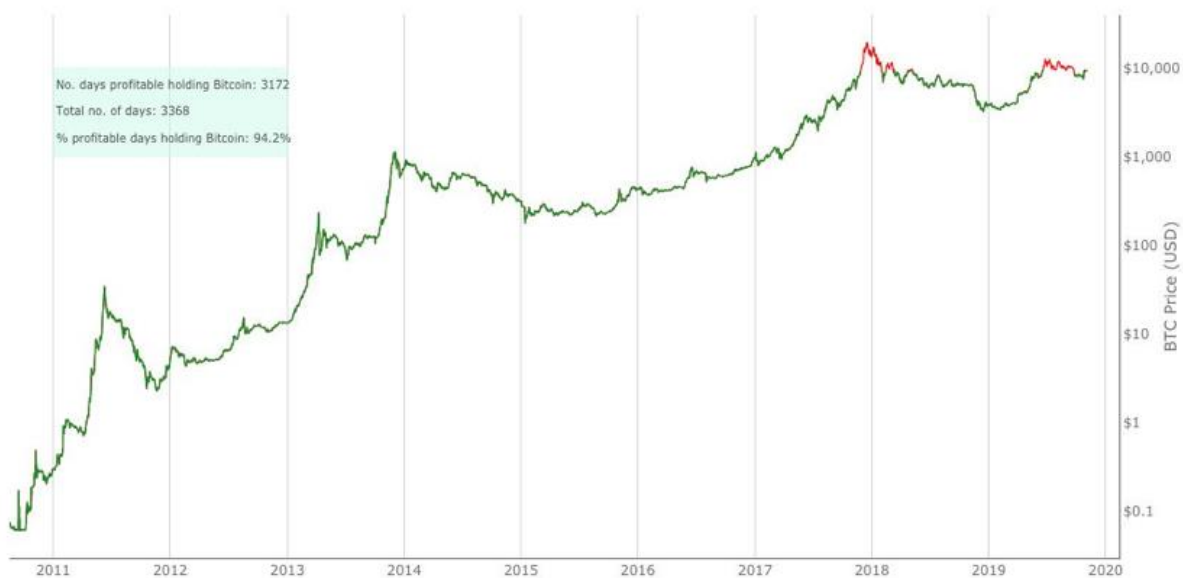
So, in terms of monetization, Bitcoin is “another gold” following a similar evolutionary path – collectible, store of value, medium of exchange, and finally a unit of account. In an even deeper sense, Bitcoin can be considered “another one of those” as a part of the resurgence of ancient wisdom in the modern world. Yoga, meditation, Ayurvedic medicine, mindfulness, paleo diets, Ayahuasca, acupuncture – citizens of the digital age are rediscovering the deep roots of humanity. As the collective learnings of mankind are now accessible to everyone with an internet connection, this is likely a key driver of this worldwide phenomenon. Bitcoin, as a pure expression of Austrian economic thought, is yet another case of ancient wisdom’s resurgence into modernity. By releasing the economic juggernaut that is Bitcoin into a world dominated by monopoly money, Satoshi put Keynesian economics and its “highly mathematized” theories (central bank circumlocutory propaganda) to the test and, thus far, has succeeded wildly in disproving their validity.

<https://twitter.com/murraysuggests/status/1181515143240409089?s=21>

Bitcoin is the best performing asset in human history, even when its sharp drawdowns are taken into account. It has offered the highest risk-adjusted rate of return of any asset class over the past decade (as quantified by the Sharpe ratio), and outperforms even further when only the negative volatility is taken into account (most of Bitcoin’s price volatility has been positive). Indeed, it has been difficult to invest in Bitcoin unsuccessfully:

Bitcoin Profitable Days

Source: lookintobitcoin.com



These are the days.

As you've said Ray, "the greatest success you can have as the person in charge is to orchestrate others to do things well without you." This is exactly what Bitcoin does for all current and future generations; it takes monetary policy out of the sphere of political influence and protects it with timeless, immutable, and mathematically-enforced rules beyond the machinations of mankind. These rules are fixed and fully transparent — resistance to confiscation, censorship, inflation, and counterfeiting — for all to see and rely upon across time. In this sense, Bitcoin is a timeless monetary system into which people can escape the walled-garden economies of a central bank dominated world; an man-made antidote to the poisoned society of man — as Henry Miller described it:

"Society had so complicated the relations between men, had so enmeshed the individual with laws and creeds, with totems and taboos, that man had become something unnatural, something apart from nature, a phenomenon which nature herself had created, but which she no longer controlled."

By providing a more sound substrate for economic planning and coordination, Bitcoin promises to reduce the toxic bureaucracies that have festered around the central banking model. Outfitted with a sound store of value, people will no longer be forced out further along the risk curve to protect their wealth, making real estate more affordable and unicorn companies more rare. As state revenues naturally decline as a result, government-sponsored "zombie" companies and monolithic "too big to fail" institutions will gradually slip into irrelevance. Finally able to protect their wealth from confiscation via inflation, people will be better equipped to capitalize their own businesses and pursue their dreams. And a world in which people are doing what they love is better for everyone. The majority of most people's lives is spent working to earn money, and Bitcoin stands to change the very nature of both work and money. In this sense, Bitcoin is bound to change mankind more than he will ever change Bitcoin.

Meaningful Work

(p.538) "We work with others to get three things: 1) Leverage to accomplish our chosen missions in bigger and better ways than we could alone 2) Quality relationships that together make for a great community 3) Money that allows us to buy what we need and want for ourselves and others... (p.216) man is perpetually suspended between the two extreme forces that create us: 'Individual selection which prompted sin and group selection which promoted virtue.'"

Since time immemorial, man has been driven to take both selfish and selfless actions. The principles which guide people's actions are a composite of family values, social experience, incentive structures, and natural predilection. Many of us inherit the political and religious leaning of our parents or family, which

influence our value systems. However, our experience in the world also shapes (and continually reshapes) our values as well. These external influences are both, of course, undergirded by our natural inclinations and preferences. In short, we are all born unique, but are also products of our environments. Money, as the most interconnective social phenomenon in the world, is one of the most significant external forces shaping our thinking, planning, preferences, relationships, and actions. Think about it: how many times have you thought or talked about money in the past 24 hours? For most of us, many, many times. The nature of the money we use is a powerful determinant of whether we act viciously or virtuously.

In this respect, Bitcoin has an interesting impact on personal character. As Jimmy Song laid out ([here](#), [here](#), and [here](#)), Bitcoin (and hard money more generally) encourages people to develop virtues such as prudence, temperance, and justice. Since fiat currency suffers from perpetual dilutions of value, its users are incentivized to spend and borrow; in other words, to be less prudent with their money. Bitcoin is the reverse; its fixed supply and diminishing inflation rate ensures that it appreciates as global economic output grows and incentivizes people to save and invest. As more people adopt Bitcoin, their time preferences are shifted to become more future-oriented. In this way, Bitcoin encourages people to treat the future as something to be invested for instead of borrowed against.

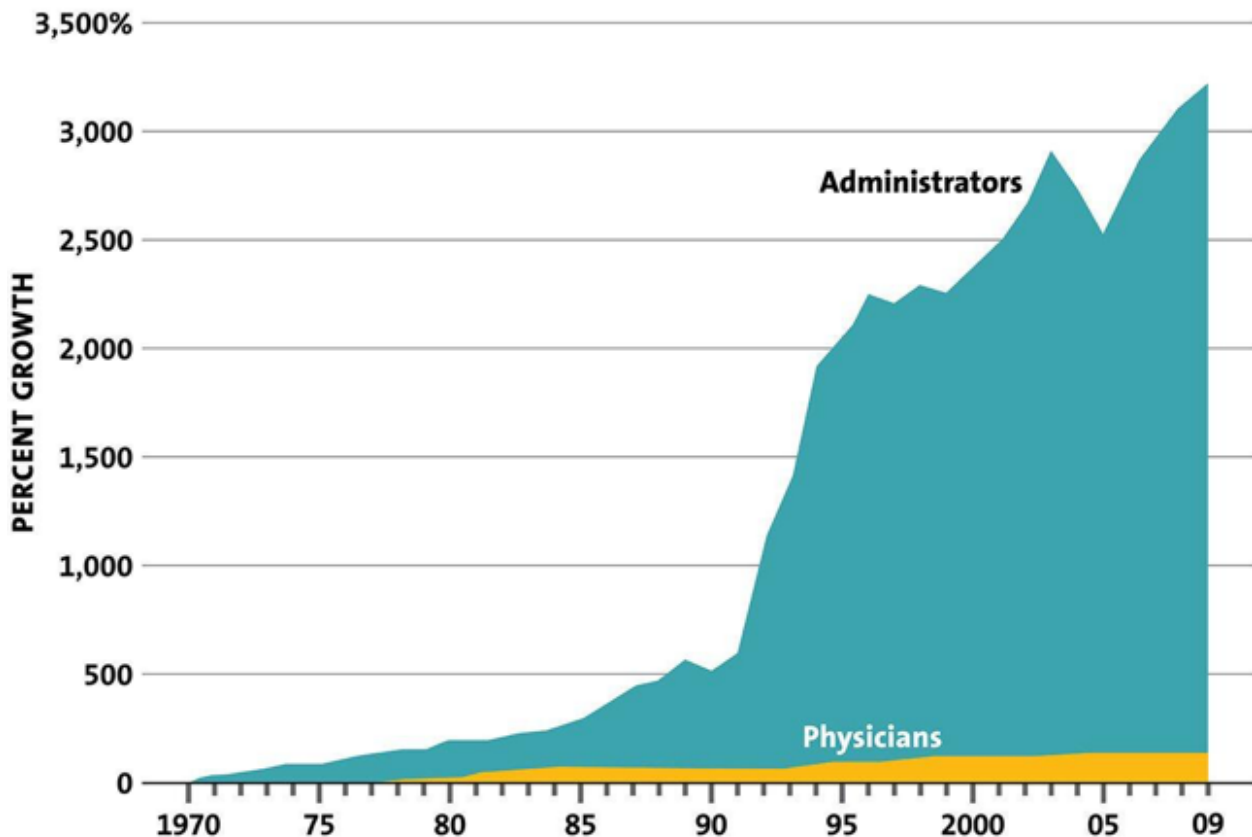
Since its supply is unmanipulable, Bitcoin is gradually eroding the financial capability of governments to provide guarantees in the form of welfare or bailouts. It's easy to see how this softens temperance: if you knew your job were guaranteed no matter your performance, how hard would you try? Similarly, a long history of tax-payer funded bailouts for failed banks without skin in the game have encouraged them to take on steadily more risk, as any gains realized from their efforts accrue to their shareholders whereas any catastrophic losses that are incurred are paid for by taxpayers (against their will). This contradicts the tradition in ancient Catalonia, in which failed bankers were beheaded in front of their banks (talk about skin in the game). By providing a means of privatizing gains and socializing losses, governments cause the market to misprice risk and erode the value of temperance: the skill of rightsizing one's exposures in life on the risk and reward spectrum. With the risk of failure removed, beneficiaries of government guarantees no longer have skin in the game, and therefore take on risks intemperately. Repeated blow ups and taxpayer anger, as savings are eroded to bail out "too big to fail" institutions, fragilizes the delicate bonds that hold society together.

Justice is embodied in fair treatment; it encompasses integrity, honesty, and respect. When an action is taken that benefits one group disproportionately at the expense of another, we can say that it is unjust. Inflating money supplies is an unjust action, as it does not offer a single equitable benefit, and instead

enriches the politically-favored few closest to the monetary spigot at the expense of the many farther away from it. Using inflation as a means of funding welfare and warfare, new government programs are continually implemented while old ones are kept functional despite their inefficiency or uselessness. As Milton Friedman once said, “Nothing is so permanent as a temporary government program”. Again, government intervention severs skin in the game and decouples the intention of these programs from their results. The impact of this is a swelling class of government dependents, workers, and contractors that function inefficiently and only exist because of the government’s ability to create new money. Interventionism of this kind distorts the information provided by market pricing and, therefore, makes fair dealings much more difficult. In a free market run on hard money, only industrious people who add value and deal fairly in an economy are rewarded. Paradoxically, as governments strive to ensure equality of outcomes, they incentivize unjust treatment. At the core of this rottenness is monetary inflation: a legally enforced injustice.

In an economy run on soft money, intermediary business models and professional roles designed to extract value from the money that originates at the center (the central bank) and flows outward into an economy (through successively lower tier banks and eventually to businesses and consumers) start popping up everywhere. These intermediary functions add little value to an economy yet capture a disproportionate share of the value of economic output; a dynamic commonly called “rent-seeking” that is unsurprisingly pervasive in industries that suffer from extensive government meddling like healthcare, education, and banking. After the last vestiges of hard money were abandoned in 1971, rent-seeking has exploded; consider the case of healthcare:

GROWTH IN PHYSICIANS AND ADMINISTRATORS



SOURCE: Bureau of Labor Statistics; NCHS; Himmelstein/Woolhandler analysis of CPS

Physicians are productive, administrators are extractive: the cartelization of healthcare is a fiat disease.

Meaningful work is being compromised by central banking. There has been a demographic shift from value-additive to value-subtractive positions – as evidenced by the training of more bankers than engineers, or the academic credentialing transition from medicine to finance. In a free market, compensation is reflective of a role's usefulness to society. But with monetary socialism, there are greater financial incentives to work closer to the spigot of fiat currency in roles that are mostly non-productive and extractive. Hayek summed this up nicely:

"It is not merely that if we want people to give their best we must make it worthwhile for them. What is more important is that if we want to leave them the choice, if they are to be able to judge what they ought to do, they must be given some readily intelligible yardstick by which to measure the social importance of the different occupations. Even with the best will in the world it would be impossible for anyone intelligently to choose between various

alternatives if the advantages they offered him stood in no relation to their usefulness to society.”

One more thing: most rent-seeking jobs suck! How many accountants, bankers, or administrators do you know that “love” their job? Many of these jobs are a direct result of the lacking social scalability inherent to monetary socialism. The more we can globally standardize onto a hard money, the more productivity we generate collectively, the lower the cost of living becomes, and the less we have to work individually.

Money is just a means to an end: as you’ve said Ray, (p. 417) “Remember that the only purpose of money is to get you what you want, so think hard about what you value and put it above money.” I think it’s safe to say that most people want to live a fun and productive life full of fulfilling relationships. To this end, the type of money society runs on is of paramount importance. The utility, supply, and value of fiat currency cannot be trusted; since money is the trust network through which all of our commercial relationships are carried out, this lack of trust in the money infects the trust relationships amongst its users. Again, to get what we want, we need reliable protocols for commercial interaction like private property rights, rule of law, and manipulation-proof money. As central banks confiscate and redistribute wealth created by the work of others, they cut these cornerstones of capitalism and weaken the foundations of civilization.

Money and speech are media of expression; any inhibition or censorship of these societal building tools, which together are responsible for nearly all human coordination and communication, contradicts the most basic liberties (1st Amendment in the US) intrinsic to Western Civilization. There is zero justification for a system that suppresses verbal or financial expression. By organizing ourselves within a truly free market capitalist system that incentivizes basic morality (don’t steal, don’t kill), we can advance our civilization to new levels and dramatically improve the quality of human relations.

Meaningful Relationships

(p.216) “The rewards of working together to make the pie bigger are greater than the rewards of self-interest, not only in terms of how much pie one gets but also in the psychic rewards wired into our brains that make us happier and healthier.”

The history of mankind has been marred by episodic violence – skirmishes between individuals, tribes, and, later, nation-states have been a consistent thread in the story of humanity. Like other animals, man seeks to maximize the odds his genes will be passed on to successive generations and will fight tooth and nail for his chance. Counterbalancing this self-seeking behavior are the

benefits offered by a peaceful and cooperative society — the division of labor, rising standards of living, and more free time to spend as one sees fit. Between the 16th and 19th centuries, conflict-related deaths as a share of world population averaged less than 1%. In the 20th century, this figure more than quadrupled to over 4%:

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

This is no coincidence. Inflating fiat currency supplies gives governments a much cheaper and more surreptitious way to finance military operations as opposed to direct taxation or selling of war-time bonds. As Ron Paul said:

“It is no coincidence that the century of total war coincided with the century of central banking... If every American taxpayer had to submit an extra five or ten thousand dollars to the IRS this April to pay for the war, I’m quite certain it would end very quickly. The problem is that government finances war by borrowing and printing money, rather than presenting a bill directly in the form of higher taxes. When the costs are obscured, the question of whether any war is worth it becomes distorted.”

As the enablers of inflation, this institutionalized system of time theft and financial subjugation, central banking is the mechanism through which government confiscates the resources necessary to fund its belligerent efforts. As Mises remarked in 1919:

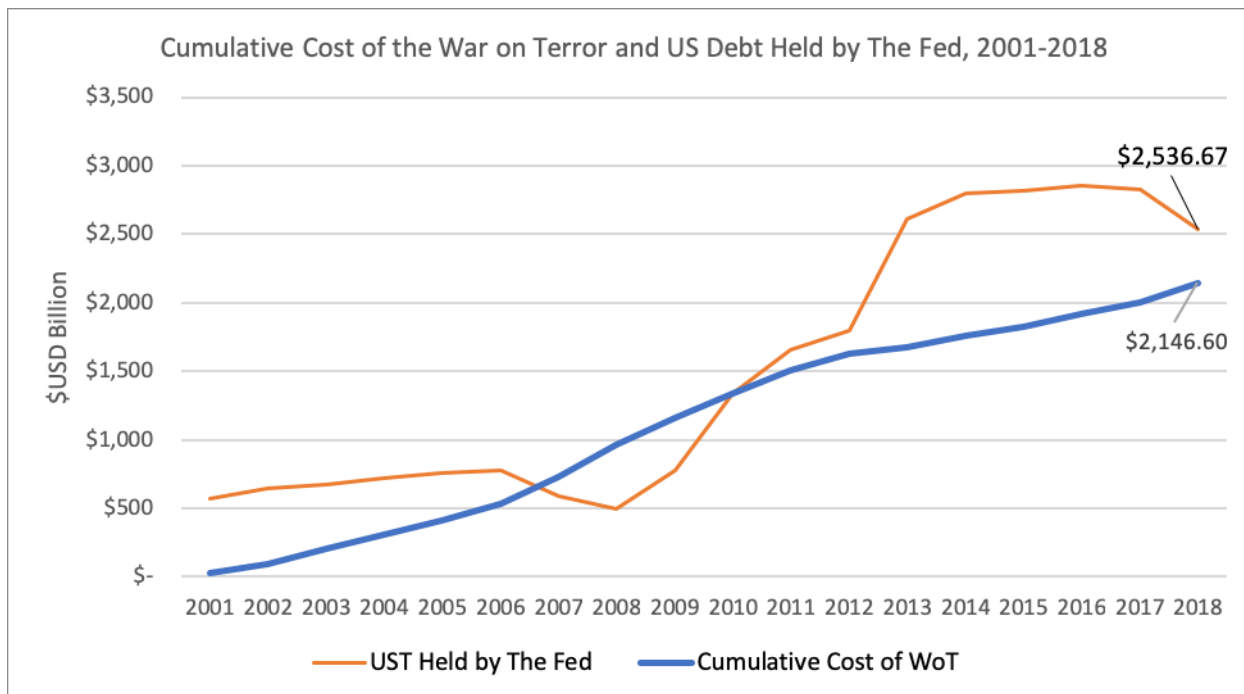
“One can say without exaggeration that inflation is an indispensable means of militarism. Without it, the repercussions of war on welfare become obvious much more quickly and penetratingly; war weariness would set in much earlier.”

Before the fiat currency experiment, it was a common refrain among warring nations that “the gold standard must be abandoned”. Clearly, it was in the best interest of these nations to sever the monetary anchor to time since debt-based money unlocked much more potential for borrowing against the future (via inflation) to finance current war efforts. Of the three ways governments can generate revenue — taxation, borrowing, and inflation — the latter is clearly

more preferable for governments as its negative consequences are spread out over long periods of currency debasement and the shadowy, implicit tax imposed by inflation in the form of rising prices is less well understood by citizens (and rising asset prices helps paper over the perceived damage, although this is largely illusory).

Expansionary monetary policy was the key to financing the US military operations during the Vietnam War. Although the war-time economy seemed strong during the 1960s, US citizens would suffer economically in the echo of this economic intervention as the 1970s became mired in stagflation (low growth, high unemployment, and high inflation). Besides the death and destruction wrought during the war, there was economic devastation in the US and abroad. Between 1965 and 1984, the Dow index suffered a drawdown of 80% from its peak value on an inflation-adjusted basis in the wake of this soft-money-fueled-military-spending-spree. Unfortunately, this pattern of warfare funded through inflation would persist well into the new millennium.

After its great successes with its War on Poverty and War on Drugs, early in the 21st century, the US would launch its “War on Terror”. Over the course of the following 17 years, with the cumulative cost of the “war” (more accurately, an imperialistic military campaign) reaching over \$2.1T in direct governmental expenses, we witnessed The Fed print money and purchase US government debt (US Treasuries or UST) almost exactly equal to the cost of the war:



Clearly, it is no exaggeration to say that the US central bank money machine and the US war machine are intimately connected. Central bank enabling of government war machines is a perpetual bane to humanity. Neither central

banks nor military regimes are accountable to anything other than their own self-interests. In reckless pursuit of their own politicized ends, these institutions siphon away vast swathes of societal wealth to fund destructive military campaigns; this “twin demon” problem of wealth confiscation and capital destruction is the most anti-economic force in the world today. In the face of this diabolic menace, the world has but one hope: the separation of money and state.

As with all other critical commodities and industries, the free market is the best mechanism for allocating capital, promulgating innovation, and properly pricing risk. The singular purpose for the monopolization of the market for money by government is its unquenchable thirst for power; it imposes itself on citizens with hortatory messages from central banks and relies on the submissiveness of citizens. Fiat currency facilitates an exploitative relationship between governments and their citizens in which the former harvest the fruits of the latter’s labor in exchange for “protection”.

Wars do not protect the public, they tax it. Wars do not promote the public good, they destabilize it. Wars do not stimulate economies, they devastate them.

Throughout history, money has been both the means and ends of all war. People have always fought to control more resources or territory, and have wreaked havoc on each other in the process. Warfare is antithetical to meaningful relationships. If we want to build a world with more meaningful relationships, we must mitigate mankind’s ability to wage war against himself. An unmanipulable, uninflatable, and confiscation-resistant free market monetary alternative like Bitcoin is a good start: it holds within it the promise of starving the state of the virtually unlimited resources the fiat currency printing press feeds into it. When people have a choice to opt out of the inflationary economic order, governments lose the ability to tax them (both explicitly and implicitly through inflation) which mitigates state revenue and its ability to wage war.

Warfare, its attendant loss of life, and the destruction of capital it causes are mitigatable outcomes of money market monopolies. As with the other negative consequences of monopolization – like food shortages, unemployment, price signal distortion, and exacerbated business cycles – war can be curtailed by open and free markets, which create incentives for cooperation and long-term relationship building. As an unstoppably free market, Bitcoin is rendering irrelevant the artifices which preserve monetary monopolies and returning the market for money to its naturally free state. It accomplishes this by virtue of its intrinsic truthfulness and transparency which are, interestingly, two of the key ingredients to Ray’s free market for ideas – the idea meritocracy. As you said Ray, “In my case, I wanted meaningful work and meaningful relationships, and I believed that being radically truthful and

radically transparent were required to get those”. A money that embodies these free market qualities is likely to influence its users to behave accordingly; this would create cultural effects diametrically opposed to those spawned by fiat currencies today. Simply, hard money like Bitcoin lowers societal time preferences; it encourages people to invest in themselves, seek meaningful work aligned with their skills, forge meaningful relationships, and to collaborate over longer time horizons. Critically, in a world run on Bitcoin, funding perpetual warfare via inflation would be a relic of mankind’s barbaric past — making Bitcoin the ultimate boon to the meaningfulness of relationships. But to get there, we must face reality head on and deal with it as it is, which brings to the here and now.

Facing Reality

(p.138) “Man’s most distinctive quality is our singular ability to look down on reality from a higher perspective and synthesize an understanding of it.”

Since 2008, central banks across the world have injected an unprecedented flow of fiat currency liquidity into the economic system. Expectantly, this has furthered wealth disparity and sewn new seeds of systemic risks. Although we remain in a historically long economic bull run, these hidden risks appear to be rousing from their dormancy. No matter what form the next crisis takes, central banks have only three options to try and mitigate its consequences: 1) cutting entitlement benefits, 2) raising taxes, and 3) printing money. All three of these options will hit those living on fixed-income — retirees, pensioners, and the working poor — the hardest. Of the three, printing money is historically most favored by central bankers as it can be done (and is being done) with little political fuss or muss.

These systemic risks are compounded by negatively yielding government bonds, which most retirees, who typically have lower risk appetites because of their age, depend on for fixed-income in their twilight years. Since these many of these instruments now suffer from negative yields, this forces investors with low risk appetites, including retirees and pension funds, to keep their nest-eggs “at risk” in equities markets, lower quality bonds, or even riskier assets. This contradicts the standard American dream in which you spend your younger years earning and investing in higher risk assets, like equities, so that as you neared retirement you could gradually transition your exposure to lower risk investments that generate a relatively predictably, consistent return — like bonds. This approach gives you exposure to higher upside when you are young and reduces downside exposure as you age, so that your nest-egg doesn’t get crushed in a stock market crash.

Bitcoin can help those living on fixed-income protect themselves from the accumulation of hidden risks created by the optionality-theft central banks impose on citizens. A small allocation of less than 5% gives those vulnerable to

economic contractions a kind of insurance policy – a put option on the idiocy inherent to a politically-charged, debt-based monetary system. Once again we find the wisdom of Taleb, as this is an expression of the barbell strategy: an approach to investing and other aspects of life in which assumes a large exposure to a low-risk, low-reward element and small exposure to a high-risk, high-reward element. In fact, a portfolio with 95% cash and 5% Bitcoin outperformed the S&P500 on risk and return every year over the past 6 years:

https://twitter.com/100trillionUSD/status/1136969637588021250?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E1136969637588021250&ref_url=https%3A%2F%2Fjameso.be%2F2019%2F08%2F24%2Fbitcoin-is-for-this.html

After decades of flooding the market with cheap money, central banks have distorted free market incentive systems and made economies dependent on this artificial liquidity to stay afloat. Even the indication of quantitative tightening sent markets tumbling in 2018, which was quickly reversed by The Fed's now infamous "dovish pivot" back to a more accommodative monetary policy. As this soft money is continually injected into the economy, it is flowing to hard assets so that investors can protect their wealth against the inevitable inflation quantitative easing creates, thus further distorting soft-money-denominated prices and setting the stage for new bubbles in markets like real estate and equities. At the core of this perpetual monetary easing is the (perhaps well-intentioned but certainly misguided) attempts of central banks to "create price stability" and "smooth out the business cycle" – which, intentionality aside, is equivalent to an arsonist racing to extinguish the fire he started. To state the argument again succinctly: printing money does not create stability of any kind, it distorts price signals and exacerbates the severity of economic cycles.

Further, it is printing of money that has created the deeply negative bond rates we are seeing in Europe. As the European central bank (ECB) keeps printing money, it must buy bonds to inject this cash into the economy, which drives up the price of bonds and depresses their yields. So, we get into this (familiar) fiat currency trap in which the attempts to keep the economy healthy by injecting artificial liquidity hurt the most vulnerable among us, those living on fixed-income, the most. Bitcoin fixes this: by taking monetary policy out of the hands of people, who are as incapable of "managing" a complex system like the economy as much as they are the weather, it eliminates the vector by which policymakers create these economic distortions that they then try to fight off using the same policy tools that created the problems in the first place. Since Bitcoin's supply is absolutely scarce, whatever portion you own of the total supply, you can be 100% certain that you will always have at least that fraction; this is the crucial discovery of absolute scarcity that Bitcoin represents, a one-time event that can never be recreated.

Another way soft money is distorting markets is through “share buybacks”, in which corporations take out cheap loans and use the proceeds to buy back their own shares. This action is an expression of the belief that the company’s stock will outperform the cost of capital net of inflation over the loan term. Also, the agency problem rears its head again here, as the reduction of shares outstanding helps corporate executives hit their “earnings per share” targets on which their bonus packages are based. This “financialization” of the real economy is a product of the flawed incentives inherent to fiat currency. Unsurprisingly, in the wake of the past 10 years of reckless money printing, corporate share buybacks have become the dominant source of demand for equities:

Corporate buybacks are dominant source of equity demand

Category	Net US equity demand (\$ billions)			
	2016	2017	2018	2019E
Corporations	\$ 697	\$ 296	\$ 509	\$ 600
Foreign Investors	(188)	125	(94)	25
Pension Funds	(217)	(162)	(243)	(100)
Mutual Funds	(112)	(134)	(124)	(175)
Households	(151)	226	191	50
Life Insurance	98	(45)	(18)	-
Other	(12)	(17)	9	-
<i>less</i>				
Foreign equities by US	22	167	128	350
Credit ETFs	96	123	100	50
Included among holders above are:				
Equity ETF purchases	\$ 188	\$ 347	\$ 210	\$ 300

A perverse configuration of dependencies arises as a result: low risk appetite investors have been driven out of “safe” investments like bonds because of their negative yields, thus pushing them further out along the risk curve into equities or worse. However, due to the soft money fueled share buybacks outlined above, the dominant source of demand for these equities are the corporations buying their own stock with artificially cheap money, making their share prices perversely dependent on the continued central bank provisioning of low interest rate loans. So now, in a twisted turn of fiat disease, entire retirement portfolios and pension funds have been forced into dependency on the continued accommodative monetary policy of central banks, which can only maintain their confiscation via inflation so long as the

underlying society remains sufficiently productive and submissive to its authority.

Facing reality, we see that the fiat currency experiment is in the endgame now. If interest rates aren't held down or if central banks stop injecting liquidity in steadily larger doses, the economy will crash cataclysmically. Even if they do, it is only a matter of time before society begins to come unglued, as it always does when its trust fabric, money, is sufficiently debased. So, the time is now to accept our reality, learn the lessons of history, and plan for a better future. Although it's probably clear by now, fiat currency is not a viable monetary system. In any case, let's "look down on the reality" of different monetary systems to glean some comparative insight as to their fundamental nature and what would best suit us from an organizing principle perspective. In a sense, each particular kind of money represents a liquid equity stake in its respective monetary system. Let's compare:

Fiat Currency: Liquid equity in a central bank, a privately owned and operated monetary monopoly

- Only Class B Shares available, All Class A Shares owned by Central Bank Shareholders
- No voting rights
- Board observation rights limited to public central banker appearances
- Converts greed into monetary dilution, confiscation via inflation, and trade wars
- Liquid equity subject to unlimited dilution
- Liquid equity subject to deauthorization
- Liquid equity subject to censorship
- Liquid equity subject to confiscation
- Liquid equity has no claim on underlying assets of monetary network (gold)

Gold: Semi-liquid equity in the world's original, physical, and free market money

- Class A Shares = Physical Gold, Class B Shares = Gold Certificates
- No voting
- Governed by nature, no board to observe (only for Class A)
- Converts greed into monetary value and unforgeable costliness

- Liquid equity subject to unlimited dilution, although historically this is low and predictable
- Liquid equity immune to deauthorization (only for Class A)
- Liquid equity immune to censorship (only for Class A)
- Liquid equity subject to confiscation
- Liquid equity is the underlying asset (gold, only for Class A)

Bitcoin: Liquid equity in the world's only global, digital, final settlement monetary network

- Class A Shares = Private Key, Class B Shares = Bitcoin Exchange IOUs
- Pro-rata voting rights, option to fork network to new ruleset
- 100% transparent ruleset, no board to observe
- Converts greed into monetary value, unforgeable costliness, and network security
- Liquid equity immune to dilution
- Liquid equity immune to censorship (only for Class A)
- Liquid equity resistant to confiscation (only for Class A)
- Liquid equity is the underlying asset (Bitcoin, only for Class A)

Ultimately, none of our individual opinions matter about this; it is up to the free market to decide. Fortunately, Bitcoin exists as a free market alternative upon which society can stand and clean up the mess central banks and governments have created for the world. Only time will tell how this all plays out. Remember: the escalating stock-to-flow ratio of Bitcoin is relentless. At this point, it is fiducially irresponsible to ignore this asset completely, and the pain of having no exposure to it will likely only worsen with time.

<https://twitter.com/Breedlove22/status/1155265716834062336?s=20>

With that, let me briefly summarize my arguments before closing:

Distorted price signals are the “nerve damage” inevitably suffered by an economic order based on central banking. As is true with all industrial monopolies, the profits for few are subsidized at the expense of many. Bitcoin fixes this by disintermediating the market for money and restoring its natural supply and demand dynamics. As Ray says, “An idea meritocracy requires people to do three things: 1) Put their honest thoughts on the table for everyone to see, 2) Have thoughtful disagreements where there are quality back-and-forths in which people evolve their thinking to come up with the

best collective answers possible, and 3) Abide by idea-meritocratic ways of getting past the remaining disagreements.” These three requirements of the idea meritocracy, closely reflected in free markets, can be summarized as honesty, quality competition, and conflict-resolution. Bitcoin satisfies all three: it is completely transparent (honesty), secured by a free market for mining (quality competition), and governed by a community-determined ruleset that is algorithmically enforced (conflict-resolution protocol). Bitcoin embodies idea-meritocratic elements, and is one of the only sources of truth in modernity. As Einstein said: “The significant problems of our time cannot be solved by the same level of thinking that created them.” In the same way that we needed the breakthrough of double-entry bookkeeping to catalyze capitalism, as it enabled us to synchronize our economic efforts further across spacetime, we now need the triple-entry accounting system intrinsic to Bitcoin to break the central bank monopoly and more greatly amplify the synchrony of mankind’s economic efforts into futurity.

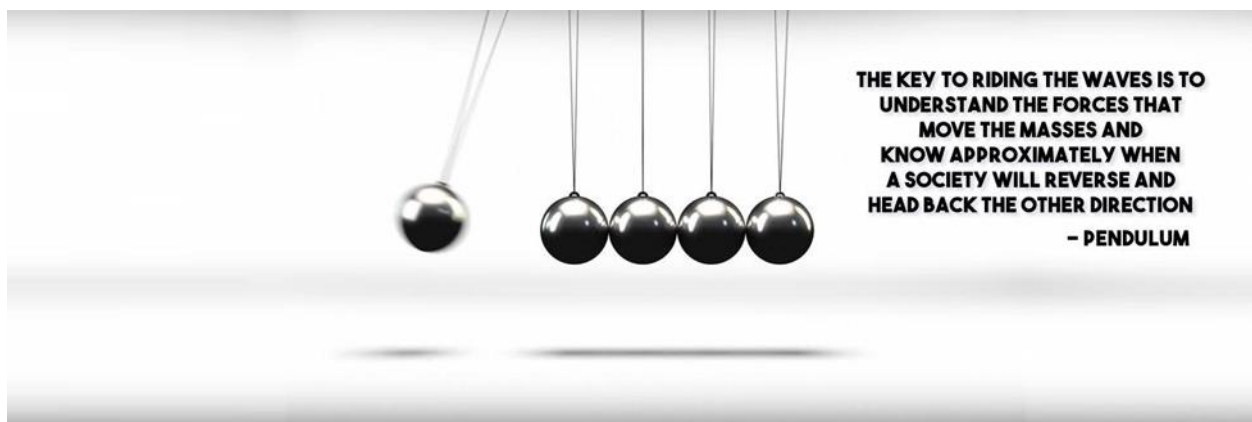
Bitcoin is an open-source protocol for exchanging value. Such openness ensures that Bitcoin’s code cannot be manipulated to benefit anyone at the expense of anyone else. The rules governing Bitcoin are founded in the (absolutely) uncompromising laws of mathematics — nature’s fundamental language. Bitcoin is the zero-marginal-cost-marketplace into which all available energy maybe sold; this means that every joule of energy which cannot find a more profitable employment flows into the “alchemization of digital gold” (the ultimate energy unemployment relief program, if you will). This realigns the race to the bottom associated with fiat currency, in which all monopolists are incentivized to devalue their currencies and secretly tax their people, to become a race to the bottom for the cheapest energy sources, thus spurring innovation in the realm of energy efficiency worldwide, forever. This perpetual bounty program for cheap energy becomes increasingly economically compelling as more monetary value accretes to Bitcoin, as more stranded joules become savable.

With central planning, any defectors from the single unitary plan become enemies of the state. This concentrates power in the hands of a progressively smaller few, which makes the intoxication of power more potent and attracts the most unscrupulous among us to seek its reigns. Bitcoin is the exit option, the plan B, for those enslaved by the prevailing monetary monopolies; it allows defectors a way out of the panopticon constructed by politicians and bankers by simply exercising their freedom of speech. It is a peaceful revolt against the institutionalized system of time-theft we call central banking. In the same way that Galileo’s new perspectives on the heavenly bodies shattered the political influence of the church over time, Bitcoin obliterates political control over money because it is the one-time discovery of absolute scarcity — a quintessential property of time that lives beyond the reach of man-made legal frameworks.

The idea meritocracy is the depoliticization of decision-making; Bitcoin is the depoliticization of money.

Bitcoin is an idea meritocracy and unstoppable free market for money, it is naturally outcompeting all monopoly-insulated monies by transcending the laws which protect them and forcing them into the competitive sphere in which only their merits matter. Bitcoin is a free-market-chosen-hard-money emancipating the monopoly-warrenred economic fiefdoms all over the world. Bitcoin is an idea meritocracy consisting of: radical truth (true consensus, immutable records, carrier of truthful price signals) + radical transparency (open-source, inflation-immune, transparent and reliable money supply) + believability weighted decision making (one hash equals one vote, skin in the game governance). In this way, it is a free market money that is subsuming all economies facilitated with fiat currencies (centrally planned monies) into itself. Bitcoin is unregulatable, unstoppable, perfectly transparent implementation of energy-based, absolutely scarce, hard money devouring all softer forms and infusing the value stored therein into itself, once and for all. Bitcoin is hard money bending monetary history back towards its free market point of origin.

In the grand arc of human history, Bitcoin represents a reversion to a free-market-chosen hard money system. Ray, Bitcoin is the paradigm shift you've seen coming; once again, nature's pendulum is changing directions:



As Alexander the Great once said:

"Through every generation of the human race there has been a constant war, a war with fear. Those who have the courage to conquer it are made free and those who are conquered by it are made to suffer until they have the courage to defeat it, or death takes them."

Courage can only exist in the face of fear. If you listen closely, you may hear the devil whispering "You can't withstand the storm." And if you listen closely to your heart, to the warrior within, you will hear him respond, "I am the storm."

The Coming Storm

In the 19th century essay by Georgi V. Plekhanov titled *The Role of the Individual in History*, a strong case is made for the inevitability of the path which charts itself as an expression of the unpredictably free action of people. As a process, human history expresses laws (principles) by which to orient its constituents. As an actualization, human history is made by those who set and solve the problems of progress in accordance with the conditions of their respective epoch, regardless of its laws. In this sense, a great man is great because “he possesses qualities which make him most capable of serving the great social needs of his time”, and will carry out his sacred duties lawlessly whenever necessary.

Restoration of individual sovereignty is the chief aim of separating money and state. Free markets are idea meritocracies; minimized barriers to the interplay, recombination, and reproduction of knowledge are the defining characteristics of both. And knowledge growth is the key driver of innovation, evolution, and economic growth. Bitcoin is both a free market money and a free market in and unto itself, with entrepreneurs freely entering and exiting its mining network. Consistent with Ray’s definition of an idea meritocracy, Bitcoin is radical truth and radical transparency in action, governed with skin in the game. As the central pillar of every economy, it is critical that the market for money remain free and unobstructed by monopolists, else we witness the continued cartelization of those industries closest to its economic influence. Bitcoin is free market money born out of societal necessity; the absolutely inelastic fabric of trust necessary to save mankind from his own self-destructive greed.

Paradoxically, it is only when people are free to act on their own accord that they become conscious of economic necessity by virtue of having their own skin in the game. Those who are coerced by regulations or insulated from the consequences of their actions by government monopolies, guarantees, or other obstructions suffer from a disconnect with reality and atrophy over time. In this sense, freedom is the conscious awareness of necessity; acceptance of the opportunity costs to be incurred in action, awareness of the obstructions to be overcome, and understanding of natural laws. Value is the bridge between the conscious awareness of life’s necessities and the freedom to choose; it is expressed in price: the intersection of (objective) supply with (intersubjective) demand. Without an objective touchstone for the value of things (hard money), market signals are distorted and capital allocations are manipulated, causing societies to trend towards centralized power concentrations (bigger government), nationalization of assets (less free enterprise), and marginalization of citizenries (inflation, taxation, and conscription). Entrepreneurs are elemental to free markets and antithetical to state control. Leaving each person free to pursue profits by whatever (nonviolent) means necessary ensures that markets generate the lowest prices, highest satisfactions of wants, and continuous streams of innovations for all to enjoy.

Freedom allows people to self-actualize the actions they themselves deem necessary as they face the inherent scarcities of existence. Freedom, in a profound sense, is necessity transformed into action. A profound definition like this is fractal, in that it does not refute its superficial form, but is instead inclusive of it. Once an individual overcomes the restrictions imposed both within and without himself, he is born again; his “free actions become the conscious and free expression of necessity.” By transcending the government coercion of money production, Bitcoin facilitates a reversion to man’s natural, sovereign state of being; an existence with more freedom of expression and less oppression. By incinerating the opacity of central banking with the light of pure transparency, drowning the lies inherent to fiat currency in a ceaseless flow of indisputable truth (a new block roughly every 10 minutes), and like the free people whose sovereignty it is reinvigorating, Bitcoin is swelling into a great social force that is:

“Bursting on cunning falsehood

Like a storm of wrath divine...”

Bitcoin is the first social institution in history with the potential to subvert the greatest man-made scourge humanity has ever faced – the infamous wealth-extracting, disparity-driving, and warfare-financing duopoly of monopolists: governments and central banks.

Thank you for reading “An Open Letter to Ray Dalio re: Bitcoin”

Follow me on Twitter: [Robert Breedlove](#)

My sincerest gratitude to these amazing minds:

[@real_vijay](#), [Saifedean Ammous](#), [Brandon Quittem](#), [Dan Held](#), [Naval Ravikant](#), [@NickSzabo4](#), [Nic Carter](#), [@MartyBent](#), [Pierre Rochard](#), [Anthony Pompliano](#), [Chris Burniske](#), [@MarkYusko](#), [@CaitlinLong_](#), [Nik Bhatia](#), [Nassim Nicholas Taleb](#), [Stephan Livera](#), [Peter McCormack](#), [Gigi](#), [Hasu](#), [@MustStopMurad](#), [Misir Mahmudov](#), [Mises Institute](#), [John Vallis](#), [@FriarHass](#), [Conner Brown](#), [Ben Prentice](#), [Aleksandar Svetski](#), [Cryptoconomy](#), [Citizen Bitcoin](#), [Keyvan Davani](#), [@RaoulGMI](#), [@DTAPCAP](#), [Parker Lewis](#), [@Rhythmtrader](#), [Russell Okung](#), [@sthenc](#), [Nathaniel Whittemore](#), [@ck_SNARKs](#), [Trevor Noren](#), [Cory Klippsten](#), [Knut Svanholm](#)

Special thanks to the man himself: [Ray Dalio](#)

And anyone else I forgot :)

Sources

- a. <https://www.amazon.com/Principles-Life-Work-Ray-Dalio/dp/1501124021>
- i. Where you see page numbers marked (p.##) throughout this essay, they are referencing Ray's book, Principles
- b. <https://twitter.com/LukeGromen/status/1100068098189733888/photo/1>
- c. <http://www.bbc.com/future/story/20190218-are-we-on-the-road-to-civilisation-collapse>
- d. <https://www.linkedin.com/pulse/populism-weakening-economy-limited-central-bank-power-ray-dalio/>
- e. <https://www.businessinsider.com.au/the-worst-gold-chart-of-all-time-2013-4>
- f. <https://inthelongrun.co.uk/tag/treasury-bonds/>
- g. <https://etfdailynews.com/2015/02/25/100-reasons-why-the-federal-reserve-should-be-shut-down/>
- h. <https://medium.com/@RobertNYC/monetary-madness-438836c44464>
- i. <https://fred.stlouisfed.org/series/M1>
- j. <https://history.stackexchange.com/questions/7887/did-rothschild-say-this-famous-quote-if-yes-what-did-he-mean-by-it>
- k. <https://www.dropbox.com/s/iwtk4rhcx3tvnud/Kenetic%20CCC%20Master%20Deck.pdf?dl=0>
- l. <https://wisdomsummary.com/the-wittgensteins-ruler/>
- m. <https://www.monticello.org/site/research-and-collections/private-banks-spurious-quotation>
- n. <https://wthappenedin1971.com/>
- o. <https://medium.com/@100trillionUSD/modeling-bitcoins-value-with-scarcity-91fa0fc03e25>
- p. <https://medium.com/@jimmysong/bitcoin-and-virtue-part-1-prudence-78a7dfad0b33>
- q. https://www.brainyquote.com/quotes/milton_friedman_382646
- r. <https://twitter.com/ArryinSeattle/status/1168294075180580864/photo/1>
- s. <https://mises.org/library/how-central-banks-fund-our-age-endless-war>
- t. <https://fas.org/sgp/crs/natsec/R44116.pdf>

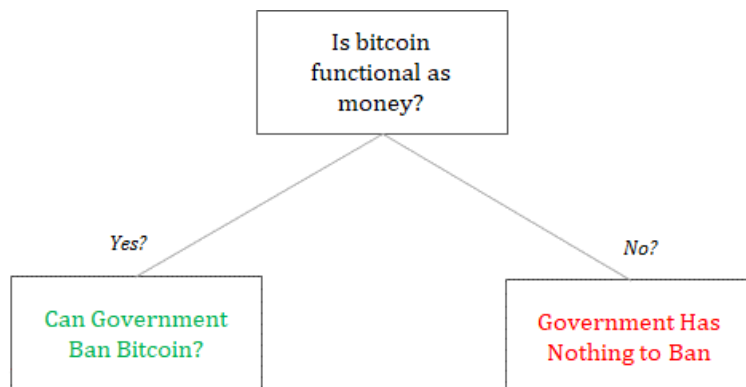
- u. <https://medium.com/incerto/what-do-i-mean-by-skin-in-the-game-my-own-version-cc858dc73260>
 - v. <https://janicekobelsky.mykajabi.com/blog/the-best-way-to-earn-trust-stand-under-your-own-arches>
 - w. <https://twitter.com/Breedlove22/status/1192291536379056128>
 - x. <https://www.amazon.com/Crazy-Cock-Henry-Miller/dp/0802132936>
 - y. <https://www.amazon.com/Complete-Essays-Montaigne-Michel/dp/0804704864>
 - z. <https://medium.com/coinshares/beware-of-lazy-research-c828c900b7d5>
 - aa. https://twitter.com/crypto_voices/status/1157639340870311936
 - bb. <https://cdn.mises.org/Road%20to%20serfdom.pdf>
 - cc. <https://jameso.be/2019/08/24/bitcoin-is-for-this.html>
 - dd. <https://www.amazon.com/Bitcoin-Sovereignty-mathematics-Knut-Svanholm/dp/1090109911>
-

Bitcoin Cannot be Banned

By **Parker Lewis**

Posted November 8, 2019

The idea that somehow bitcoin can be banned by governments is the final stage of grief, right before acceptance. The consequence of the statement is an admission that bitcoin “works.” In fact, it posits that bitcoin works so well that it will threaten the incumbent government-run monopolies on money in which case governments will regulate it out of existence to eliminate the threat. Think about the claim that governments will ban bitcoin as conditional logic. Is bitcoin functional as money? If not, governments have nothing to ban. If yes, then governments will attempt to ban bitcoin. So the anchor point for this line of criticism assumes that bitcoin is functional as money. And then, the question becomes whether or not government intervention could successfully cause an otherwise functioning bitcoin to fail.



As a starting point, anyone trying to understand how, why, or if bitcoin works should assess the question entirely independent from the implications of government regulation or intervention. While bitcoin will undoubtedly have to

co-exist alongside various regulatory regimes, imagine governments did not exist. On a standalone basis, would bitcoin be functional as money, if left to the free market? This will inevitably lead to a number of rabbit hole questions. What is money? What are the properties that make a particular medium a better or worse form of money? Does bitcoin share those properties? Is bitcoin a better form of money based on its properties? If the ultimate conclusion becomes that bitcoin is not functional as money, the implications of government intervention are irrelevant. However, if bitcoin is functional as money, the question then becomes relevant to the debate, and anyone considering the question would need that prior context as a baseline to evaluate whether or not it would be possible.

By design, bitcoin exists beyond governments. But bitcoin is not just beyond the control of governments, it functions without the coordination of any central third parties. It is global and decentralized. Anyone can access bitcoin

on a permissionless basis and the more widespread it becomes, the more difficult it becomes to censor the network. The architecture of bitcoin is practically purpose-built to resist and immunize any attempts by governments to ban it. This is not to say that governments all over the world will not attempt to regulate, tax or even ban its use. There will certainly be a fight to resist bitcoin adoption. The Fed and the Treasury (and their global counterparts) are not just going to lay down as bitcoin increasingly threatens the monopolies of government money. However, before debunking the idea that governments could outright ban bitcoin, first understand the very consequence of the statement and the messenger.

The Progression of Denial & Stages of Grief

The skeptic's narrative consistently shifts over time. Stage one of grief: bitcoin could never work – it is backed by nothing. It is nothing more than a present-day tulip mania. With each hype cycle, the value of bitcoin rises dramatically and is then followed by a correction. Often extolled as a crash by skeptics, bitcoin fails to die and in each instance, it finds support at levels higher than prior adoption waves. The tulip narrative becomes tired and the skeptics move on to more nuanced issues, re-anchoring the debate. Stage two of grief follows: bitcoin is flawed as a currency. It is too volatile to be money, or it is too slow to be a payments system, or it cannot scale to satisfy all the payments in the world, or it wastes energy. The list goes on. This second step is a progression of denial and it is a significant departure from the idea that bitcoin is nothing more than nothingness.

Despite the supposed flaws, the value of the bitcoin network continues to rise over time. Each time it does not die, it gains strength. While the skeptics are busy pointing out flaws, bitcoin never sleeps. An increase in value is driven by a very simple market dynamic: more buyers than sellers. That is all and it is a function of increasing adoption. More and more people figure out why there is fundamental demand for bitcoin and why/how it works. This is what creates long-term demand for bitcoin. As more people increasingly demand it as a store of wealth, there is no supply response. There will only ever be 21 million bitcoin. No matter how many people demand bitcoin, the supply side is completely fixed and inelastic. As the skeptics continue to shout the same tired lines, the crowd continues to parse the noise and demand bitcoin due to the strengths of its monetary properties. And no constituency is more well-versed in the arguments against bitcoin than adopters of bitcoin themselves.



Bitcoin FUD (Fear, Uncertainty & Doubt) Dice v1 and v2, courtesy of Nic Carter.

Desperation begins to kick in, and the debate re-anchors once again. The narrative predictably shifts. It is no longer that bitcoin is not backed by anything, nor that it is flawed as a currency; instead, the debate centers on regulation and government authorities. In the final stage of grief, it is actually that bitcoin works too well, and as a consequence, the government will never let it happen and ban it. Really? So human ingenuity somehow re-invents money in a technologically superior medium, the consequences of which are mind-bending, and the government is somehow going to ban that? Recognize that in claiming as much, the skeptics are admitting defeat. It is the dying whimper in a series of failed arguments. The skeptics simultaneously accept that there is fundamental demand for bitcoin and then pivot to the unfounded belief that governments can ban it.

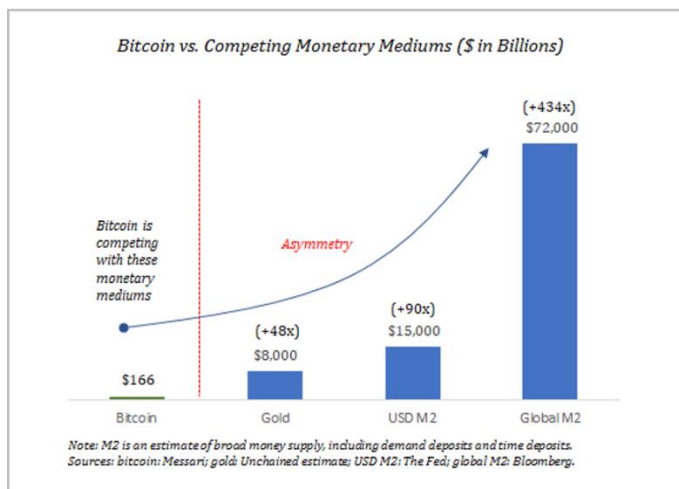
Play this one out. When exactly would developed world governments actually step in and attempt to ban bitcoin? Today, the Fed and the Treasury do not view bitcoin as a serious threat to dollar supremacy. In their collective mind, bitcoin is a cute little toy and is not functional as a currency. Presently, the bitcoin network represents a total purchasing power of less than \$200 billion. Gold on the other hand has a purchasing power of approximately \$8 trillion (40x the size of bitcoin) and broad money supply of dollars (M2) is approximately \$15 trillion (75x the size of bitcoin). When does the Fed or Treasury start seriously considering bitcoin a credible threat? Is it when bitcoin collectively represents \$1 trillion of purchasing power? \$2 trillion or \$3 trillion? Pick your level, but the implication is that bitcoin will be far more valuable, and held by far more people globally, before government powers that be view it as a credible competitor or threat.

President Trump & Treasury Secretary Mnuchin on Bitcoin (2019)

"I won't be talking about Bitcoin in 10 years, I can assure you that [...] I would bet even in 5 or 6 years I'm no longer talking about Bitcoin as Treasury Secretary. I'll have other priorities [...] I can assure you I will personally not be loaded up on Bitcoin." – Treasury Secretary Steve Mnuchin

"I am not a fan of Bitcoin [...], which [is] not money, and whose value is highly volatile and based on thin air." – President Donald J. Trump.

So the skeptic logic follows: bitcoin does not work, but if it does work, the government will ban it. But, governments in the *free* world will not attempt to ban bitcoin until it becomes more apparent that it is a threat. At which time, bitcoin will be more valuable and undoubtedly harder to ban, as it will be held by far more people in far more places. So, ignore fundamentals and the asymmetry inherent in a global monetization event because in the event you turn out to be right, the government will step in to regulate bitcoin out of existence. Which side of the fence would a rational economic actor rather be on? Owning a monetary asset that has increased in value so dramatically that it threatens the global reserve currency, or the opposite – not owning that asset? Assuming an individual possesses the knowledge to understand why it is a fundamental possibility (and increasingly a probability), which is the more defensible and logical position? The asymmetry alone dictates the former and any fundamental understanding of the demand for bitcoin only reinforces the same position.



But Bitcoin Cannot Be Banned.

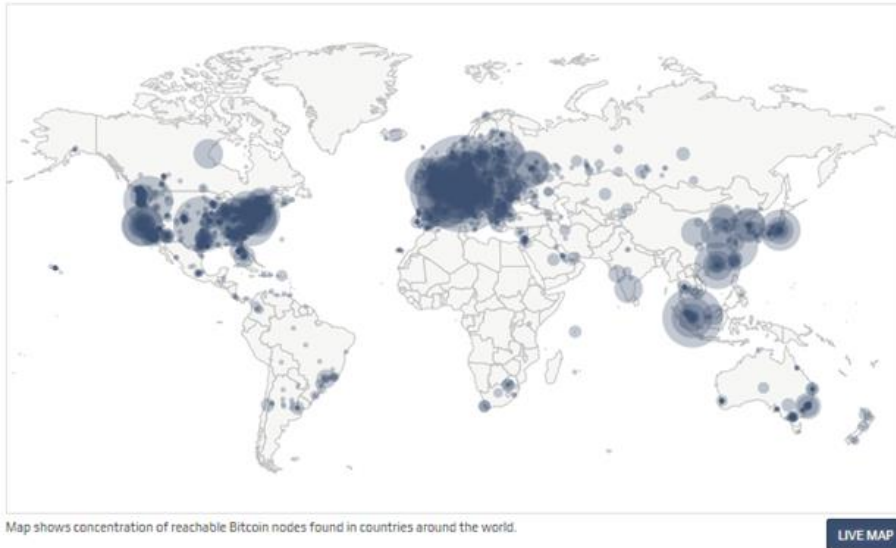
Think about what bitcoin actually represents and then what a ban of bitcoin would represent. Bitcoin represents the conversion of subjective value, created and exchanged in the real world, for digital keys. Said more plainly, it is the conversion of an individual's time into money. When someone demands

bitcoin, they are at the same time forgoing demand for some other good, whether it be a dollar, a house, a car, or food, etc. Bitcoin represents monetary savings that comes with the opportunity cost of other goods and services. Banning bitcoin would be an affront to the most basic freedoms it is designed to both provide and preserve. Imagine the response by all those that have adopted bitcoin: "Well that was fun, the tool that the experts said would never work, now works too well, and the same experts and authorities say we can't use it. Everyone go home. Show's over folks." To believe that all the people in the world that have adopted bitcoin for the financial freedom and sovereignty it provides would suddenly lay down and accept the ultimate infringement of that freedom is not rational.

"Money is one of the greatest instruments of freedom ever invented by man. It is money which in existing society opens an astounding range of choice to the poor man - a range greater than that which not many generations ago was open to the wealthy.." - F.A. Hayek

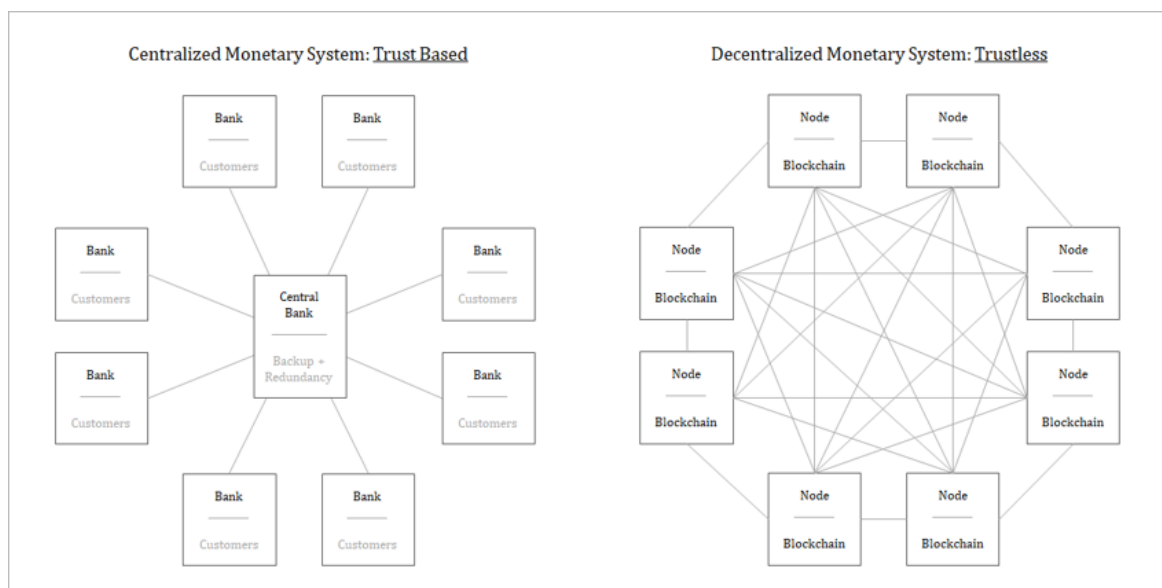
Governments could not successfully ban the consumption of alcohol, the use of drugs, the purchase of firearms, or the ownership of gold. A government can marginally restrict access, or even make possession illegal, but it cannot make something of value demanded by a broad and disparate group of people magically go away. When the U.S. made the private ownership of gold illegal in 1933, gold did not lose its value or disappear as a monetary medium. It actually increased in value relative to the dollar, and just thirty years later, the ban was lifted. Not only does bitcoin provide a greater value proposition relative to any other good that any government has ever attempted to ban (including gold); but by its nature, it is also far harder to ban. Bitcoin is global and decentralized. It is without borders and it is secured by nodes and cryptographic keys. The act of banning bitcoin would require preventing open source software code from being run and preventing digital signatures (created by cryptographic keys) from being broadcast on the internet. And it would have to be coordinated across numerous jurisdictions, except there is no way to know where the keys actually reside or to prevent more nodes from popping up in different jurisdictions. Setting aside the constitutional issues, it would be technically infeasible to enforce a ban of bitcoin in any meaningful way.

Bitcoin Node Concentration by Country (earn.com)



Even if all countries in the G-20 coordinated to ban bitcoin in unison, it would not kill bitcoin. Instead, it would be the fait accompli for the fiat system. It would reinforce to the masses that bitcoin is a formidable currency, and it would set off a global and hopeless game of whack-a-mole. There is no

central point of failure in bitcoin; bitcoin miners, nodes and keys are distributed throughout the world. Every aspect of bitcoin is decentralized, which is why running nodes and controlling keys is core to bitcoin. The more keys and the more nodes that exist, the more decentralized bitcoin becomes, and the more immune bitcoin is to attack. The more jurisdictions in which mining exists, the less risk any single jurisdiction represents to bitcoin's security function. A coordinated state level attack would only serve to build the strength of bitcoin's immune system. It would ultimately accelerate the shift away from the legacy financial system (and legacy currencies), and it would accelerate innovation within the bitcoin economic system. With each passing threat, bitcoin innovates to immunize the threat. A coordinated state level attack would be no different.



Permissionless innovation on a globally decentralized basis is the reason bitcoin gains strength from every attack. It is the attack vector itself which causes bitcoin to innovate. It is Adam Smith's invisible hand on steroids. Individual actors may believe themselves to be motivated by a greater cause, but in reality, the utility embedded in bitcoin creates a sufficiently powerful incentive structure to ensure its survival. The self-interests of millions, if not billions, of uncoordinated individuals aligned by their individual and collective need for money incentivizes permissionless innovation on top of bitcoin. Today, it may seem like a cool new technology or a nice-to-have portfolio investment, but even if most people do not yet recognize it, bitcoin is a necessity. It is a necessity because money is a necessity, and legacy currencies are fundamentally broken. Two months ago, the repo markets in the U.S. broke, and the Fed quickly responded by increasing the supply of dollars by \$250 billion, with more to come. It is precisely why bitcoin is a necessity, not a luxury. When an innovation happens to be a basic necessity to the functioning of an economy, there is no government force that could ever hope to stop its proliferation. Money is a very basic necessity, and bitcoin represents a step-function change innovation in the global competition for money.

And more practically, any attempt to ban bitcoin or heavily regulate its use by any jurisdiction would directly benefit a competing jurisdiction. The incentive to defect from any coordinated effort to ban bitcoin would be far too high to sustain such an agreement across jurisdictions. If the United States made the possession of bitcoin illegal tomorrow, would it slow down proliferation, development and adoption of bitcoin and would it cause the value of the network to decline intermittently? Probably. Would it kill bitcoin? No. Bitcoin represents the most mobile capital in the world. Countries and jurisdictions that create regulatory certainty and place the least amount of restrictions on the use of bitcoin will benefit significantly from capital inflows.

Banning Bitcoin Prisoner's Dilemma

	Country B Bans Bitcoin (cooperates)	Country B Accepts Bitcoin (defects)
Country A Bans Bitcoin (cooperates)	<u>Bitcoin wins</u> Ban fails, bitcoin adoption accelerates Fiat currencies deteriorate more rapidly	<u>Bitcoin wins</u> Capital outflows from Country A Capital inflows to Country B
Country A Accepts Bitcoin (defects)	<u>Bitcoin wins</u> Capital outflows from Country B Capital inflows to Country A	<u>Bitcoin wins</u> Everyone wins Benefits from trade & specialization

In practice, the prisoner's dilemma is not one-to-one. It is multi-dimensional involving numerous jurisdictions, all with competing interests, making any attempts to successfully ban bitcoin that much

more impractical. Human capital, physical capital and monetary capital will flow to the countries and jurisdictions with the least restrictive regulations on bitcoin. It may not happen overnight, but attempting to ban bitcoin is the equivalent of a country cutting off its nose to spite its face. It doesn't mean that countries will not try. India has already tried to ban bitcoin. China has attempted to heavily restrict its use. Others will follow. But each time a country takes an action to restrict the use of bitcoin, it actually has the unintended effect of promoting bitcoin adoption. Attempts to ban bitcoin are an extremely effective marketing tool for bitcoin. Bitcoin exists as a non-sovereign, censorship-resistant form of money. It is designed to exist beyond the state. Attempts to ban bitcoin merely serve to reinforce bitcoin's reason for existence and ultimately, its value proposition.

The only winning move is to play

Banning bitcoin is a fool's errand. Some will try; all will fail. And the very attempts to ban bitcoin will accelerate its adoption and proliferation. It will be the hundred mile-per-hour wind that fuels the wildfire. It will also make bitcoin stronger and more reliable, further immunizing it from attack and reinforcing its antifragile nature. And in any case, believing governments will ban bitcoin, if it becomes a credible threat to global reserve currencies, is an irrational reason to discount it as a savings technology. It both cedes that bitcoin is viable as money, while at the same time ignoring the principal reasons as to why: decentralization and censorship-resistance. Imagine understanding the greatest present secret in the world and not capitalizing on the asymmetry and utility that bitcoin provides in fear of government. More likely, either someone understands why bitcoin works and that it will not fail at the hands of a government, or a knowledge gap exists as to how bitcoin is able to function in the first place. Begin by understanding the fundamentals, and then apply that as a baseline to assess any potential risk posed by future government intervention or regulation. And never discount the value of asymmetry; the only winning move is to play.

Next edition: Bitcoin is Not for Criminals (...it's for everyone)

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

To subscribe to weekly releases of *Gradually, Then Suddenly*, please click [here](#).

How I explain Bitcoin to normies...

By **Willy Woo**

Posted November 17, 2019

How I explain Bitcoin to normies...

Bitcoin is the first invention of something on the Internet that cannot be copied. When something is scarce, it can store value, fine art and gold are some examples.

Here's some buckets that people store value in:

Gold: \$8T Stocks: \$75T Fiat: \$90T Real Estate: \$220T

And now, we can store value online...

Bitcoin: \$150B

We are in a post-industrial Internet age.

Bitcoin is growing from being a thimble to a bucket.

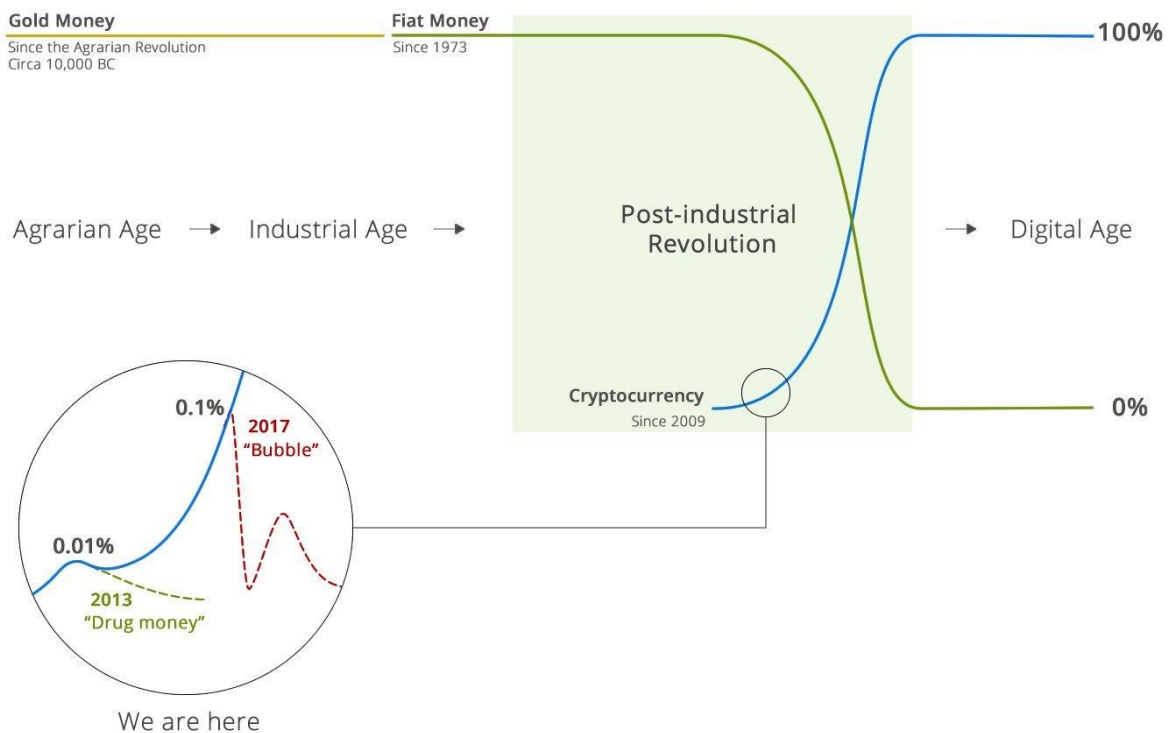
Let's look at how quickly it has grown in its 10 years.

It's on track to exceed M1 USD in the next 5 years... That's to say all the money in cash, credit card and cheque accounts, of the world reserve currency.



What's happening, as we move from the Industrial Age to the Digital Age, is money itself is becoming digitally native and programmable.

Here's the 10,000 year view.



@woonomic

As the Bitcoin asset class inflates with value, it has outperformed every other asset class for its entire 10 year history.

Under the lens of ROI adjusted for risk, it's as performant today as it was in 2009, you haven't missed the boat.

Bitcoin Risk Adjusted Returns vs Other Assets

source: charts.woobull.com



After that, they'll usually ask about buying some Bitcoin.

I think my hit rate is +90%.

You may at this point warn them to avoid fake Bitcoins until they know exactly what they are, i.e. BCH and BSV. I say this in case they start going to bitcoin dot com by mistake.

I usually send them somewhere depending on their country.

Next year I'll recommend LVL when they do integrated banking and crypto accounts.

(Disclosure: I'm an LVL seed investor and yes that's a reflink)

Then I recommend Exodus Wallet as it's super intuitive and its best kept secret is amazing tech support (replies in under 15mins).

(Disclosure: I'm a seed investor in Exodus too, amazing product.)

/ fini

Footnotes:

1) I do not go into technical underpinnings, when I buy a phone I don't need to know how an ARM chip works.

2) I do not go into the ethos of decentralisation, uncensorable, unconfiscatable money. People will rabbit hole after they have skin in the game

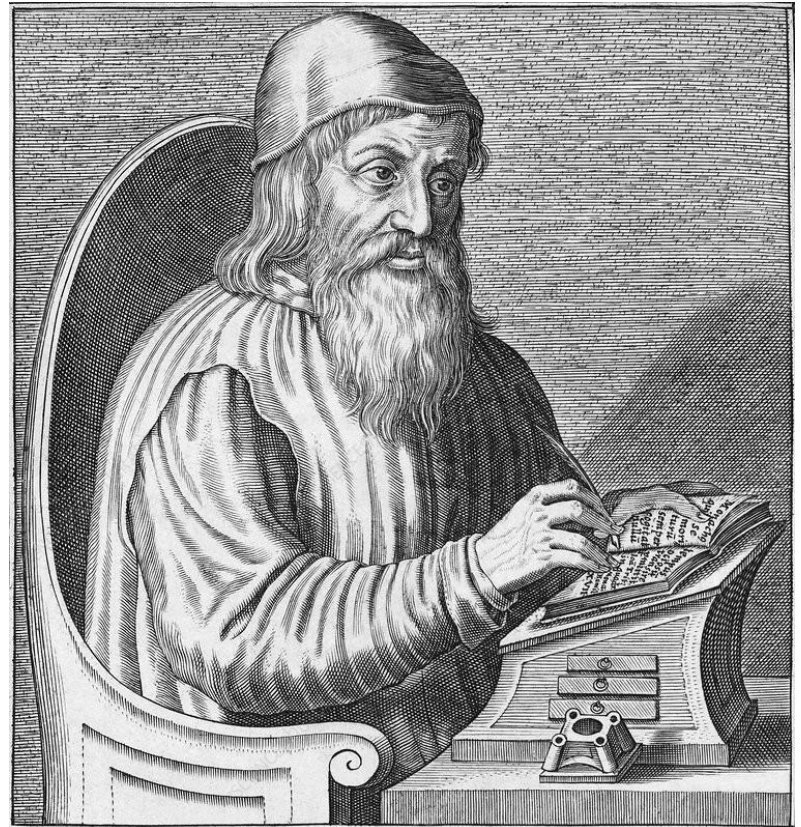
Johannes Trithemius, Archmage of Secrets

By **David Morris**

Posted November 6, 2019

In approximately 1499, in early Renaissance Frankfurt, a wunderkind bishop and magician named Johannes Trithemius completed work on a trilogy of books known as the *Steganographia*.

The first two volumes were remarkable enough: they appeared at first to be concerned with magic, particularly techniques for using spirits to communicate over long distances. These books were not commercially published until 1606, but quickly after they became widely available, it was discovered that they were in fact written in code. The mystical 'cover' content was simply a ruse: the books were guides to the practice of 'secret writing' — or, in Latin, 'crypto-graphia.'



They were among the first books ever published on the subject of code, and proved wildly popular — both in underground circulation during Trithemius' lifetime, and in their later, wider release. Trithemius' work on code likely had real-world impact, with use of the work specifically mentioned in histories involving secret government communication in the 17th century ¹.

But the third book of the *Steganographia* was something different: even after being decoded, it appeared to be about matters of magic. It contains an inscrutable array of numerical tables and charts correlated to the names of angels (Geradiel, Uriel, etc.), purportedly all part of the method of calling on the power of these beings. Reputedly, Trithemius also destroyed portions of the work containing instructions for prophecy — though this was likely a bit of myth-making.

Incredibly, it wasn't until nearly half a *millenia* after Trithemius penned this third volume that its true meaning was discovered. Two researchers discovered the truth, independently and nearly simultaneously – first a professor of German in 1996, and then an AT&T mathematician in 1998. What looked like coded descriptions of magical rituals were in fact instructions for secret communication² – a code within a code.

Where Trithemius discussed using the power of spirits to communicate without words, he seems to have been winkingly referring to the power of numerical code to carry meaning. This is striking given that Trithemius' work, taken at face value as a magical text, went on to be mined for centuries by would-be magicians hungry for methods to summon demons. It may also explain why Trithemius was not more aggressively condemned by the Church for his work during his lifetime – we can imagine him carefully explaining to ecclesiastical authorities that the *Steganographia* was not exactly as it seemed.

Secret writing as a practice, codified in a way theoretically accessible to a wide swathe of learned society, was itself a radical innovation in Trithemius' time, and likely viewed with extreme concern by established authorities. And in fact, coded language became, in the latter half of the second millennium, a crucial element of statecraft and spycraft, intrigues and revolutions. The same force continues into the present day in the form of encrypted internet communication, making Johannes Trithemius, in quite a direct sense, the first cypherpunk.

But I'm concerned with a stranger connection within Trithemius' project: What are we to make of his subversive act of obfuscation between code and magic? The *Steganographia* mined an existing conjunction between coded language and magic incantations: both a form of mystification, of obscuring. The word 'occult,' as Eugene Thacker and Mark Fisher have emphasized, takes its root from the Latin for secret or concealment. Magic deals in the occulted world – the planes of being beyond what humans can experience. Coded language created a new space for shared secrets, allowing a kind of 'occulting' of the social world³.

Magic is always a sort of symbolic obfuscation. Magical symbols are imbued with resonance and power through the process of what we would call memetics. By spreading through the minds of beings primed to believe in them, vague magical symbols can gain an eerie physicality: just as Trithemius metaphorized coded language as magical spirit-talking, the power of shared symbols can be described in supernatural terms as telepathy, curse, or mind control.

The fact that magical symbols are vague and indirect is precisely what can give them real-world power, when wielded by certain hands. For the well-

intentioned magician, perhaps a poet or shaman, the vagueness of magical symbol can become a pathway to insights that are not easily articulated in precise, rational terms. But in the wrong hands, for instance those of a political demagogue, magical language, chants and symbols can organize impulses too dark for the human spirit to accept when stated outright.

In this very real way, the practice of magic harnesses the misty realm of things like consciousness, reflection, and intention, connecting them to indeterminate symbols that can nonetheless push through into the hard-edged world of action and impact. Magic becomes an alternate frame for viewing a wide spectrum of social incantations — the Pledge of Allegiance is a ritual of binding, each paycheck an indulgence, the iPhone a saintly fetish, whispering hallucinations. Magic is threaded throughout our obsessive, repetitive world.

Coded language is in a sense the inverse. Its essence is actionable, meaningful data or expression. The series of mathematical transformations enacted on that data — the ritual, if you will — replaces legible content with seemingly random signals. It renders the message unintelligible except as a message. Like McLuhan's light bulb, code is itself nothing, yet refigures a base dimension of (social) reality. Where once we were in darkness, Edison brought light. And conversely, where once we had only words with meaning, Trithemius brought the world secret messages, pings, blips — visible but unknowable information.

Trithemius had to be a visionary to grasp the worth of coded communication. But we take it for granted, encountering coded messages daily without truly seeing them: scanning systems, identification cards, and, of course, computers. There are reasons both of real secrecy and mere efficiency behind the use of codes for communication between organizations or agencies or governments. But for whatever reason, the sort of code pioneered by Trithemius has become a major tool for ordering, regulating, and managing our societies and our world.

Our existence within a coded reality — our daily encounter with the UPC code on the goddamn cereal box — can be regarded as the postmodern corollary to the mysteries of nature confronted by our long-ago ancestors. Once it was the outside world that constantly hid its deeper principles from us. Now our fellow humans do the same.

And just as the mysteries of nature gave birth to attempted explanations in the form of myth, folklore, and religion, the mystery of code primes our being to quest into darker levels of social (un)meaning. If everything is code, where beyond or below the apparent everyday are the lines of communication and levers of power that guide both the agreements of the powerful, and the resistance of the weak? Could these messages be all around us, yet evade our notice?

Among other things, then, code becomes a way for humans to revive a sense of the mystical. Its practice and, perhaps more importantly, its cultural resonance, have allowed our highly advanced and regimented society to retain something of its wildness. We are animals, and ultimately, we demand freedom and possibility. We demand, even, risk and chaos.

... This is the first part of one chapter of my new book, Bitcoin is Magic. I'll be publishing the rest of the chapter soon ... or you can just grab the book, in paperback or for Kindle, today.

-David Morris

1 Robert Hooke (1705). The Posthumous Works of Robert Hooke. Richard Waller, London

2 This is according to AT&T's Dr. Jim Reeds, one of two researchers independently broke Trithemius' code.

3 If Trithemius was just posing as a 'magician' while in fact remaining faithful to his Catholicism, he is also a useful figure for definition of 'magic' in contemporary politics and ideology. We have mentioned the formulation, drawn from Aleister Crowley and carried on by Alan Moore, that magic is an attempt at direct, individual intervention in the world. For Moore, religion is in particularly stark contrast to this, as a form of submission to authoritarianism — but there is a converse formulation, by which religion is a vehicle not for submission, but for *faith*. Faith is a spiritual submission to being itself as a mystery beyond any mere human grasping, and implies an ultimate rejection of ANY human authority in the face of the numinous, mystical all-power of God.

“The Sovereign Individual” Investment Thesis

By Phil Bonello

Posted November 12, 2019

Globalization, Digital Money, & Dissident Technology

Information technology alters global power dynamics in a few key ways:

Instant information dissemination reduces commercial and jurisdictional barriers to entry *and* barriers to exit. This increases competition by facilitating global entrepreneurship.

The creation of non-sovereign, digital money decreases the power of inflation and taxation. Financial services can also more easily address the global market.

Encryption reduces the cost of protection and decreases the leverage of violence at scale. This leads to the rise of dissident technology.

Each of these categories represents a huge shift in society. They present massive opportunities. This post is an introduction into each of these changes and examines the source of user demand through the lens of the following human motivations:

Acquire (greed) – Desire to collect physical objects as well as immaterial ones like power, status, and influence

Defend (fear) – Desire to protect ourselves and our property

Bond (belonging) – Desire to form relationships

Learn (curiosity) – Desire to satisfy our innate curiosity

Feel (escape) – Desire for sensory stimulus and pleasure

Identifying investment opportunities through the lens of unchanging human motivations is inspired by Bezos’ excerpt:

“I very frequently get the question: ‘What’s going to change in the next 10 years?’ And that is a very interesting question; it’s a very common one. I almost never get the question: ‘What’s not going to change in the next 10 years?’ And I submit to you that that second question is actually the more important of the two – because you can build a business strategy around the things that are stable in time.”

Examining shifts in power dynamics helps us recognize overarching trends. Examining human behaviors *within* each trend helps us understand specific

points of investment leverage. While the set of human motivations is constant, the weighting of each changes based on environment.

“The lamb and the lion keep a delicate balance, interacting at the margin. If lions were suddenly more swift, they would catch prey that now escape. If lambs suddenly grew wings, lions would starve. The capacity to utilize and defend against violence is the crucial variable that alters life at the margin.”-
The Sovereign Individual

Information technology has altered the balance between the lion and the lamb. It allows us to communicate and coordinate globally. Encryption allows us to store and protect assets against sophisticated attacks. For better or worse, commerce will increasingly be conducted outside the reach of governments’ protection. This increase in individual power will cause a shift in human behavior from “Acquire” to “Defend”. As the phrase goes, “With great power there must also come – great responsibility.”

ACQUIRE → **DEFEND**

Theory of Change #1: Globalization is an equalizing force

Instant information dissemination reduces commercial and jurisdictional barriers to entry *and* barriers to exit. This increases competition by facilitating global entrepreneurship.

Almost all information is readily available online. Increasingly, commerce occurs online. Most work can be coordinated remotely.

This will likely lead to greater income equality between jurisdictions but potentially greater income inequality overall. Highly skilled entrepreneurs have unprecedented leverage to outperform, and unskilled workers have unprecedented, global competition for work. As someone raised in the United States where wage expectations are high, this idea can be unsettling and unpopular.

Competitive wages of remote work overpower jurisdictional boundaries and restrictions. With a diminishing importance on physical availability, the leverage governments have over their citizens decreases. Citizens increasingly become customers, and governments compete for their business. Look no further than the success of Singapore as an example of a highly favorable business environment.

There will be a strong equalizing effect that lower cost jurisdictions and workforces will have on economies. Developed countries may experience uncomfortable periods of deflation. Developing, business friendly jurisdictions

will see outsized economic growth. This creates a wide range of investment opportunities spanning all human behaviors.

The table below is an example of potential investment opportunities and the corresponding demand sources. Green denotes demand now. Orange denotes demand later. “xx” denotes the dominant user motivation.

	Acquire	Defend	Bond	Learn	Feel
Custom education services					
Interactive displays	x			xx	
Learning management	x			xx	
Education assessment systems	xx			x	
Microlearning	x			xx	
Gamified education	x			x	x
Infrastructure in business friendly jurisdictions	x	xx			
Customized media feeds	xx		x	x	x
Local, on-demand manufacturing	xx	x			
Distributed/Outsourced Work	xx	x			
Distributed team building	xx		x	x	x
E-Sports	x		x	x	xx

Education is an especially interesting sector. A high degree of information asymmetry provided institutions enormous power, a monopoly over reputation (degrees), and thus the ability to charge high prices. But with the transcendence of location and vanishing information asymmetry, education is ripe for change. We’re in the beginning stages.

Education is expected to grow to a \$10 trillion industry by 2030 and the industry would be expected to add close to 100 million teachers. That is a massive resource requirement, and with interest in top level higher education falling rapidly, we will see a migration to lower cost, borderless solutions. Further, higher education has been massively subsidized; using the United States as an example, student loan debt sits at a staggering \$1.5 trillion. Government intervention has artificially kept demand for traditional institutions afloat.

The progression in educational demand is straightforward. Scalable, online programs educate highly competitive workforces at a fraction of the cost. These workforces undercut the wages that were once expected from graduates of traditional institutions. Expected value of traditional education falls dramatically and almost all learning is driven to more efficient providers.

Theory of Change #2: Digital money is the foundation for global financial services

The creation of non-sovereign, digital money reduces the power of inflation and taxation. It also further reduces friction of global commerce. With the

advent of Bitcoin, we saw a major governmental lever begin to dissolve. The follow-on effects are not yet obvious.

The fact is, Bitcoin reduces government revenue potential by providing a way to opt out of hyper inflationary forces and by altering taxation enforceability. With digital money, personal wealth becomes more difficult to seize and easier to transport. It further reduces geopolitical borders and allows the cybereconomy to flourish without gatekeepers. Bitcoin allows individuals to better *defend*. Defend against inflation. Defend against seizure. Defend against censorship. As these needs grow, so too will the value proposition of Bitcoin and ancillary applications.

This is another uncomfortable idea as a citizen of the United States. The USD seems infallible. But when growth slows, the first button nations push is the one that turns on the printing press. It’s happening as we speak. After weak attempts to tighten, money supply is rapidly increasing again. This view is not reserved only for Bitcoiners, libertarians, and gold bugs. Ray Dalio’s recent writings ([here](#) and [here](#)) echo this sentiment.

We’re seeing the beginnings of a fintech stack built to support natively digital money and exploit the benefits it provides. Currently, exchanges, custody, mining, and borrowing/lending are the leaders.

Bitcoin businesses can be separated into demand now and demand later:

Speculation (now) – Exchanges, funds, data providers, brokerage services

Defense (later) – Decentralized exchanges, self-sovereign custody, trustless payment products, fiat-to-Bitcoin on-ramps

	Acquire	Defend	Bond	Learn	Feel
Exchanges	xx	x			x
Asset managers	xx	x		x	
Lending/Borrowing	xx	x			
Data providers	xx	x		x	
Custody and private key management		xx		x	
Robust/defensible on-ramps	x	xx		x	
Gaming	x		x		xx
Payment services (new fee models)	xx	x			x
Gifting/Rewards	x		xx	x	
Decentralized exchanges	x	xx			

Right now, the dominant use case for digital money is speculation (drive to acquire). Secondary demand comes from users defending against inflation, asset seizure, taxation or regulatory hurdles (drive to defend). Interestingly, the products that have most effectively delivered on speculative *and* censorship

demands are Bitmex, Binance, and USDT. No wonder they have been so successful.

Exchanges are a good case study for thinking about market demand. Decentralized exchanges (DEX) were all the rage in 2018 but have seen limited adoption. We won't see adoption of fully decentralized solutions until there is greater demand for regulatory arbitrage and dissent. That demand isn't present today but with growing capital controls we will see migration to non-corruptible services.

Along similar lines, solutions that facilitate trust minimized on-boarding, custody, and commerce will become more important. I'm particularly interested in watching adoption trends of onramps like LocalBitcoins, payment services like opennode, BTCPay, and Zap, and key management systems like Casa.

With these products, financial services companies will finally be able to target billions of users around the world. Jill Carlson hits the nail on the head:



Jill Carlson @jillruthcarlson · Nov 7

With the Internet the addressable market for so many companies went from local (millions) to global (billions).

What got left out? Financial services. Locked in by jurisdictional regulations & currencies.

Crypto for the first time unlocks a global market for financial services.

Theory of Change #3: Encryption enables dissident technology

Encryption reduces the cost of protection and decreases the leverage of violence. This enables significant power to move from the center and toward the margins (free markets). See this post from the FBI general counsel on why encryption is such powerful force and how governments are unable to stop it.

Continued recognition of vulnerabilities in infrastructure and applications, and the development of viable replacements, will lead to demand for an antifragile, censorship resistant, borderless webstack. I had been struggling to find a proper description for these “crypto” applications, and I think Maya Zehavi captures it perfectly with “dissident tech”.



Maya Zehavi - DePi 🍕 @mayazi · Nov 6

Dissident tech is going to be a thing sooner than any of us realize & it fits right into crypto for the most part

Further, aggregators and public service providers are honey pots that have become targets for attack because there is an asymmetric reward profile.

-

Attack on corporation: Large Reward

Strong Security

-

Attack on individual: Small Reward

Strong Security (power of encryption)

However, this switch from centralized systems to distributed systems requires a fundamental shift in human behavior. We are used to outsourcing our security and protection. This is why we see limited adoption of crypto applications. It's not *just* a scalability issue. It's a demand issue. Our environment hasn't yet warranted a behavior change but the undercurrents are growing. More specifically, the demand for these distributed technologies comes from two angles:

Cost efficiencies – removing middle men can decrease predatory rent seeking. This is a marginal benefit and not powerful enough to force a switch.

Defensibility – These systems have the potential to be antifragile, safer, and censorship resistant (dissident). These are 10x improvements.

	Acquire	Defend	Bond	Learn	Feel/Escape
User controlled identity and data	x	xx			
Verification services	x	xx			
Data marketplaces	x	xx			
File storage	x	xx			
Video encoding	x	xx			
Location services	x	xx			
Mesh networking	x	xx			
Distributed computing	x	xx			
Decentralized finance	x	xx			
Censorship resistant domains	x	xx			

Consider the ability to run applications on a personal, encrypted single server (Urbit style), store your data locally, and get paid to share it through homomorphic encryption on an open market without the potential for data duplication. This would transform the incentives of internet companies who currently rely on data mining, it gives a huge amount of power back to the users, and it would generate countless new business models. The incentives to force this behavior change aren't here yet, but they *are* coming.

Conclusion

- Online education will continue to equalize workforces. Wages in developed countries will trend lower while wages in developing countries will grow.
- Digital money is the catalyst for truly global fintech companies. The regulatory pushback will be intense but futile.
- There is a growing need but not an imminent demand for dissident technologies. We have to focus on incentives and user demand.

The Sovereign Individual popularized many of these ideas in 1997, and they have begun to take hold. We are still in the early stages. I think the tipping point will be in the next 10 years. This framework only scratches the surface, and I plan to follow up with deeper research into each section.

Thanks to Nathaniel Whittmore, Ryan Yi, Christian Kaczmarczyk, and Jimmy Cofsky for feedback on this piece.

Digital Money

The Most Exciting Investment of the Century

By Phil Bonello

Posted October 22, 2019

Software is eating the world and money is no different.

Bitcoin is the best performing asset of the decade. It is uncorrelated to other asset classes, and it is still underpriced relative to the likelihood it becomes a widely adopted store of value.

In 2018, crypto asset prices crashed and for good reason. 2017 saw a meteoric rise in prices and extreme irrational exuberance. The euphoria was followed by a much-needed return to rational pricing. But don't let the bubble scare you. It's important to understand the motivation behind Bitcoin and why it represents a historic investment opportunity and a step toward greater self-sovereignty.

Following the global financial crisis in 2008, central banks launched Quantitative Easing to fuel economic expansion, or more accurately, forestall a massive and global recession. The tradeoff – economies became dependent on cheap money. Bitcoin emerged on the eve of this experiment.

With about \$184 trillion in global debt, central banks, in particular the Federal Reserve, attempted to tighten monetary policies in 2018, but due to concerns of slower than forecasted economic growth, they have since reversed course. QE is back. The 2019 U.S. budget deficit has now passed an eye-popping \$1 trillion. If you were writing the script for a non-sovereign, fixed-supply, digital form of money to gain mass adoption, this is how you would write it. With massive debt looming and monetary policy front-and-center, it is becoming clearer that we need other options.

The good news is that institutional infrastructure is being built to transition our monetary system to the digital age. It is still early, but there are strong efforts underway. Fidelity launched their Bitcoin custody services, the Intercontinental Exchange (ICE) launched physically settled futures contracts for Bitcoin, and endowments and pensions are exploring the best way to gain exposure. The IMF is also taking serious notice.

Instead of adopting the currency of another country—such as the U.S. dollar—some of these economies might see a growing use of virtual currencies. Call it dollarization 2.0. So in many ways, virtual currencies might just give existing currencies and monetary policy a run for their money. The best response by

central bankers is to continue running effective monetary policy, while being open to fresh ideas and new demands, as economies evolve. – Christine Lagarde, IMF Managing Director, 2017

One way to think about an investment in non-sovereign, digital money is as a put option on dominant fiat currencies. In the 1990's it was impossible to imagine that the internet would replace newspapers, TV, and retail stores, among other things. Similarly, today it is difficult to imagine a crypto asset becoming the basis of a global monetary standard. But how farfetched is the idea, really?

Software is eating the world and paper money is next on the menu. The specific outcome is less important than recognizing this paradigm shift. Public blockchains enable ownership and transfer of *fully digital* assets without a trusted intermediary for the first time. This is revolutionary.

As most things have gone from analog to digital, why would sovereign currencies be immune from this transition? The force of technology is unstoppable.

For over 5000 years humans converged on gold as the global monetary standard for good reason. Sure, it was viewed as beautiful, but more importantly, gold has been resistant to rampant supply inflation. It has maintained its purchasing power throughout history.

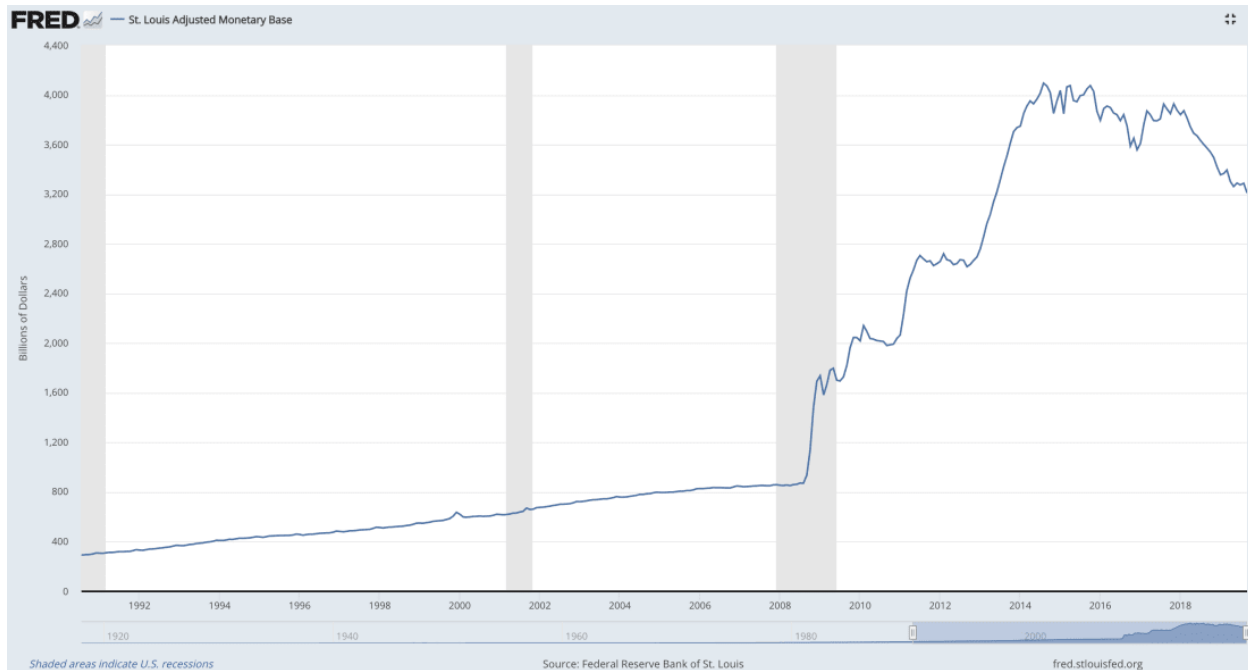
Where gold has failed is in its transportability and verifiability. It's hard to transport gold. This is an important issue in an increasingly global economy. Gold is also hard to verify with certainty. The very existence of gold reserves is often taken on faith. We are required to believe in systems and organizations that have been established to take care of us and our money. This faith has given power to central banks to print money, backed by a sovereign government. This works well enough as long as nations are economically prosperous. But there are many recent examples of catastrophic hyperinflation that renders the currency worthless. Look no further than the current media headlines covering Venezuela, Turkey, and Iran. Their currencies are circling the drain.

As sovereign currencies go, the US dollar is a relatively stable money; it's the de facto global reserve. It's our best bad idea. However, it is important to note that it's only been 48 years since the US abandoned the gold standard... The free-floating USD hasn't been battle tested.

There is no example of a fiat currency ever holding its value. The British Pound Sterling is the oldest survivor at 317 years. The British Pound was originally defined as 12 ounces of silver. Today it is only worth .5% of its original value. The burden of proof is on current monetary regimes and it's not looking good.

Consider the chart below. Since 1969 the annualized compounded *supply* of USD has increased at 9% a year. This equates to a doubling of US dollar supply every 8 years. By this metric, the US dollar is a poor store of wealth.

Additionally, and as a historical rule, if a money's supply can be increased, it will be increased. Salt, Rai stones, copper, sea shells, and numerous examples of government-issued monies have fallen victim.



Source: Federal Reserve Bank of St. Louis

Bitcoin is still a speculative vehicle today, but it picks up where gold left off. It is incredibly inflation resistant; there will never be more than 21 million. It also succeeds where gold failed. It's easily transportable; we can send a million dollars of BTC around the world for \$.10. It is also easily verifiable; sharing a public key allows full transparency of the balance in a digital wallet.

There is a good chance that Bitcoin or another emergent crypto asset will become the global monetary standard. One way to quantify the market opportunity is by estimating Total Address Market (TAM). To that end, note the following:

	Estimated Value (\$bn)	Multiple on BTC	Source
BTC Value	\$ 150.00	x	OnchainFX
10% of Global Gold Value	\$ 770.00	5x	Visual Capitalist
Global Gold Value	\$ 7,770.00	52x	Visual Capitalist
US Debt Balance	\$ 22,000.00	145x	USDebtClock.org
Global M1 Money	\$ 34,000.00	225x	CIA 2017
Global M2 Money	\$ 86,000.00	570x	CIA 2017

It will increasingly be viewed as responsible and prudent to hold some wealth in crypto assets as a hedge against fiat monies. This portfolio adjustment also mitigates the risk that one's wealth will be devalued relative to a new global monetary standard.

Booms and busts will be a natural part of global adoption. Prices will continue to be volatile - likely an order of magnitude more volatile than developed market public equities. But with each boom and bust, confidence in digital currencies grows as they prove their anti-fragility and refuse to die.

There are a lot of obstacles ahead, but the possibility of a new global monetary standard presents an amazing step for individual sovereignty and an incredible investment opportunity.

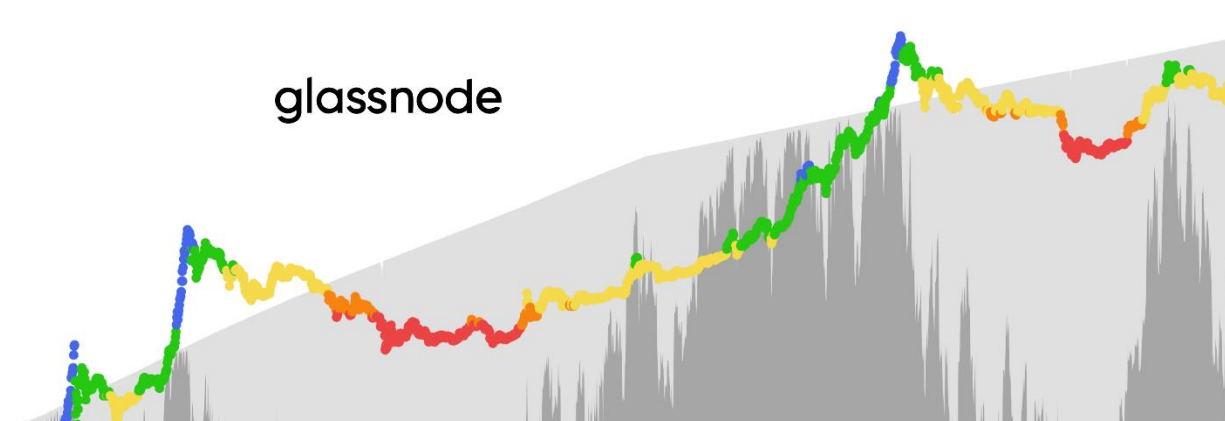
Paper is poverty. It is only the ghost of money, and not money itself. – Thomas Jefferson to Edward Carrington, 1788

Dissecting Bitcoin's Unrealised On-Chain Profit/Loss

Introducing a New Set of Metrics to Help Time Bitcoin Market Cycles

By Rafael Schultze-Kraft

Posted November 13, 2019



Understanding the state of the Bitcoin blockchain with respect to the price at which BTC is being valued by the market is indispensable for any investor in this new asset.

In fact, Bitcoin *on-chain* data has been used in conjunction with *off-chain* market data in order to create metrics and indicators that help investors gain fundamental insights into the current state of the market, understand investor sentiment, or model the value of Bitcoin.

Popular examples are MVRV and SOPR.

These metrics have in common that they make use of Bitcoin's underlying UTXO structure by comparing the value of Bitcoin at two different points in time: The **current price** and the price at the time a UTXO (bitcoin) was created (last moved), i.e. the **realised price**.

Here, we make use of the same underlying concept in order to answer a fundamental question:

If all bitcoins were sold today, how much would investors stand to gain or lose?

Or to put it differently: **How much of Bitcoin's circulating supply is at any given point in time in profit or loss – and to what extent?**

The ability to access this information is important to investors with regard to Bitcoin's primary narrative: to act as a digital, permissionless, censorship-resistant Store of Value (SoV).

To answer these questions, we take three different approaches and define new sets of metrics – each adding an additional level of detail:

1. The number of current UTXOs that are in profit/loss

A UTXO is in profit (loss) if the current price is higher (lower) than the price at the time the UTXO was created.

2. The current supply of Bitcoin that is in profit/loss

A bitcoin is in profit (loss) if the current price is higher (lower) than the price at the time the bitcoin last moved.

3. The unrealised profit/loss of the current Bitcoin supply

The profit (loss) of a bitcoin is calculated by taking the difference between the current price and the price at the time the bitcoin last moved.

Let's dig in.

Number of UTXOs in Profit/Loss

The number of UTXOs in profit/loss is computed in a straight-forward manner: We simply count all existing UTXOs whose price at creation time was lower or higher than the current price, respectively.

Figure 1 below shows the absolute amount of UTXOs in profit/loss at any given point in time.

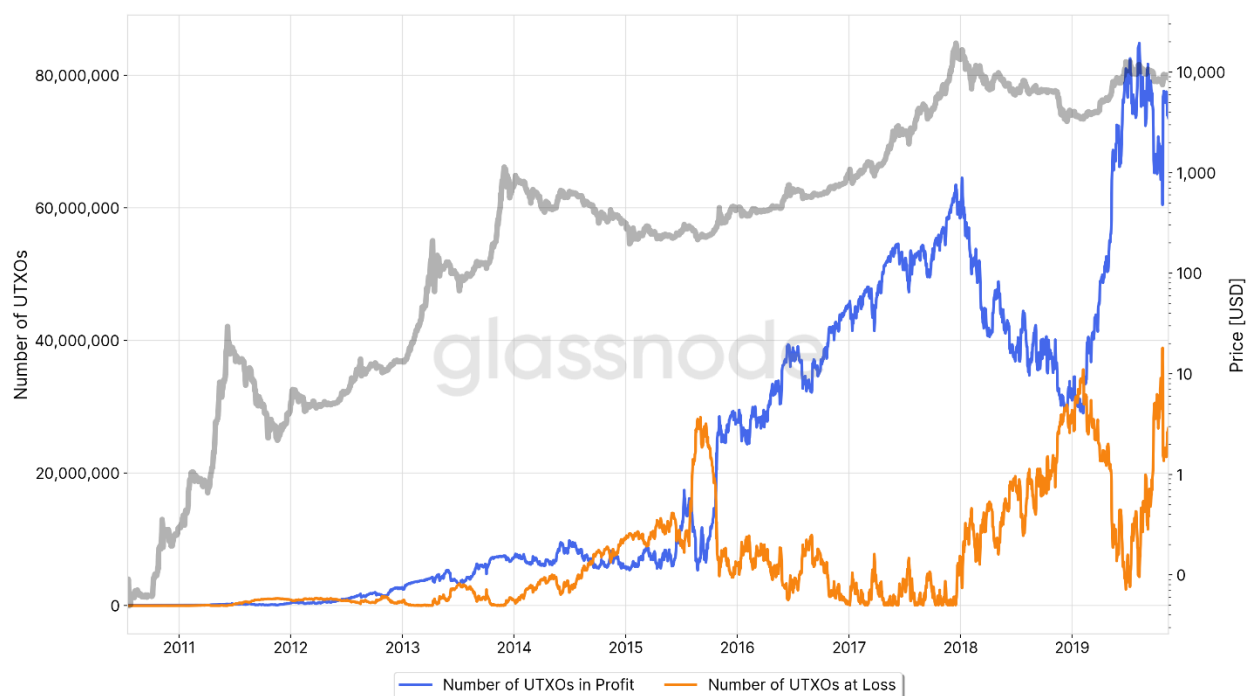


Figure 1 – Number of UTXOs in Profit and Loss

In order to account for the increasing number of UTXOs over time, we normalise these time series by the size of the UTXO set and obtain the relative number of UTXOs in profit/loss, i.e. the percentage.

Figure 2 below represents the 50d MA of the relative UTXO counts in profit. Note that when this metric approaches 100%, it has historically been a good indicator for global market tops.



Figure 2 – Relative Number of UTXOs in Profit, 50d Moving Average

The bull run of 2017, however, shows a distinct behaviour with a sustained period of profitable UTXOs above 95% – a clear indication of the remarkable nature of the bull run that year. Throughout those months, the metric can be used to help identify short-term cycles and as a clear indicator to stay highly alerted throughout the mania of such periods.

Note that the relative number of UTXOs in profit approaches 100% every time a previous ATH price is broken – this is self-evident as it becomes nearly impossible to be in losses once a new ATH is surpassed. Therefore, we applied the simple 50d MA, which we have found to fit historic data optimally and which creates a signal that serves to indicate global/local Bitcoin cycle tops as shown above.

Live implementations of UTXOs in Profit/Loss metrics are available in Glassnode Studio:

[Percent UTXOs in Profit](#) [UTXOs in Profit](#) [UTXOs in Loss](#)

Circulating Supply in Profit/Loss

A similar but even more informative metric is the number of circulating bitcoins that are in profit or loss. Instead of counting UTXOs, we now consider their bitcoin value (i.e. individual bitcoins) and sum up those whose price at the time they last moved was lower or higher than the current price, respectively.

The stacked graph below shows the supply of bitcoins in profit/loss at any given point in time.

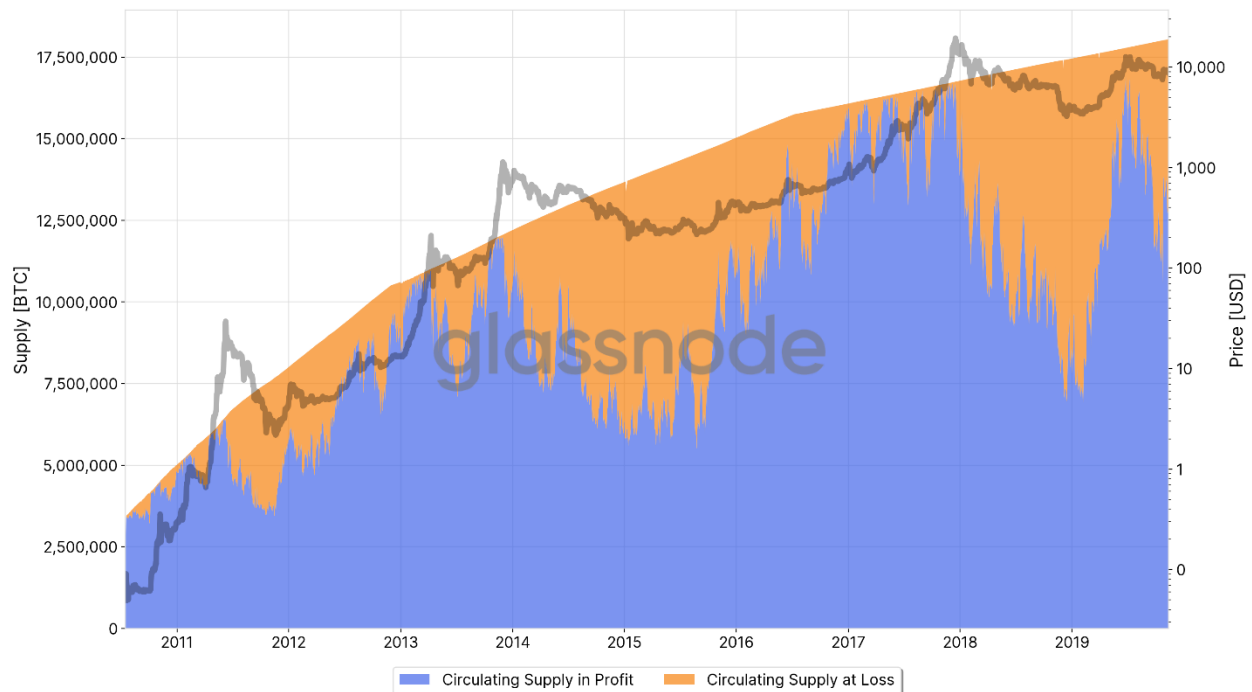


Figure 3 – Circulating Bitcoin Supply in Profit and Loss

Similarly, we adjust this data by dividing by the circulating supply and obtain the relative Bitcoin supply (i.e. percentage) that is in profit/loss.

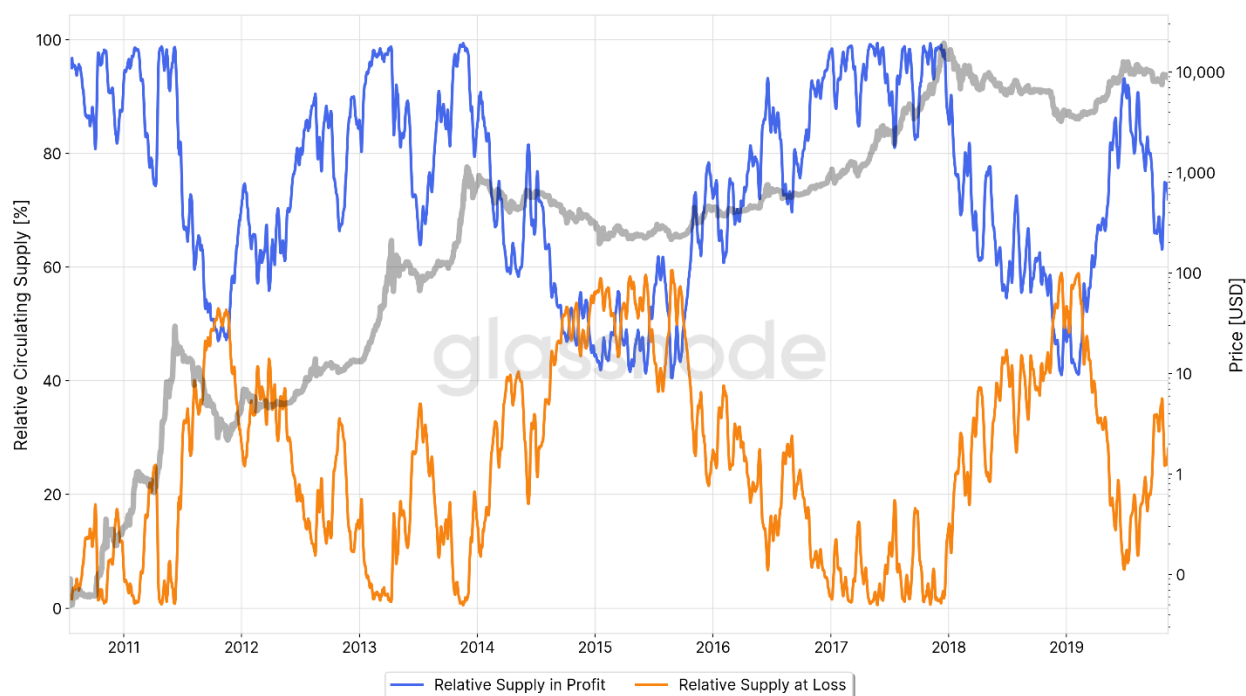


Figure 4 – Relative Bitcoin Supply in Profit and Loss

The resulting graph is a metric we have found to be exceptionally useful to help understand Bitcoin market cycles.

Let's take close look at the **Percent of Supply in Profit**, again applying the 50d MA.

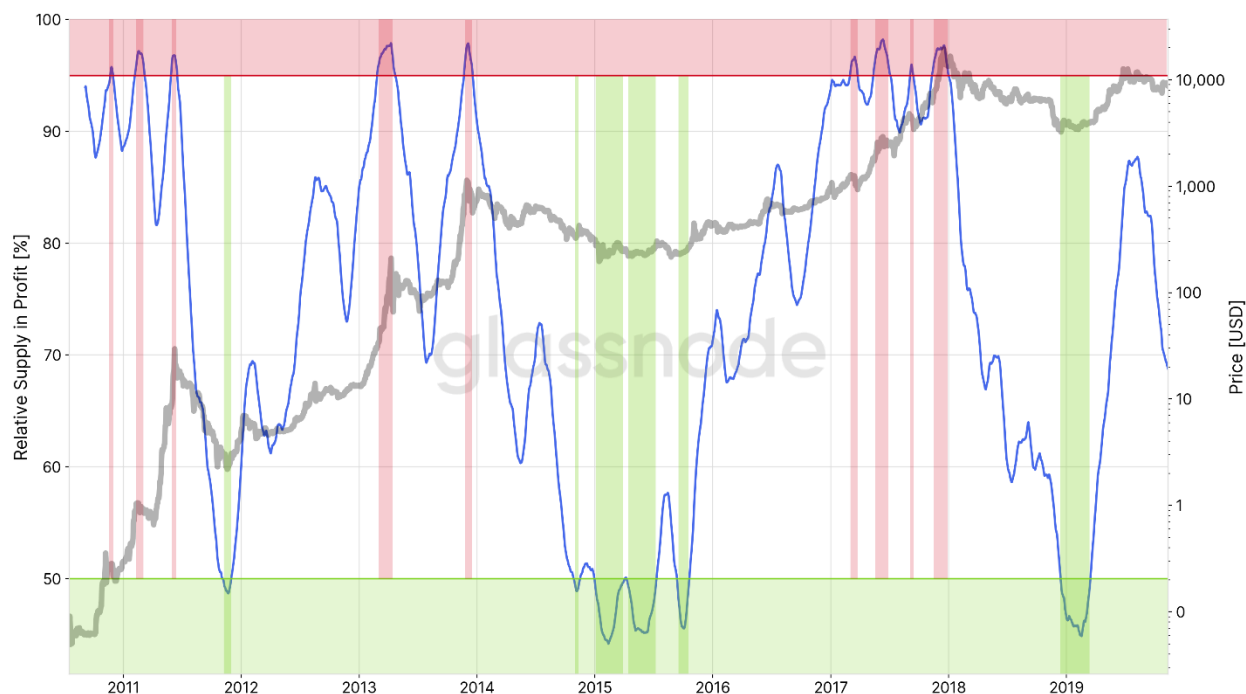


Figure 5 – Relative Bitcoin Supply in Profit, 50d Moving Average

The Percent of Supply in Profit metric represents an oscillator that allows us to better understand the current state of the Bitcoin market:

- In a similar fashion to the relative UTXO count chart above, using a simple threshold at 95% helps to identify **market tops**.
- By looking at periods in which the relative supply in profit falls below 50%, this indicator is useful to help identify **market bottoms** and convenient entry points.

Live implementations of Supply in Profit/Loss metrics are available in Glassnode Studio:

[Percent Supply in Profit](#) [Supply in Profit](#) [Supply in Loss](#)

Unrealised Profit/Loss

Finally, we take a step further and look at the **Unrealised Profit/Loss** of Bitcoin.

In comparison to simply summing up the circulating supply that is in profit or loss, Unrealised Profit/Loss takes into account the actual USD value by which a bitcoin is in gains/losses. In other words, we weight each circulating bitcoin by the difference between the current price and its realised price and sum up all bitcoins in profit and loss, respectively.

Mathematically speaking *Unrealised Profit (UP)* and *Unrealised Loss(UL)* are defined as

$$UP = \sum_{UTXOs} \text{value} \cdot \max(0, price_{\text{current}} - price_{\text{realised}})$$

and

$$UL = \sum_{UTXOs} \text{value} \cdot \max(0, price_{\text{realised}} - price_{\text{current}})$$

respectively.

The following graph shows Bitcoin's raw Unrealised Profit/Loss.

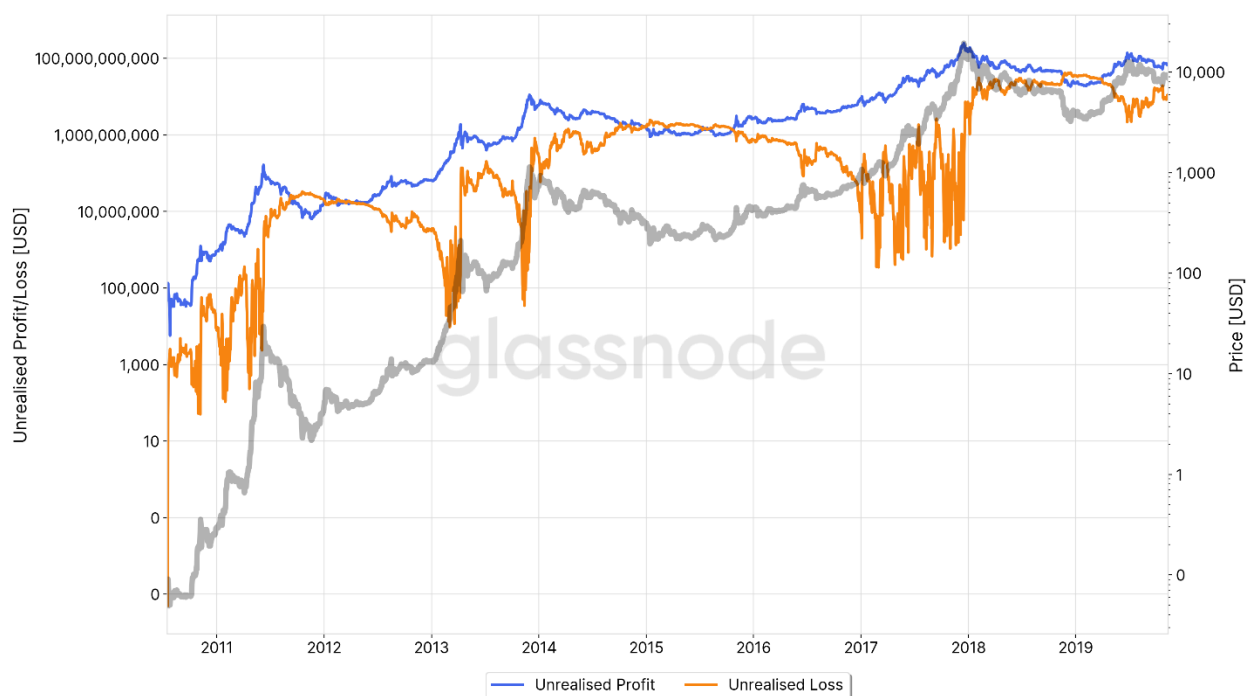


Figure 6 – Unrealised Bitcoin Profit and Loss

While the UP line very much resembles the shape of the Bitcoin price, the amount of unrealised loss (UL) shows a distinctive pattern with clear-cut downward spikes at periods in which the losses are virtually non-existent. These moments naturally correspond to those in which the relative number of bitcoins/UTXOs in profit approaches 100% (see *Figures 2+5*).

In order to obtain a conclusive and more informative metric, we normalise the data by the market cap, giving us the **Relative Unrealised Profit (RUP)** and the **Relative Unrealised Loss (RUL)**. The resulting signals clearly reveal distinct patterns at different states of the market cycles.

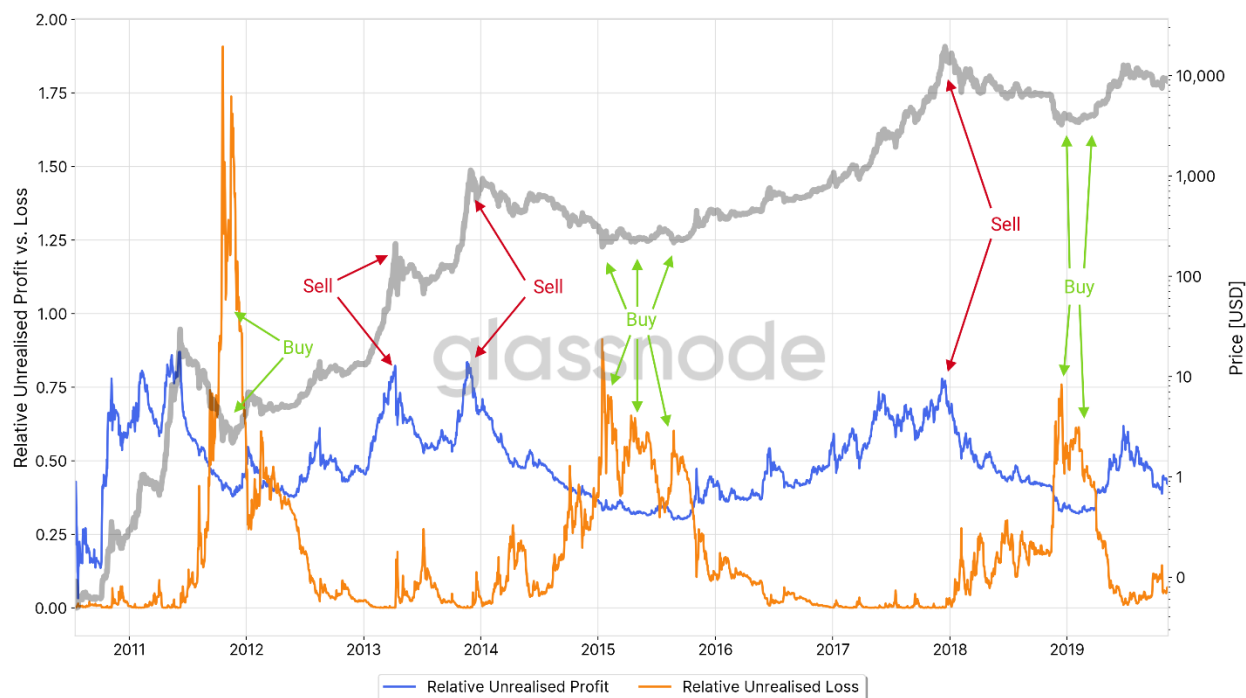


Figure 7 – Relative Unrealised Profit and Loss

In particular we see how the RUP spikes ($RUP > 0.75$) indicate potential tops and selling points. Conversely, periods in which the RUL exceeds the RUP ($RUP < RUL$) have been historically indicative of market bottoms and good buying opportunities.

By taking the delta of both curves, we finally calculate the **Net Unrealised Profit/Loss (NUPL)**.

Deconstructing this signal into different bands gives insight into market sentiment derived from on-chain data. The thresholds below are set at 0.0, 0.25, 0.5, and 0.75. Even though arbitrary, historically they show accurate patterns that can be attributed to distinct sentiments throughout the macro cycles of Bitcoin.



Figure 8 – Net Unrealised Profit/Loss (NUPL)

By mapping these bands to the price of Bitcoin we see how the **NUPL** represents different periods of the Bitcoin market cycles. Understanding the current NUPL value can help investors navigate through different stages of the market and identify periods of profit taking as well as efficient entry points.



Figure 9 – NUPL Bands applied to the Bitcoin Price

UPDATE: Net Unrealised Profit/Loss has been previously derived by Adamant Capital in a different manner: They calculate it by subtracting realised cap from market cap, and dividing the result by the market cap, i.e. $(\text{Market Cap} - \text{Realised Cap}) / \text{Market Cap}$. This is mathematically in fact equivalent to the derivation introduced here: $\text{Unrealised Profit} * \text{Market Cap} - \text{Unrealised Loss} * \text{Market Cap}$.

Live implementations of Unrealised Profit/Loss metrics are available in Glassnode Studio:

[Net Unrealised Profit/Loss \(NUPL\)](#) [Relative Unrealised Profit \(RUP\)](#) [Relative Unrealised Loss \(RUL\)](#)

Summary

We explored and presented a set of on-chain metrics that incorporate the relationship between the current price and the realised price of Bitcoin. In particular we defined metrics related to

1) the **Number of UTXOs in Profit/Loss**, 2) the **Bitcoin Supply in Profit/Loss**, and 3) the **Unrealised Profit/Loss**.

These metrics help in understanding the current profit and loss of stakeholders in the Bitcoin network using on-chain data – information that is crucial to evaluate the state of Bitcoin as a Store of Value (SoV).

Moreover, these metrics are indicative of the Bitcoin market cycles and shed light on investor sentiment at different stages, most notably using Net Unrealised Profit/Loss.

With the present work, we have equipped Bitcoin investors with a new set of tools providing a better understanding of Bitcoin's market cycles and its economics. The introduced metrics can be used to assist investment strategies that go beyond simple HODLing, and help to avoid buying towards the top and selling near the bottom of Bitcoin's cycles.

Metrics Overview

UTXOs

Percent UTXOs in Profit UTXOs in Profit UTXOs in Loss

Supply

Percent Supply in Profit Supply in Profit Supply in Loss

Unrealised Profit/Loss

Net Unrealised Profit/Loss (NUPL) Relative Unrealised Profit (RUP) Relative Unrealised Loss (RUL)

glassnodeinsights

All analyses in this article were done using data from Glassnode Studio. For API access to this data visit the [Glassnode API page](#).

- Sign up for the Glassnode Insights Newsletter
- Follow us and reach out on Twitter
- For on-chain metrics and activity graphs, visit Glassnode Studio
- For automated updates about on-chain activity on exchanges, visit our Glassnode Alerts Twitter

Disclaimer: This report does not provide any investment advice. All data is provided for information purposes only. No investment decision shall be based on the information provided here and you are solely responsible for your own investment decisions.

Glassnode

Contextualised and actionable market insights, reports and analyses drawn from on-chain data.

Thanks to Rafal Bromirski, Glassnode, and Matthias Bachmann.

Bitcoin is guerilla warfare.

By AMERICAN HODL

Posted November 13, 2019

Bitcoin is guerrilla warfare.

Sovereign individuals vs sovereign collectives.

They're marching in formation and we're hiding in forests.

They're following a hierarchical structure and we're winging it.

They don't know the territory...

The battleground is our native soil.

Bitcoin Is The Only Way To Opt-Out

A Cashless Future Is A Dystopia

By Rhythm

Posted November 19, 2019



The world is becoming increasingly digital. Remaining tethered to a physical piece of paper for transactions seems archaic at first thought. Choosing between making a payment via a scan of a phone or credit card versus the need to carry around a wallet full of cash is obvious. It is not without consequences, however. The convenience of a cashless society comes with the cost of privacy.

Coin Center, a non-profit research and advocacy center focused on public policy issues facing cryptocurrency, has published a report [here](#). Below in quotations are a few sections taken from the report:

In a world without cash (a bearer and peer-to-peer form of money) all transactions must be necessarily intermediated by financial institutions. Intermediated transactions are by their nature subject to surveillance and

control. If third-party financial institutions must be part of all transactions, then they will be privy to the intimate details of everyone's financial life. They can also choose to disallow certain transactions and potentially even certain persons from transacting. - Coin Center

We have already seen financial data used by governments all across the world to suppress their citizens. It may be as seemingly inconsequential as de-platforming an individual deemed unsafe to the public or as oppressive as implementing a nationwide ranking system used to monitor the behavior of civilians. Both have long-reaching effects, but the latter is now just coming to fruition in China. Information from the day-to-day lives of its 1.3 billion citizens is aggregated into an overall score that deems each individual access to public facilities like the transit system. ([source](#))

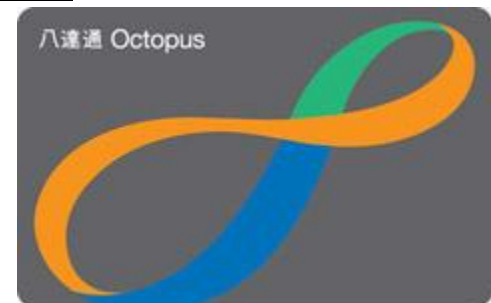
Earlier this year, China banned 23 million citizens from buying basic travel tickets due to their low social score ([source](#)). A document outlining this plan is quoted as saying, the goal is to “allow the trustworthy to roam everywhere under heaven while making it hard for the discredited to take a single step”.

“By 2020, China’s rulers aim to implement an Orwellian system premised on controlling virtually every facet of human life—the so-called ‘social credit score’” - U.S. Vice President Mike Pence. A society in which payments are all done digitally, through third parties under the authority of government, would likely enable the “blueprint” Vice President Pence is referencing to. It may even be the last missing piece to the overall plan.

It is not much of a leap to expect those same authorities to continue pushing for a cashless society. Tracking, monitoring and collecting financial data of transactions would be just one more aspect of lives being surveilled.

Without cash there is no exit—no chance for the kind of dignity-preserving privacy that undergirds an open society. - Coin Center

We are seeing an example of this in Hong Kong. Digital payments are commonplace. Most people use a debit card-like option called an “Octopus card”. When getting on a bus or purchasing something from a store, citizens just scan the card for payment ([source](#)).



Yet, protestors do not use their digital Octopus cards when gathering to demonstrate. There is a risk that the Chinese government will track the payments and determine the location of protest groups to “unmask” the individuals participating. As an example, a protestor scans their card on the metro station a block away from the protest, and then again once the protest

ends. Software can easily be created and designed to piece together the data. This is a rightful privacy concern to their freedom when used in the wrong hands ([source](#)).

Hong Kong saw massive lines at metro stations as protestors, and non-participating citizens, were not willing to use a trackable digital means of payment. “We’re afraid of having our data tracked,” a protester told reporter Mary Hui. Purchasing a physical ticket not only takes time, it also costs more than the equivalent ticket bought with the Octopus card. It is normally tourists that use the physical ticketing machines, not locals.



Mary Hui
@maryhui

There is usually never a line at the train ticketing machines. Judging from an overheard convo, it appears that people are reluctant to use their rechargeable Octopus cards for fear of leaving a paper trail of them having been present at the protest.



June 12th 2019

3,328 Retweets 6,686 Likes

“Show me the man and I’ll show you the crime” is a quote from the deputy premier, the head of Joseph Stalin’s secret police force in the former Soviet Union. He supervised surveillance and the detention facilities for “political prisoners” of one of the most ruthless and bloody government regimes in history ([source](#)). When the government can decide what is “illegal” and what is not, anything you may have done in the past can be used against you. Acts that might have been thought of as insignificant at the time are recorded. That

becomes an especially powerful tool when a government has at their disposal everything you have ever said or done online.

A French Cardinal by the name of Richelieu, in the 17th century famously said, **“If you give me six lines written by the hand of the most honest of men, I will find something in them which will hang him.”** ([source](#)). He was known for his corruption and leveraging the rule of law at the time in his favor. He prosecuted anyone that stood in his way of consolidating governmental power. Richelieu and Joseph Stalin’s deputy are speaking of the exact same thing: when the government has enough data collected on an individual, they will have no problem finding something in that pile of information to frame into evidence and level unfounded charges. It does not matter what specifically they find, as humans are prone to errors. How many emails or texts have you sent? How many tweets have you published? How many phone calls have you taken? How many times have you used your credit card?

Surveillance puts everyone at risk from overreach of even the most democratic of governments. There is no guarantee the same governing party will exist in the future, unlike the data they collected which will forever be available.

Cash is also necessary to retain agency and autonomy. Autonomy can be understood as the power to make decisions for oneself without interference from others. It’s the ability to try things one’s way, to succeed and be rewarded, or to make mistakes and learn from them. As with personal privacy, without individual autonomy there can be no meaningful open society. It is therefore imperative that we preserve our ability to use it [cash]. Yet that is not enough. As we move to an increasingly online world in which physical cash is not practical for many transactions, we must also develop and foster electronic cash that is as privacy-preserving and permissionless as physical cash. While this will have costs as well as benefits, we argue that the way to address the costs is not to prohibit electronic cash, but instead to regulate its use no differently than physical cash for which there is a robust regime. - [Coin Center](#)

Is the World Going Cashless?

In short, yes. It is happening faster than many think. Here are figures from the [World Cash Report](#):

Country	Continent	% Cash	Source
South Korea	Asia	14%	BOK study
Finland	Europe	54%	ECB Diary Study
Estonia	Europe	48%	ECB Diary Study
Latvia	Europe	71%	ECB Diary Study
Lithuania	Europe	75%	ECB Diary Study
Slovakia	Europe	78%	ECB Diary Study
Austria	Europe	85%	ECB Diary Study
Slovenia	Europe	80%	ECB Diary Study
Greece	Europe	88%	ECB Diary Study
Cyprus	Europe	88%	ECB Diary Study
Malta	Europe	92%	ECB Diary Study
Italy	Europe	86%	ECB Diary Study
Germany	Europe	80%	ECB Diary Study
The Netherlands	Europe	45%	ECB Diary Study
Belgium	Europe	63%	ECB Diary Study
Luxembourg	Europe	64%	ECB Diary Study
France	Europe	68%	ECB Diary Study
Spain	Europe	87%	ECB Diary Study
Portugal	Europe	81%	ECB Diary Study
Ireland	Europe	79%	ECB Diary Study
Sweden	Europe	20%	ECB Diary Study
United Kingdom	Europe	42%	Payments UK Diary Study
Australia	Oceania	37%	RBA Diary Study
United States of America	North America	32%	FedResSys Diary Study

The world is moving towards completely digital payments. As more of our lives are spent online, this seems inevitable. While some citizens are transitioning to a digital medium willingly, due to the benefits of convenience, not every government is taking a hands-off approach.

China

Beginning in 2016, the People's Bank of China put measures in place for reporting all domestic and overseas cash transactions of more than ~\$7,350, compared to the previous ~\$29,400 ([source](#)).

In late 2017, the Central Bank then put an annual cap of ~\$14,000 per person and daily limit of ~\$1,400 that applies to all ATM cards issued by mainland Chinese banks, covering both yuan and foreign exchange accounts ([source](#)).

Earlier this year, Chinese banks lowered the daily limit on foreign-currency cash withdrawals from an already restricted ~\$5,000 to ~\$3,000 ([source](#)).

Likely in anticipation of the government's digital currency, a new bill requires business accounts to be "registered" for any amount of cash transactions above ~\$71K. A similar measure is in place for personal accounts which will range from ~\$15k to ~\$60k ([source](#)).

As expected, the reasoning by the People's Bank of China for this restriction on larger-scale cash transactions is to prevent cash from being "exploited" by illegal criminal activities such as corruption, tax evasion and money laundering ([source](#)). This is a common theme across the world used to limit the use of cash by everyday citizens.

India

Arguably the most aggressive approach by a government to reduce the amount of cash transactions was instituted by the India ruling party in 2016. The government made a surprise announcement of the demonetization of all ₹500 and ₹1,000 banknotes used by the country ([source](#)). That had comprised 86% of India's currency at the time.

The Prime minister of India, Narendra Modi, the man instituting this action, claimed that this would seriously hinder the ability of India's massive "shadow economy" to transact and reduce the use of illicit and counterfeit cash to fund illegal activity and terrorism.

On the anniversary of this action, three years later the Former Finance Minister called for a further reduction of banknotes by demonetising the ₹2,000. These notes account for about one-third of currency notes in circulation, in terms of value ([source](#)).

It does not stop there. The Finance Ministry is aiming to put even more stringent controls on the amount of cash citizens are allowed to hold at home or in “lockers” by next year ([source](#)).

Argentina

Argentina has been plagued with a period of high inflation as government elections have shocked the economy. In September of this year, Argentina's Central Bank instituted capital controls with citizens only able to buy up to \$10,000 in US Dollars. Even companies need to get permission to buy foreign currency or precious metals, and to transfer that money abroad ([source](#)). A month later, the restrictions became more severe, with a limit of \$200 in US Dollars for citizens and a complete restriction on the purchasing of digital cash in the form of Bitcoin ([source](#)). While this move has been criticized as solely about keeping value within the local economy, it is a transition that will likely not be reverted. Once citizens are forced to maintain accounts in a digital form, the control of the government will be that much more powerful.

Lebanon

A proposed tax on the messaging app, WhatsApp, sparked nationwide protests reported in Lebanon a month ago ([source](#)). Like many protests happening around the world, there was widespread social and economic unrest building prior to these events. Lebanon has a history of government mismanagement as exemplified by its incredibly high national debt of \$86 billion. As it stands today, the country has the third highest public debt-to-GDP ratio in the world ([source](#)).

Since the protests began, banks have been closed nearly continuously. They only opened up recently to then close the following day due to the bank tellers going on strike. Citizens have had to revert to digital forms of payment and limited cash from ATMs. Lebanon's state prosecutor banned traders and money exchangers from taking “significant amounts” of physical cash out of the country ([source](#)). With protests gripping the country, the government does not want a flight of capital. But like Argentina, this move is likely to have lasting impacts.

Malaysia

The Malaysian government is planning to impose a cash transaction limit of RM25,000 starting next year, which amounts to about \$6,000 ([source](#)). “This is to address the abuse of physical cash used for illicit activities,” Bank Negara (BNM) deputy governor and chairman of the National Coordination Committee to Counter Money Laundering (NCC), Datuk Abdul Rasheed Ghaffour said.

Malta

Malta, known for more lax regulations relative to the rest of Europe, has now put a 10,000 euro restriction on cash transactions. Pressure from international institutions had the country follow suit with the rest of the Euro countries that each have similar bans in place ([source](#)).

Zimbabwe

After a historic period of hyperinflation over a decade ago, the government has just started to recirculate physical cash banknotes for citizens. Most transactions have since been digital and processed through mobile payment systems. There was even a ban in place that prevented merchants from accepting cash in or cash out for customers ([source](#)).

The amount of new banknotes has not been nearly enough to satisfy the demand. Citizens want physical cash. After a delay from the promised time of the banknotes release, ATMs were emptied instantly and a large amount of the paper went straight to the black market as they are highly valued within the country ([source](#)).

Australia

Even democracies are contemplating increased restrictions on the use of cash by its citizens. A seemingly controversial bill to ban cash payments of \$10,000 or more imposing possible two-year jail sentences, has passed the Lower House of Australia's governing body. It is important to note that this will not become law until after a Senate inquiry ([source](#)).

The proposed change was first suggested by the Government's Black Economy Taskforce as a way to stop criminal gangs using large cash purchases of cars, houses and jewelry to launder their gains from illegal activities.

Assistant Treasurer Michael Sukkar had argued that a \$10,000 cash limit for transactions between businesses and individuals would help fight the illegal cash economy by stamping out tax evasion, money laundering and other crimes.

How Does Blockchain Fit In?

The term "blockchain" in the literal sense just means a "chain of blocks", a list of records, called "blocks" - quite similar to that of spreadsheet pages. The pages are cryptographically linked together, one after another. This concept goes back nearly thirty years in cryptography and computer science, but the term and technology have been made popular recently due to the way the Bitcoin Network has emerged.

One country known to be at the forefront of surveillance technology, China, is close to launching their own national stablecoin using a blockchain database structure. They are upgrading their current mix of cash and online currency to that of a purely digital medium.

Currently, the People's Bank of China seems to be the closest to launching theirs ([source](#)). Goals you would expect from any government, like tax enforcement and censorship, become much easier with the ability to shut-off access to anyone on the system with a "flip of a switch". A digital currency would be accomodating. While Bitcoin was created to use blockchain technology as the means and censorship resistance as an end, a stablecoin would centralize and enable mass censorship, ironically, at a scale nearly impossible today. All transactions ever completed in the economy will be on a single ledger, or spreadsheet.

Traditional fiat currencies may already be mostly virtual and relatively easy to control, but there are numerous databases that transactions are spread across. Fiat is currently transferred throughout a network of payment processors and application databases that effectively become barriers to an efficient surveillance and censorship state. While we see people deplatformed across the world everyday, there are limitations to the effect of that power. Digital currencies issued on a single database, possibly a blockchain structure, eliminates this problem. It's a more perfect means of storing data that allows sophisticated tracking tools to control transactions and ultimately social behaviors, a 21st century authoritative government's dream.

What about Bitcoin?

Blockchain-based digital currencies created by governments pose a threat to citizens' right to privacy. What makes Bitcoin's blockchain unique is that no single entity controls how or what transactions are recorded on the ledger. Strip away the permissionless nature of the system, in which anyone can access and innovate upon, and you're left with something like that of China's digital currency. In other words, just an excel spreadsheet used by the government.

Bitcoin's use of a permissionless and decentralized blockchain has given people a way to opt-out of this dystopian nightmare that today's surveillance is creating. Physical cash has been used to preserve the privacy of its users for most, if not all of human history. When a dollar bill for example, is handed to another person, no one else partakes between the two parties. There is no third party in between that can record the dollar bill moving from one hand to the other. That same concept has been brought into the digital world, albeit in a unique fashion, with Bitcoin. Bitcoin is a peer-to-peer digital cash. While sophisticated tracking software for transactions recorded on the Bitcoin Network exist, second layer solutions to the network vastly decrease their

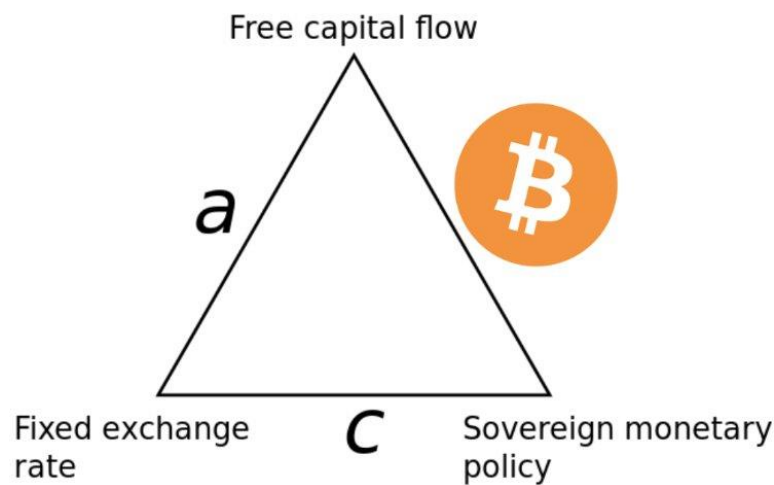
effectiveness. There are multiple implementations being actively worked on that give the users privacy while maintaining the security of the network.

It preserves the benefits of cashlike privacy while being designed for the digital age we live in. Before Bitcoin, every single payment processed had to go through the hands of a digital intermediary as the “double-spend” problem had not been solved. A trusted third party has always been required to prevent the duplication of the cash and maintain the ledger of all transactions. That problem has now been solved, and proven to work during the last decade. Bitcoin may end up taking time to integrate into our day-to-day lives, but we now know a surveillance state is no longer inevitable in the digital age.

Tweet: Bitcoin is the world's only independent central bank

By Pierre Rochard

Posted November 22, 2019

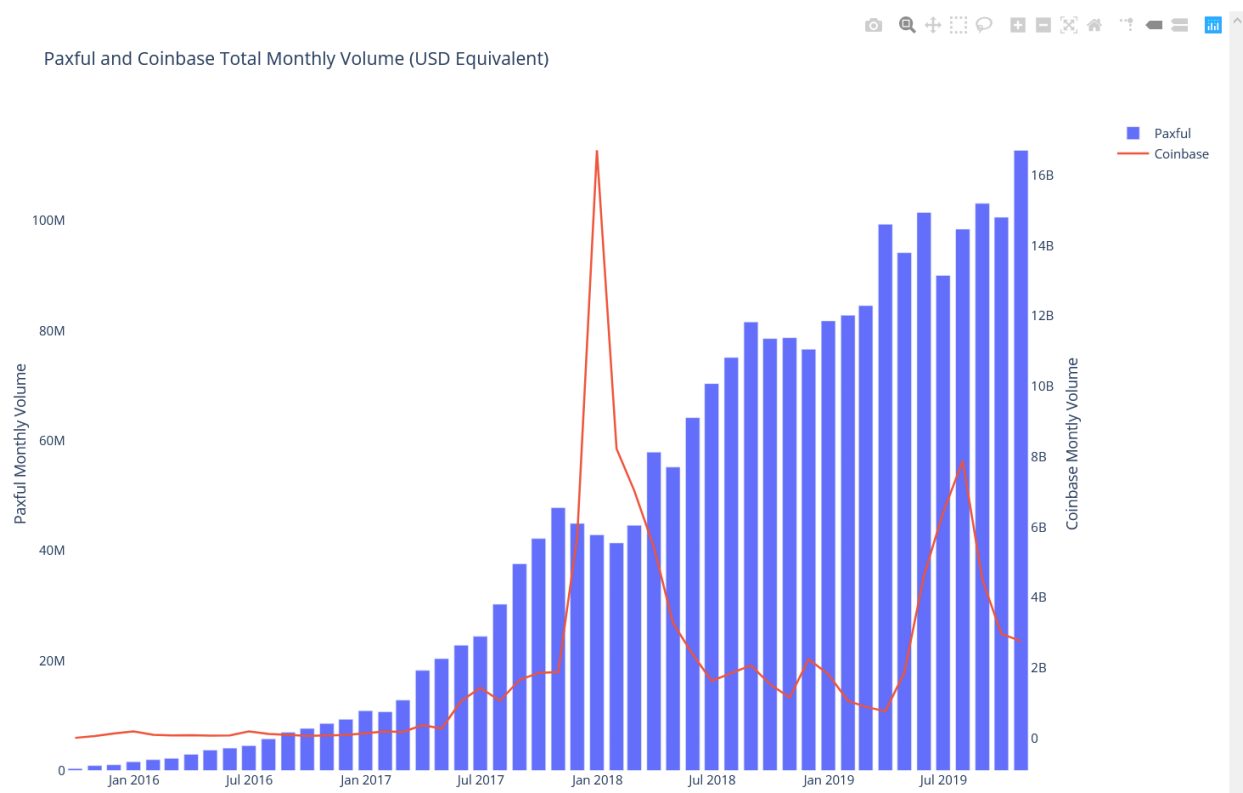


Paxful is the Most Important Bitcoin Company You Aren't Paying Attention to.

By **Matt Ahlborg**

Posted November 25, 2019

If cryptocurrency is the Wild West of money, then Paxful is Deadwood, South Dakota. Settled, errr, founded in 2015, Paxful has slowly but surely grown into a pillar of Bitcoin trading ecosystem. In total, Paxful now employs over 200 people in four offices around the world and oversees the trading of approximately \$25 million dollars worth of Bitcoin every week. And while most cryptocurrency exchanges out San Francisco way are far from their highs reached during the bubble of 2017, Paxful has seen a consistent uptrend for its entire existence.

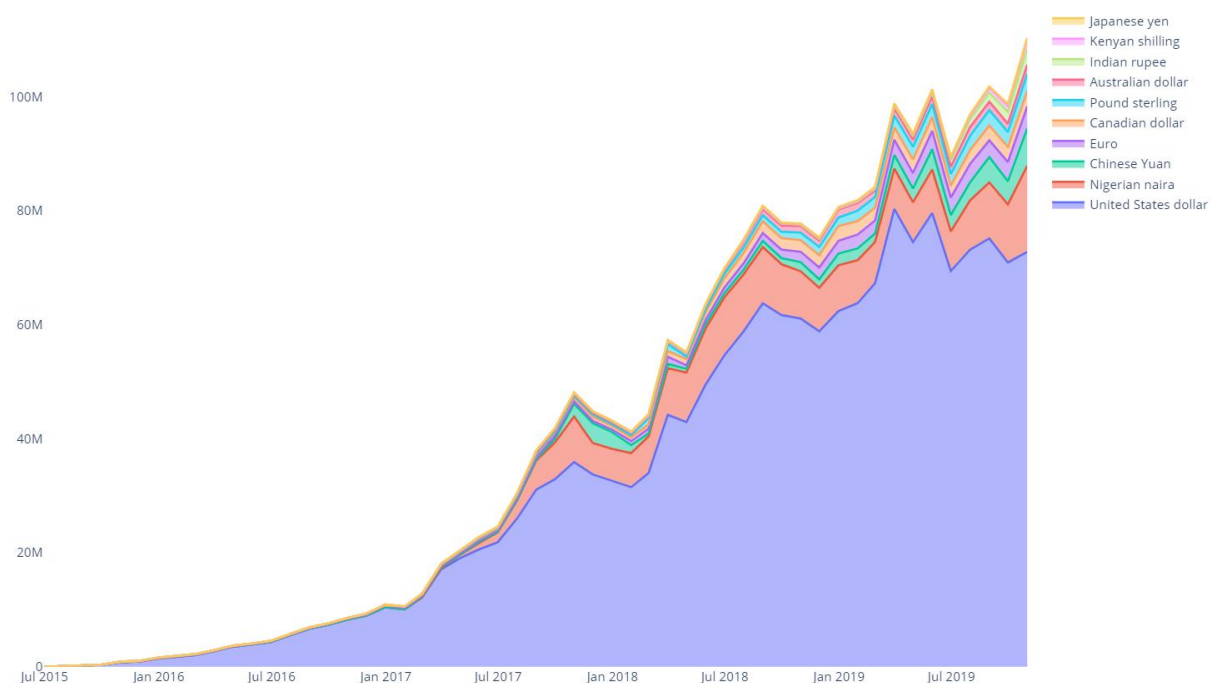


Take note of the two Y axes.

Paxful, like LocalBitcoins, is an online peer to peer (P2P) over the counter (OTC) exchange where peers interface with the advertisements of other peers offering to trade for Bitcoin using online wallets like Paypal, gift cards, domestic bank transfers, and others.

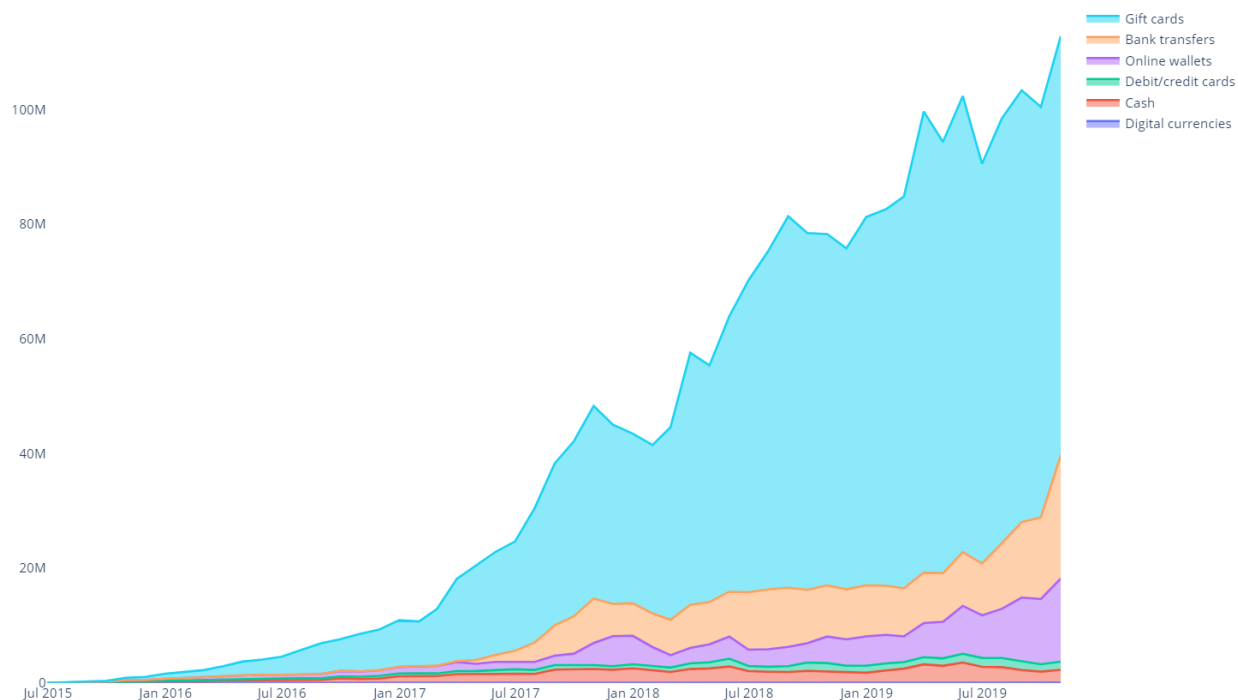
As is the case with most P2P OTC exchange models, Paxful does not custody the fiat or fiat-like wallets, accounts, or instruments (gift cards, for example) used as counterparty to these trades and instead acts as a supervising authority over peers who use these wallets, accounts, or instruments to trade amongst themselves. As such, Paxful does not need to officially connect to the banking or regulatory infrastructure of many of the countries which it operates in. Because of this model, **Paxful is able to onboard financially disconnected citizens of developing countries on a level that non-P2P OTC exchanges like Coinbase simply cannot.** As of this writing, Paxful services trades in more than 70 currencies around the world and has made much of its traction in geographic regions that many bigger exchanges have not.

Paxful Top 10 Currencies by Volume (USD Equivalent)



As shown above, US Dollar denominated transactions are by far the most popular on the platform. However, two thirds of that US Dollar volume is actually attributable to USD denominated gift card trading which, as I will show later in the article, is very international in its nature.

Paxful USD Volume by Payment Group



Online wallets are services like Paypal, Skrill, Zelle, etc. Digital currencies are things like Litecoin, Bitcoin Cash, etc.

So what is the deal with gift card trading then and how does it all work?

The Gift Card Trading Ecosystem

“Gift cards can be seen as a sort of stablecoin which are available for purchase on nearly every street corner in the world.”

Gift cards are a massive market and constitute billions in sales every year. And unlike Bitcoin, gift cards are ubiquitous at nearly every gas station, convenience store, and grocery store. Aside from being an easy, last minute gift on the way to birthday or holiday party, they also have a few other attributes which make them useful in other respects:

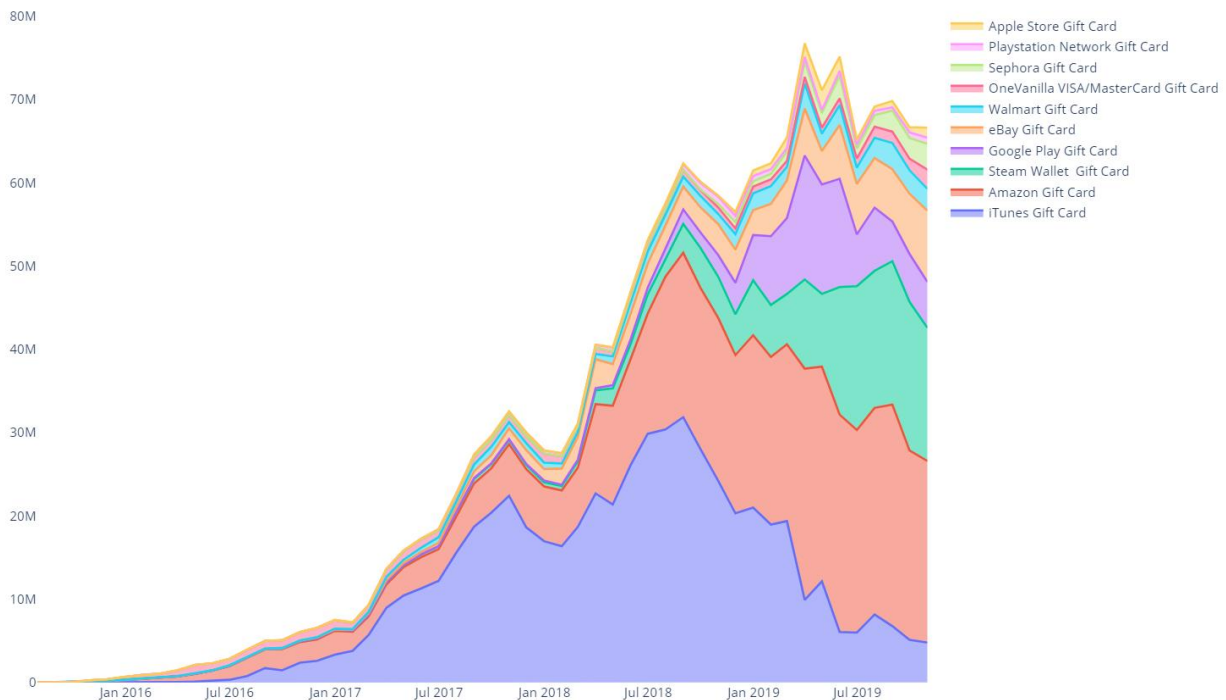


1. You can quickly and easily purchase them with cash,
2. They hold a stable value,
3. The redemption codes on the card can be digitally transferred with a simple picture,
4. It is not illegal to sell your gift card to another person.

In effect, **gift cards can be seen as a sort of stablecoin which are available for purchase on nearly every street corner in the world.** Additionally, as you will find out later in the article, the people using these gift cards as stablecoins often don't even need to know what a stablecoin is or how cryptocurrency works.

So which cards are being brought to Paxful for selling?

Paxful USD Denominated Gift Card Volume by Brand

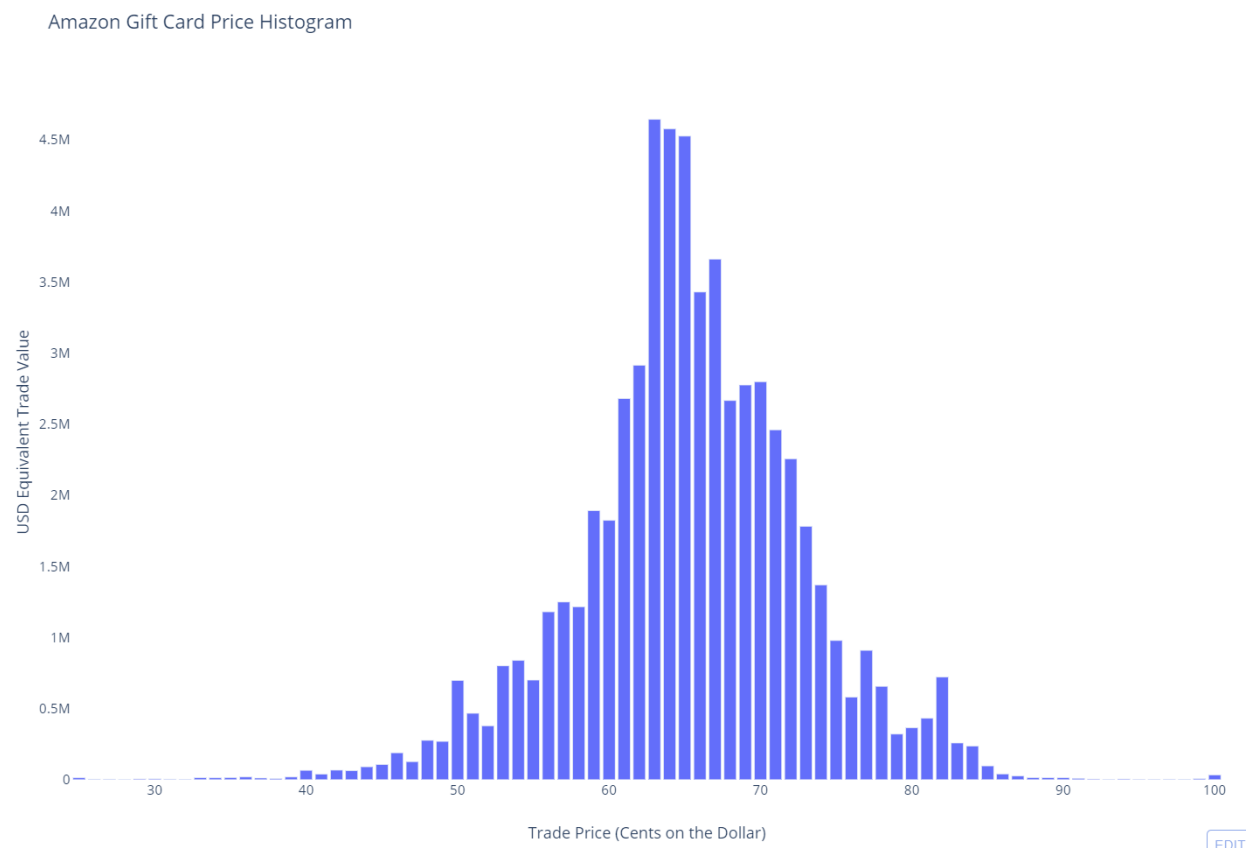


Use the legend on the right to filter out cards and adjust the date range.

Itunes gift cards were the first gift card to come to prominence on the platform. Amazon gift cards and Steam Wallet gift cards have now taken the lead. More recently, a large variety of cards have become popular.

How much are the cards selling for?

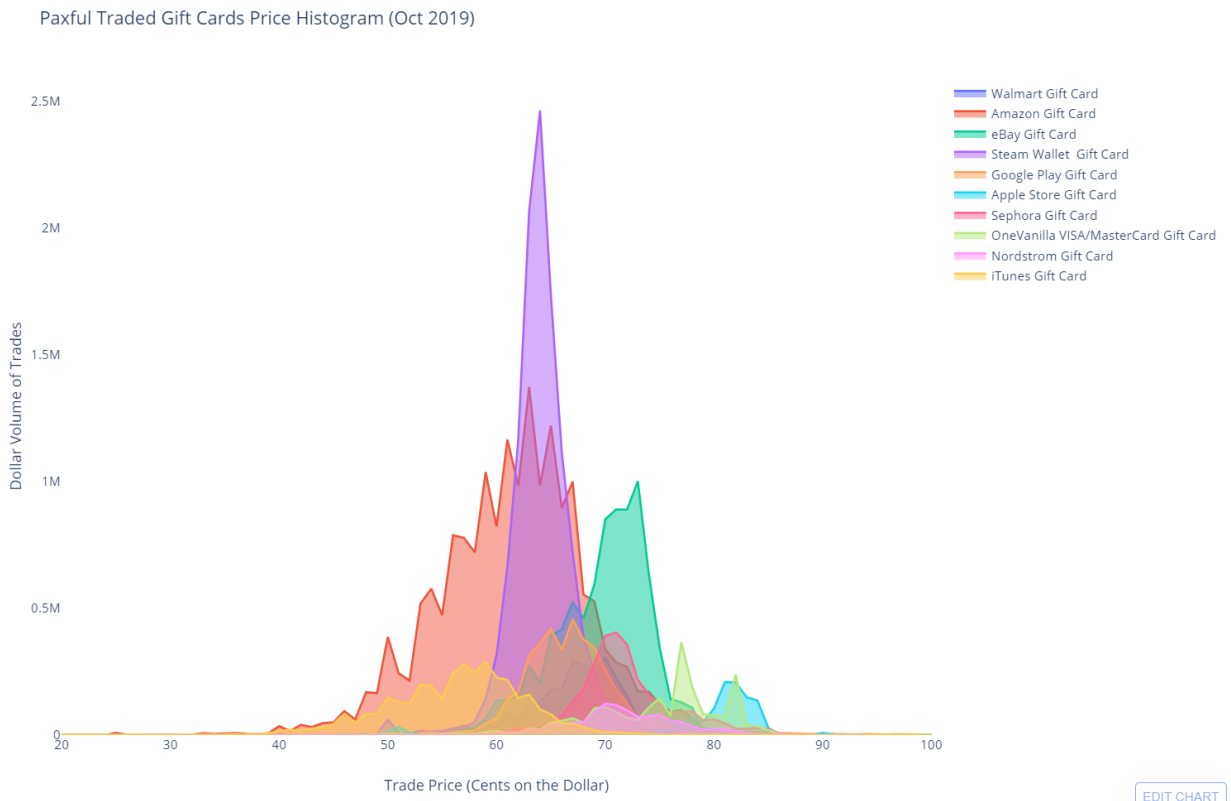
Amazon gift cards are currently the most popular gift card brand on the platform. They most frequently sell for around 64 cents on the dollar (that is, a \$100 card fetches around \$64 in Bitcoin). As shown in the distribution below, Amazon gift cards can fetch a variety of prices:



The price distribution for these cards comes from a variety of factors which effect the chargeback fraud risk that the buyer of the card takes on when purchasing the card. These factors include:

- Whether the redemption code comes from a physical card or a digital gift card,
- The amount of dollars on the card (\$25, \$50, \$100, \$200, etc),
- Whether the card is accompanied by a receipt and whether the receipt confirms the card was bought with cash (cards bought with cash have the lowest probability of a chargeback event to the card buyer),
- The reputation of the account selling it.

Additionally, each brand of card garners a different price on the platform. Below are the trade price distributions of the top ten cards by volume:

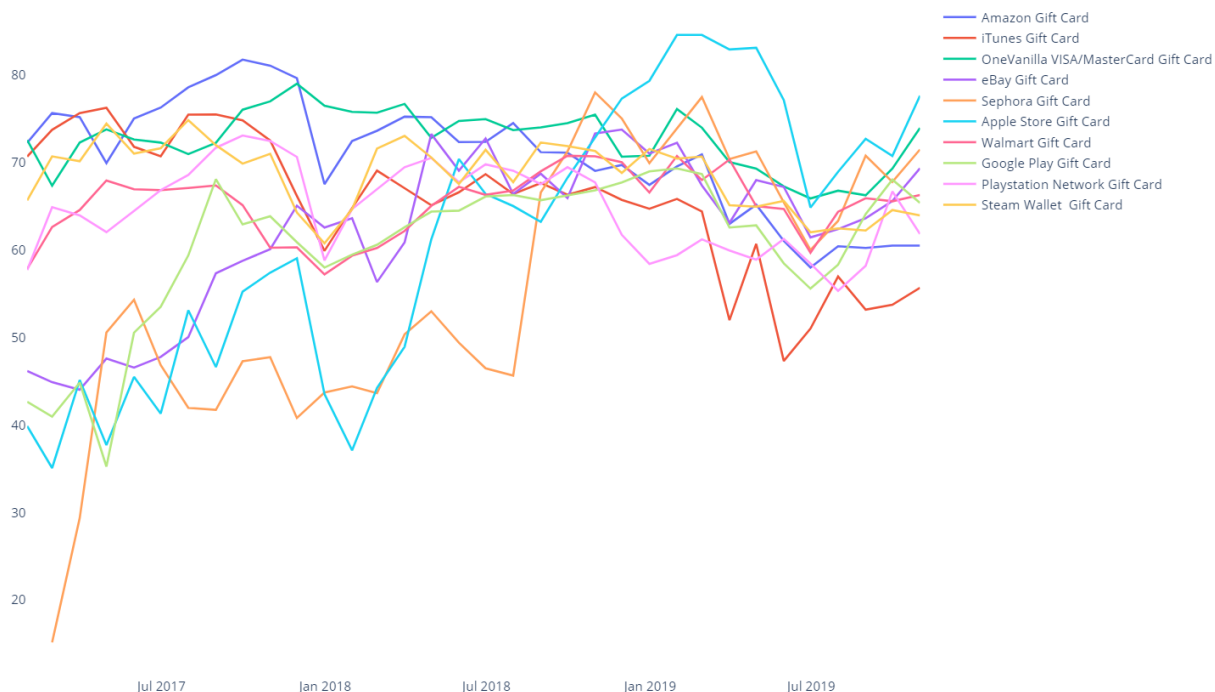


The final price for a given brand of card tends to be a function of:

- The types of items which can be bought with the card,
- The liquidity of that brand of card on Paxful (less common cards tend to sell for lower prices),
- The terms of service related to the redemption of each card (some cards have stricter redemption policies than others, affecting their fungibility).

At the end of the day, the price of every card on Paxful is determined by the collective amount that the people buying the cards are willing to pay. The chart below shows that the average price of a given brand of gift card even changes over time:

Average Cents on the Dollar Received (Top 10 Voluminous Gift Cards)



So who are the people bringing these gift cards to Paxful to sell?

This is one of the most difficult questions I've tried to answer in the course of my research. The reasons for trading a gift card are many and include the selling of unwanted spare gift cards [Appendix 1], online freelancers cashing in their earned gift cards [Appendix 2], and yes, even fraud and/or money laundering activity [Appendix 3]. Based on what I've learned up to now, I am not confident that any one of these use cases accounts for the majority of volume. Rather, I would guess that each may account for some minority portion of the volume.

Of the gift card sellers that I spoke with (as well as those who are buying gift cards from the sellers), **the cited reason for a large amount of the trades is actually remittance**. That is, immigrants in the USA are using gift cards and Bitcoin to transfer value back to their home country. For the next few paragraphs I will explore how this "gift card remittance" process works and then evaluate the data and price points to determine whether or not it could plausibly account for a sizable amount of the volume on Paxful.

Gift Card Remittance on Paxful

"The entire remittance process can be completed in 20-30 minutes with the end result of local Nigerian currency arriving to the family member's bank account."

When you go to Paxful and see advertisements looking to purchase gift cards, gift card buyer advertisements show all sorts of requirements and restrictions on the types of cards they are willing to buy. A large chunk of these advertisements demand the gift card be:

1. A Physical Gift Card,
2. Accompanied by Receipt,
3. Shows that the card was paid in cash on the receipt,
4. Purchased in the last 24-48 hours

Offer terms by owner [REDACTED]

Power Trader

SEEN JUST NOW
REPUTATION: +42222 / -109

Please ask in the chat if I accept the offer before uploading or sending any information.

*****No Ecodes whatsoever*****

The card must be bought with cash and we will not accept cards bought more than 24 hours ago. The receipt and the Amazon card must match. Only 1 card per receipt.

Step 1 - Upload a clear picture of the ENTIRE Amazon card
Step 2- Upload a clear picture of the ENTIRE Receipt
Step 3- Type the code into the chat

I reserve the right to have you verify that you're in possession of the card you are trading. If you are not, the trade must be cancelled immediately

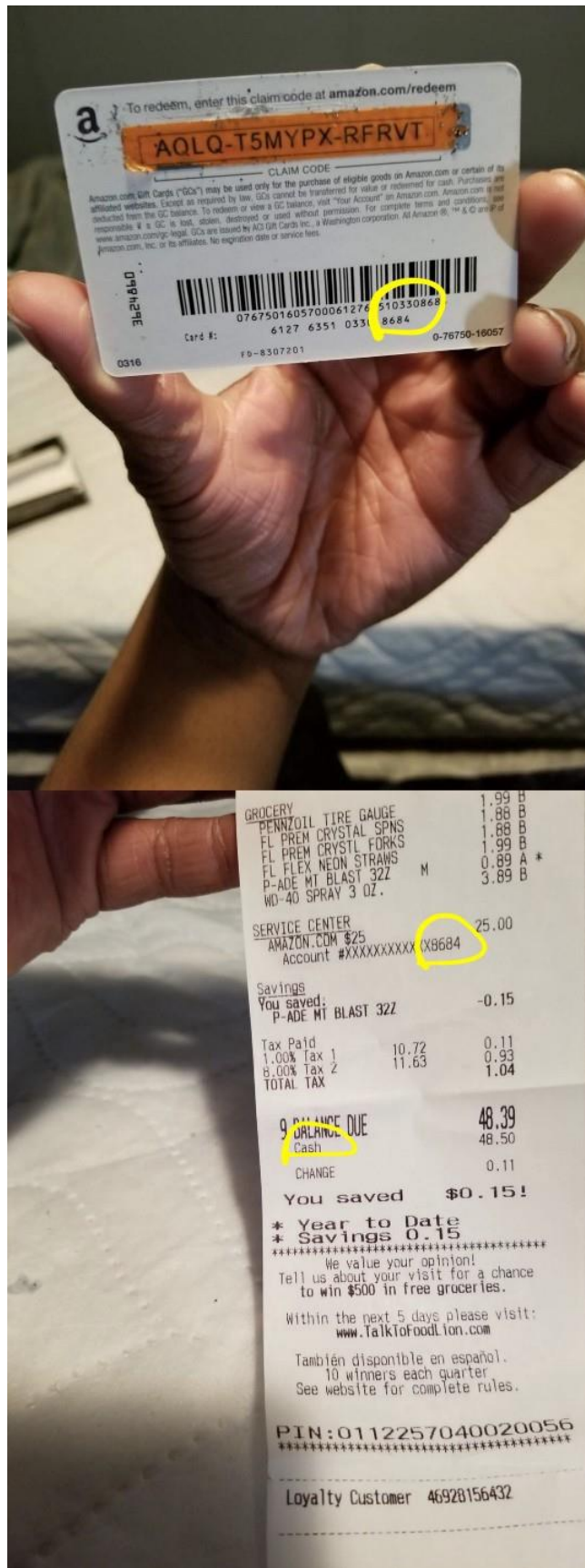
I will release the bitcoin to you once it is verified

I reserve the right to reject all trades that I deem risky

[ACCEPT TERMS AND BUY BITCOINS NOW!](#)

[Report a problem](#)

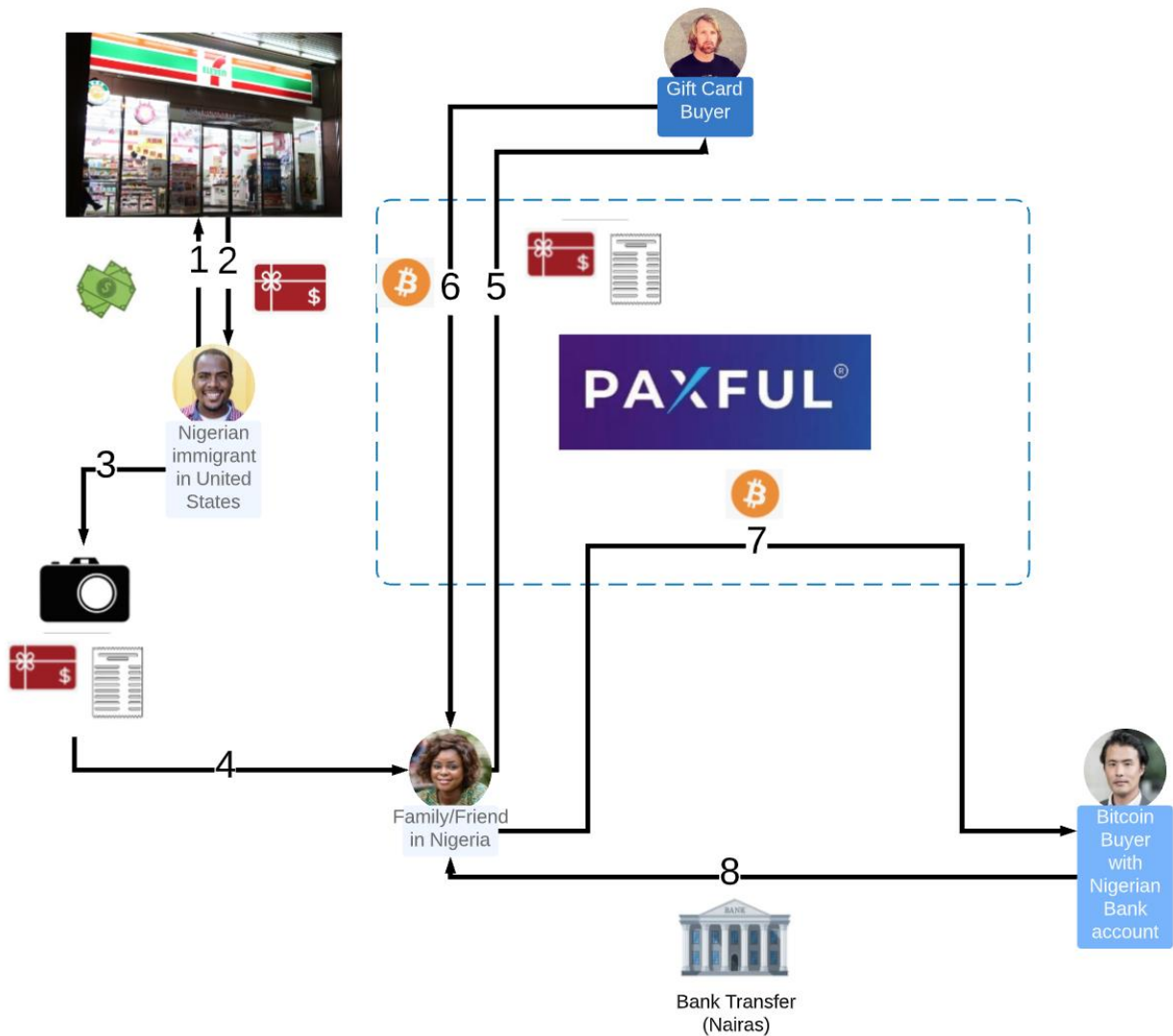
For Amazon gift cards, these advertisements match the 63-83 cent price range constituting the right side of the bell curve on the Amazon gift card distribution above. **What this means is that a large amount of the cards being sold on Paxful are purchased with the specific intent to bring them there to be sold at a substantial discount.**



In speaking with the traders who act as counterparty to those who bring these cash-bought gift cards and receipts, they tell me that the majority of the cards are coming from Nigerians or other West Africans and that their IP address according to Paxful's trading dashboard confirms this. The interesting twist however is that the receipts of these cards show that they were purchased at various convenience stores and gas stations in the USA, often times mere hours before they were uploaded to Paxful.

So what is happening here then? What I discovered is that (mostly Nigerian) immigrants in the USA are purchasing gift cards in the USA, taking a picture of the card and receipt, and then immediately sending those pictures to their family and friends in Nigeria using Whatsapp. Those on the receiving end of the gift card pictures in Nigeria are the ones who then upload the pictures to Paxful. These Nigerians in Nigeria use the gift cards to trade for Bitcoin, and they then turn around and complete a second trade which sells that recently acquired Bitcoin for Nigerian currency through a bank transfer. The whole process is described in the diagram below:

Gift Card Remittance on Paxful



The eight steps of this process are as follows:

1. Nigerian immigrant in USA gives cash to convenience store,
2. Convenience store gives gift card to immigrant,
3. Immigrant takes picture of gift card and receipt with phone,
4. Immigrant sends pictures of gift card and receipt to family or friend in Nigeria,
5. Family or friend in Nigeria gives pictures of gift card to gift card buyer,
6. Gift card buyer gives Bitcoin to family or friend in Nigeria,
7. Family or friend in Nigeria gives Bitcoin to Paxful user with Nigerian bank account,
8. User with Nigerian bank account transfers Naira to family or friend in Nigeria.

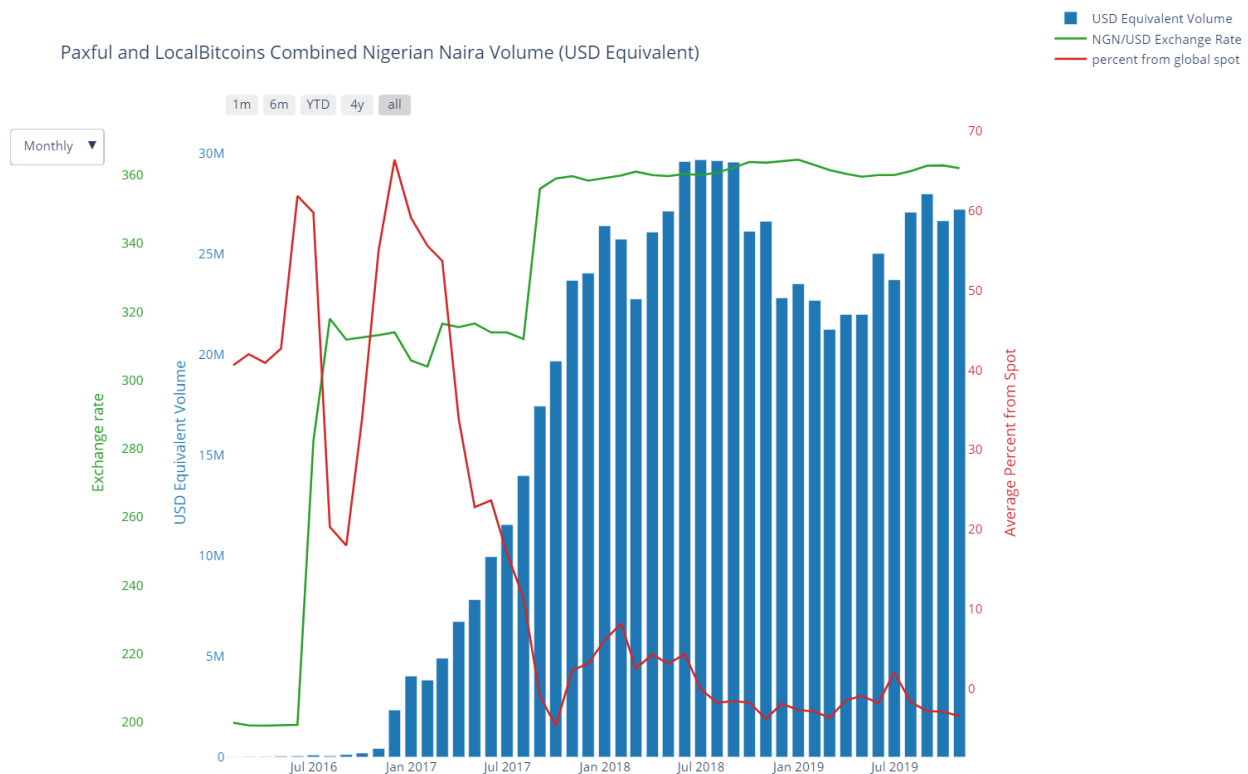
While this process may seem complicated, Nigerians who engage in these trades tell me that **the entire process can be completed in 20-30 minutes with the end result being that local Nigerian currency arrives to the family member's Nigerian bank account.**

Additionally, neither the person sending the money nor the person receiving money needs to stand in line at a remittance counter in either country and the person who sends the money does not even need to know what Bitcoin is or what Paxful is. They just need to know to purchase a gift card, take a picture of it, and send it to their family or friend in Nigeria.

So why is it mostly Nigerian immigrants then? Again, the issue is perplexing, but here is my best attempt at reasoning:

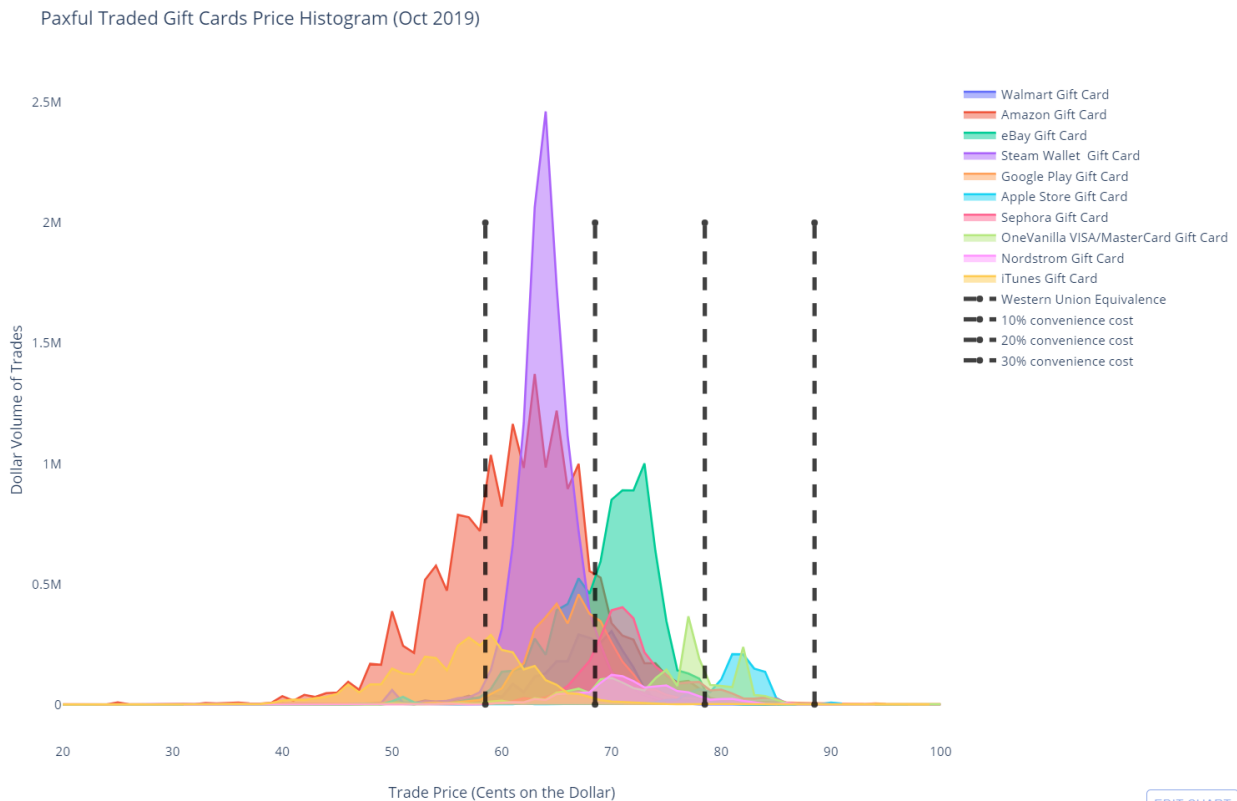
Nigeria's currency, the Naira, has been subject to varying degrees of manipulation and capital controls in recent years and has had a parallel black market rate for some time. In circumstances like these, standard remittance companies like Western Union **have to play by the rules of the local government and honor whatever exchange rate is deemed appropriate there** (instead of the black market rate). When going outside of official channels to remit (using gift cards and Bitcoin for example), remitters are able to sell for the more favorable black market rate instead of the official rate and thus receive more Nairas per dollar sent in comparison to Western Union. Another factor at play here is that during the bull run of 2017, Bitcoin buying options across Africa were very limited and caused a premium on the price of Bitcoin there, again creating favorable circumstances for people who hold Bitcoin (those who are selling gift cards). Together, these factors may have conflated to create an environment in 2017-18 such that **Nigerian immigrants in the US could actually take a 30% loss on the value of their gift card while still achieving more Nairas delivered to their families than any other traditional remittance channels offered.**

If you look at the chart below, you can see how Nigerians were able to sell Bitcoin for tens of percent above the official exchange rate during much of 2017-2018 as Nigeria imposed various sweeping measures in an attempt to control the value of its currency.



However, since that fortuitous time in 2017-18 the situation seems to have changed and that premium appears to have evaporated. More recently, the government of Nigeria has allowed the official exchange rate to float closer to the black market rate and, correspondingly, remittance companies like Western Union have been able to honor exchanges rates at or close to the black market rate as well.

If we compare the two potential remittance methods as it would play out in the present day, a crisp \$100 bill brought to Western Union would yield (after all fees) **32,208 Naira available for pick-up at a Western Union location in Nigeria**. If on the other hand you chose to use the gift card remittance method made possible by Paxful, **you would need to get 88.5 cents on the dollar for your gift card in Bitcoin to get as many Nairas as Western Union would offer** (see Appendix 4 for a full breakdown and calculation). In looking at the “*Top 10 Gift Cards by Volume Histogram*” again, you can see that no gift cards on Paxful are able to fetch 88.5 cents on the dollar. This would imply that gift card remittance is no longer economically viable and that any such continued remittance using gift cards would involve factors other than sheer cost, namely convenience and speed.



Annotations indicate the implied “convenience cost” of using gift cards instead of Western Union.

In the course of my research I purchased several Amazon gift cards on Paxful for 65 cents on the dollar, and the Nigerian counterparties I spoke to cited remittance as the reason. This means that they were receiving 26% less Nairas than the Western Union method. If we are to believe their account then we need to ask ourselves why this use case has continued to play out despite the costs.

In my estimation, the ingrained habit, convenience, and speed of using Paxful for remittance may have caused this use case to persist even though cheaper options may have re-emerged. In other words, old habits die hard and convenience trumps efficiency. The Nigerians I spoken with seemed to indicate as much as well.

In addition to convenience and speed, I've also come up with other reasons as to why gift cards may be the superior remittance method for some:

- Some Nigerians do not live near a Western Union and it appears that Western Union is currently not doing bank transfers to Nigerian bank accounts [Appendix 5]. This means that the only way to receive money via Western Union in Nigeria is to travel to a remittance counter there. Gift card remittance on Paxful however allows for near-instant bank

transfers and so the entire remittance process could be done from the phone of the Nigerian family member in the comfort of their home.

- Gift card remittance (including the final bank transfer step) works 24/7 whereas Western Union only works during business hours of Nigerian Banks (all Western Union locations are inside of banks in Nigeria).
- Another factor may be that undocumented and/or underbanked immigrants in the US may not have or be willing to provide the necessary documents to conduct official remittance.
- While losing this much value to conduct remittance seems crazy, consider the irrational success of payday lending where a significant percentage of customers are 'regulars' and perpetually lose money on the majority of their paychecks over the course of years. Human behavior isn't always rational.
- Nigerians that I've spoke with tell me that in reality, they use a hybrid of traditional remittance and Paxful to meet their needs. Larger transfers of hundreds of dollars tend to go through Western Union or informal Hawala networks whereas smaller, quicker transfers covering unexpected costs at home fall to Paxful.

If you still cannot get past the idea of an immigrant willing to turn \$100 into as little as \$65 worth of Nigerian currency in a single remittance transaction (26% less than Western Union), then we must acknowledge another possible (and previously documented [Appendix 3]) use case playing out here which is that the gift cards being brought to Paxful are coming from nefarious activity, namely West African cyber crime and the associated money laundering that goes with it.

On a related note, it was reported in August of this year that Western Union locations in Texas (home of over 40,000 Nigerian-born immigrants) blocked the sending of money to Nigeria on the heels of a major cybercrime operation in the US which resulted in the arrest of nearly 80 Nigerian nationals. In moments like these, Paxful and Bitcoin are likely answering the call for these disenfranchised communities.

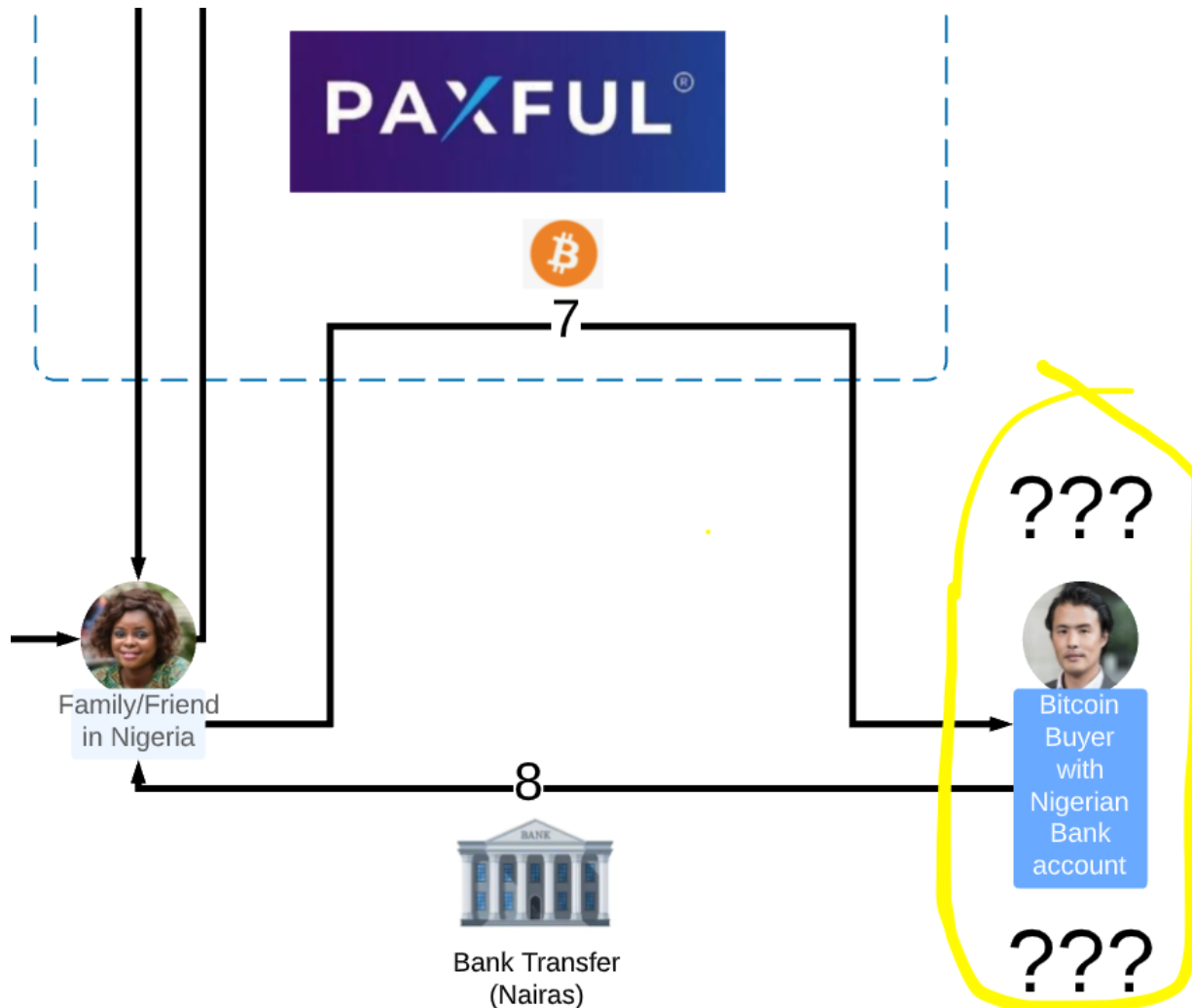


In addition to this single observation of a service outage, based on my reading of the subject over the last few years, Western Union transfers to Nigeria have been unreliable on a few occasions as the company struggles to deal with both the ramifications of anti-cybercrime policy in the USA as well as capital control mandates forced upon them by the Central Bank of Nigeria.

To summarize my thoughts on the viability and prevalence of "gift card remittance" on Paxful, I have definitely observed it happening but I also want to qualify my opinion in saying that the jury is still out in terms of how prevalent it is in comparison to other use cases.

Who in Nigeria needs to trade their Naira for Bitcoin?

Looking back on the “*gift card remittance*” flow chart from earlier in the article, we have yet to touch upon the potential reasons people in Nigeria would want to give away their Naira to acquire Bitcoin. What is Bitcoin offering them?



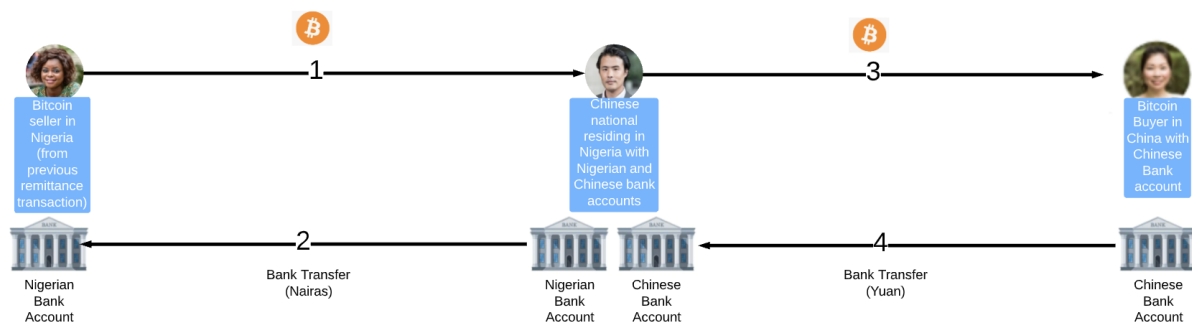
As mentioned before, Nigeria has enacted a number of capital control measures on its citizens and residents. One flavor of these controls allows only permissioned and registered individuals and entities to exchange local Naira for foreign currency. **I believe that a good amount of the people who are acquiring Bitcoin in Nigeria are ones who are not permissioned to trade for foreign currency and who still desire to gain access to it.** These people fall into two groups:

The first group would be local Nigerians who seek to purchase goods on the international market and who use Bitcoin to do so. This use case has been

anecdotal confirmed by Paxful CEO Ray Youssef's customer interactions where he learned that a group of Nigerians were using Bitcoin to purchase, ship, and sell flood-damaged automobiles from the US in Nigeria after the Central Bank of Nigeria clamped down on foreign currency exchange in 2016. I also heard something of this nature several times in the course of my interviews but it instead involved Nigerians purchasing Chinese goods from Chinese vendors who accepted Bitcoin.

The second group of people who seem to have a need for Bitcoin in Nigeria are Chinese nationals. In this scenario, the Chinese people conducting business in Nigeria are filling their bank accounts with Naira but have little recourse in repatriating the value of that Naira back to China due to the aforementioned foreign exchange controls.


In such a scenario, the Chinese national in Nigeria would conduct a P2P OTC transfer on Paxful to trade the Naira in their bank accounts for Bitcoin which they could then use to enter into a second trade to convert their Bitcoin to Yuan in their Chinese bank account. Also, an added bonus here is that Bitcoin now trades slightly below global spot against the Naira and so the transaction is likely also a nice arbitrage opportunity for them [Appendix 6].




Chinese national in Nigeria using Bitcoin to perform a capital flight and/or remittance maneuver

The other side of the trade: Who is buying these discounted Gift Cards and why?




While theoretically anyone could benefit from buying discount gift cards on Paxful for their own personal use, because buying gift cards on Paxful requires a fair amount of risk management, the majority of the discount card purchasing is actually attributable to a smaller group of professionals who perform what is known as dropshipping.





Trust · Block

Ultimate Payment



●

Seen just now

+ 37948

Positive reputation

- 134

Neutral reputation

- 76

Negative reputation

VERIFICATIONS

 Email verified

 Phone verified

 ID verified

INFO

Languages:
English (English)

33089 Trade partners

61135 Trades

Trade volume: **between 300 and 1000 BTC**

Trusted by 2646 people

Blocked by 158 people

Joined 1 year ago

BUY BITCOINS FROM

	Price	Range	Method	Speed
BUY	10079.82 USD	25 USD	Amazon Gift Card — Cash n Fast PHYSICAL CARDS ONLY RECEIPT-REQUIRED CASH ONLY	2 minutes

FEEDBACK (38175)

positive (37948) · neutral (134) · negative (76)



nellyyvee

No message left — +1 positive LOW AMOUNT

Nov 24, 2019

Amazon Gift Card [View offer](#)



Biliboi

Good loader — +1 positive LOW AMOUNT

Nov 24, 2019

Amazon Gift Card [View offer](#)



Ogbajihhfs

Good — +1 positive LOW AMOUNT

Nov 24, 2019

Amazon Gift Card [View offer](#)



Ola2126

Good — +1 positive LOW AMOUNT

Nov 24, 2019

Amazon Gift Card [View offer](#)



Chase004

No message left — +1 positive LOW AMOUNT

Nov 24, 2019

Amazon Gift Card [View offer](#)



Bathyboy

Fast — +1 positive LOW AMOUNT

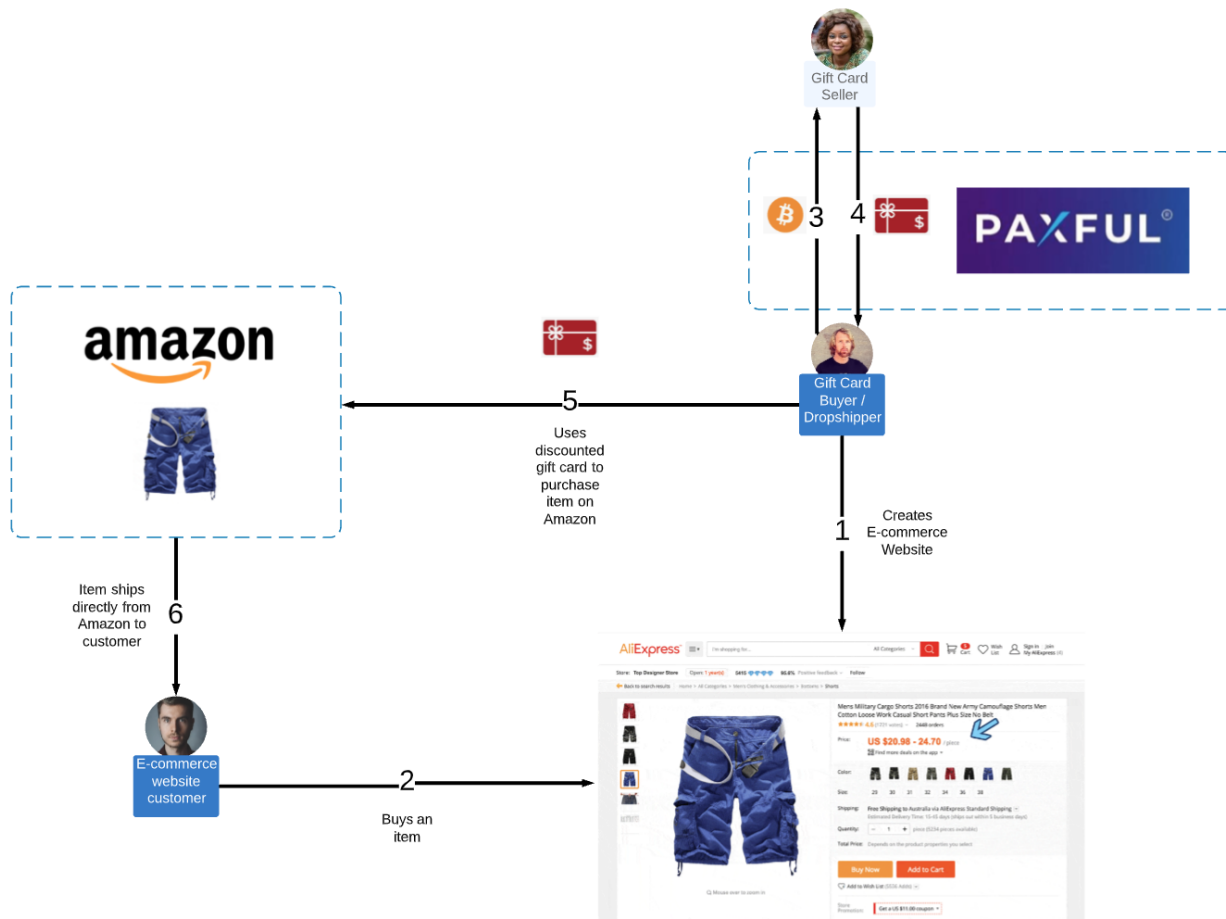
Nov 24, 2019

Amazon Gift Card [View offer](#)

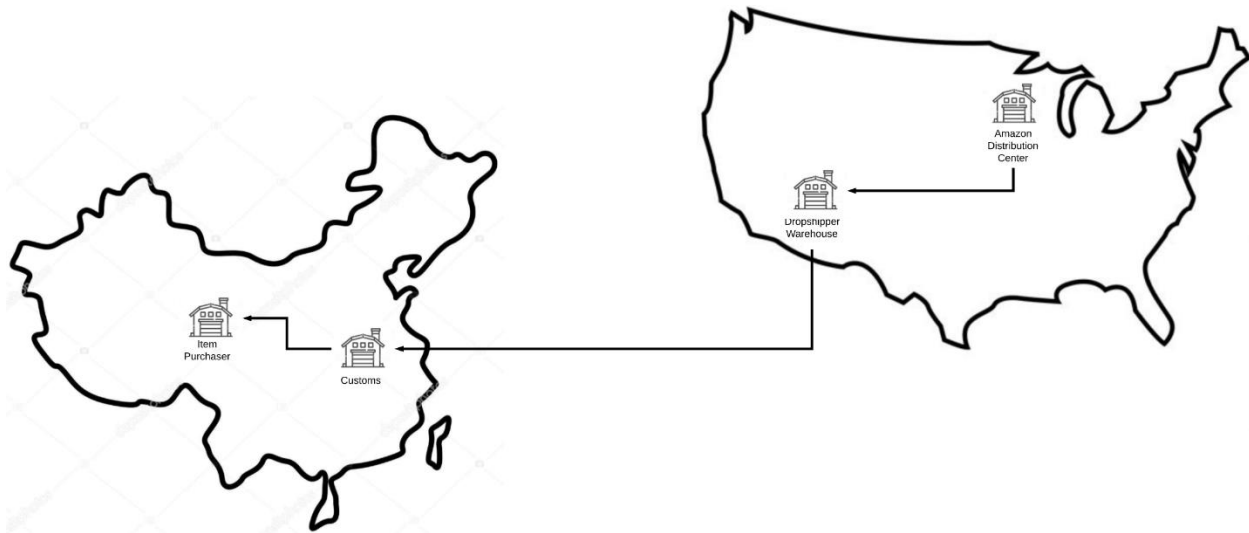
Paxful user who has bought millions of dollars worth of Amazon gift cards

Dropshipping, put simply, is where a business sells items which they do not have in their current inventory. That is, a business will post an advertisement for a particular item online and wait for a customer to come along and buy it. Once the customer elects to buy the item, the dropshipper will purchase the item directly from a supplier and have it shipped directly to the customer. In the context of Paxful and gift card trading, the most simple manifestation of dropshipping is shown in the diagram below:

Drop Shipping with Gift Cards Bought on Paxful



Dropshipping comes in many flavors, however, and can be conducted from any place in the world and to any place in the world. More sophisticated forms on dropshipping involve intermediate warehouses called shipping forwarders and play out on a global scale like this:



Based on interviews I've done with people familiar, dropshipping done with Bitcoin-traded gift cards may primarily be conducted by (1) Americans dropshipping domestically, (2) Asians with American connections/accounts shipping to Asia, and (3) Nigerians with American connections/accounts shipping to West Africa. It isn't exclusively these groups, however, and the model can be done by anyone anywhere.

In light of this dropshipping revelation, it is now clear why certain cards on Paxful are more popular than others. In general, the most popular and voluminous gift cards tend to be ones which can be redeemed for small and shippable items or which are wholly digital (Steam Wallet, iTunes, etc) and therefore globally redeemable. Additionally, I suspect that many of the goods involved in dropshipping are ones which have limited availability in various countries for reasons relating to import tariffs and protectionism.

Dropshipping as a business ranges in sophistication and is talked about at length on a variety of online forums where people strategize how to hide from and/or not upset the terms of service of Amazon or others as well as the best logistics practices, and so on.

Conclusion:

Paxful is truly a showcase of the interesting, beautiful, novel, and bizarre ways that Bitcoin is manifesting itself into our world. While I've focused primarily on gift card trading across the United States, Nigeria, and China corridors, there are many other stories playing out on Paxful as well. I tried my best to use a mixture of both qualitative and quantitative data to bring a full and accurate picture forward, but there are still many stones left unturned. Furthermore, it was a real challenge to get many of these market participants to speak with me because their activity often times fell into a legal grey area and/or were a

form of proprietary knowledge and so at the end of the day I feel like what I've uncovered is only a small representation of the true diversity and scale of these activities. I will also be very eager to learn new lessons from some of my more informed readers regarding the topics that I've covered. :)

In the next two days I will be **releasing the Paxful data to my website, UsefulTulips.org**, with daily updating charts and paired with other data layers for the public to study for themselves. If you enjoyed reading this article please follow me on [Twitter](#) where I regularly post pithy data observations and trends relating to utility use of cryptocurrency around the world. Also feel free to reach out to me on [LinkedIn](#) if you wish to chat there.

And if you would like to contribute to the project, please do so!

3DT599SqPhDakzL4cJ3tnbFTKxVBk3fwvo

Appendix:

1. Americans have tens of billions of dollars in spare gift cards laying around the house. It is a certainty that some of these gift cards are making their way to Paxful for sale. However, there are many other places on the internet where you can sell gift cards at a greater convenience and get a better price so I would think that **Paxful is not the first choice for most regular Americans selling spare cards and probably does not constitute the majority of the volume there.**
2. It is quite common for a freelancer from a developing country to accept gift cards as a form of payment. This isn't because they want the gift cards, rather, it is because it is often times the most convenient and easy way for people in other countries to pay them. Services like Paypal would generally be the first choice for freelancing, but Paypal is not available or heavily restricted in many countries and this includes most of West Africa. In these instances, gift cards are often times the next best thing. In addition to paying professional-level freelancers, there are many websites which use gift cards to pay for what I call **digital micro-services**. These micro-services are related to websites like mechanical turk, swagbucks, surveymonkey, and dozens of others which pay out hundreds of millions of dollars in gift cards every year to earners in developing countries. The interesting thing about freelancing and digital-microservices using gift cards as payment is that **the freelancer receiving these gift cards is fully aware of the fact that they are not spendable in their own country and they instead treat them as fungible stores of value which they can take to places like Paxful to redeem for cash and eventually local currency.**
3. A [report](#) published earlier this year showed that Nigerian based romance scammers were using Paxful to cash out gift cards sourced from their

victims. Additionally, it's also seems possible that Paxful is a tool used in the vast world of credit card fraud.

For a \$100 transfer Western Union offers an exchange rate 3.2% worse than the official exchange and they would additionally charge you an \$8.50 flat fee. After all fees and exchange rate considerations, you would have 32,208 Nairas available for pickup in Nigeria.

Summary	
Exchange Rate ^{2,25}	
1.00 USD = 352.1600 NGN	
Transfer amount	91.50 USD
Transfer fee ^{2,25,26}	+ 8.50 USD
Service time: ¹	In minutes

The following equation shows the equivalent rate that a gift card would need to receive in order for parity with Western Union:

R = Amount of remittance (USD)
 XR = BTC to NGN exchange rate on Paxful
 N = Amount of Nairas received in Nigerian Bank account using Western Union
 GCR = Gift Card Rate

R = \$100
 XR = 365
 N = 32,299

$GCR = N / (R \times XR)$
 $GCR = 32,208 / (100 \times 365)$
 GCR = 88.5%

Source: <https://www.westernunion.com/us/en/send-money/app/price-estimator>

4.

5.

6. Despite the logic of this activity and hearing of it second-hand from Nigerians, I wasn't able to get testimony from a Chinese person in Nigeria who could confirm this.

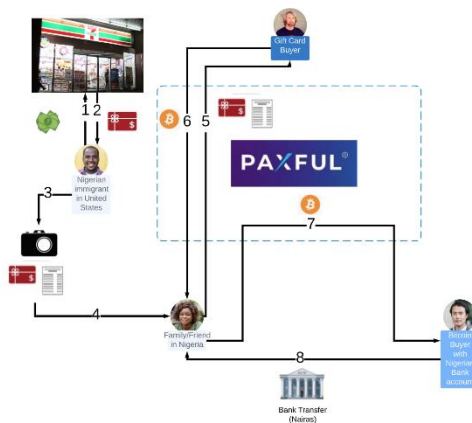
Thanks to my research sponsor [dlab](#), several employees at Paxful for interviews, [Reggie Adaka](#), LocalBitcoins and forex trader of Nigerian origin residing in the UK,

[Eduardo Gomez](#), Head of Support at Purse.io, Venezuelan-born LocalBitcoins trader, and sovereign individual, **several Nigerian gift card sellers including Victor Oluwasegun**, **several gift card buyers/drop shippers**, and [Nick Plante](#) for reviewing my grammar and overall readability.

Also thanks to my data analysis volunteer [Boaz Sobrado](#). We are looking for some front end help with the website so if interested please contact me.

Conflict of interest disclosure:

Paxful has discussed paying me to research and write future articles.



Disclaimer:

WORDS

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

This Journal does not contain reference to any of the investment products or services currently offered by the operator of the journal, that means any business I am associated with. Bitcoin, shitcoins, and related technologies can be volatile. Don't buy what you can't afford to lose and please do your own research.

Bitcoin has paved the way for some VERY radical technology AND it's very confusing. Read more. Ask questions. The purpose of this Journal is to provide archive and curate the best commentary and culture in the bitcoin space.

Nothing within this Journal constitutes investment, legal, tax or other advice. This Journal should not be used as the basis for any investment decisions which a reader may be considering. Any potential investor in bitcoin or shitcoins, even if experienced and affluent, is strongly recommended to seek independent financial advice upon the merits of the same in the context of their own unique circumstances.

Share this journal early and often. Engage the authors and tell them what you think. We sharpen our position through discourse and debate.

DYOR | BTFD | HODL



Thanks for your attention and support. I appreciate your feedback and hope you enjoy this publication.

- @_joerodgers