WORDS

March 2020

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

Contents

Goals and Scope

WORDS is a journal of Bitcoin commentary, established February 13, 2019. Its purpose is to document and advance commentary and research in disciplines of particular interest 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. *WORDS hopes to* continue and expand the tradition established by publications such as the *Journal of Libertarian Studies* and *Libertarian Papers*.

History

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

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

Enter *WORDS*. Published independently, *WORDS* is a journal that welcomes submissions on a range of topics of interest to the Bitcoin 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. *WORDS* is open access, and we encourage readers to "read, download, copy, distribute, print, search, or link to the full texts of these articles...or use them for any other lawful purpose." We want our ideas read, spread, and copied.

Support WORDS

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

Support WORDS

Spread the word

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

Follow us on social media

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

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

Twitter

Subscribe to our newsletter

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

Subscribe

Our pledge

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

A Cover Letter to Ray Dalio

By Hass McCook

Posted February 22, 2020

In this epic piece, Robert Breedlove takes a massive dive into Bitcoin, and presents one of the most solid cases for Bitcoin that's out there.

That said, it's not always easy to get the very busy (and skeptical) Ray Dalio's of the world to sit down for a few hours, so I hope this cover letter can encourage him to have an open mind, and give Bitcoin a few hours of his time. ROI on those few hours could be bigger than any return he's witnessed in his highly illustrious and successful career.

Bitcoin is most definitely not an "easy get". Most ultra-bullish Bitcoiners only become that way due to a deep understanding of the history and properties of money-as-we-know-it, the technology behind Bitcoin, macro, micro and behavioural economics, as well as the dynamics of start-up companies and technologies in bootstrapping themselves and realising network effects. Less technical people observe the IQ density of the space, through its industry leaders and broader development community, which allows for a high level of believability-weighted decision making. I believe you have one of the best grasps of these concepts in the world, so I ask that you humour me for a few minutes to allow me to demonstrate just how much Bitcoin aligns with your personal views and fundamentals. This journey isn't quick — the most dedicated Bitcoiners have put in thousands of hours of research and knowledge development, as well as many hundreds of days "in the saddle" with exposure to the whims of the Bitcoin Rollercoaster. I hope that by the end of this letter you will at least consider revisiting the topic of Bitcoin with a bit more depth.

Bitcoin has been likened by some to be reflective of a startup organisation; currently heading into its Series B fund raise. Bitcoin is a well-oiled "un-organization" with founders but no CEOs, many volunteers but no employees, where the best ideas are developed and implemented by consensus regardless of who proposed the idea, and provably non-diluting equity available to anyone who is willing to trade their energy for it. This is all baked into the code, and it is radically transparent for anyone wishing to participate in the ecosystem. So transparent, that an individual can verify anything they need to about the Bitcoin network by simply running some software on a very basic computer setup in the order of $200 and with the most basic of internet connections. It may likely be one of the best real-life examples of an

Idea Meritocracy at play — the cultural paradigm that you originated at Bridgewater.

Idea Meritocracies are microcosms of what a “truly free” market should be. There aren’t many, if any, examples of free markets in the wild; except of course, Bitcoin. The competition in the Bitcoin space is merciless, where the best products having a shelf-life of months before being made redundant by superior products. Most industry leading service providers will find themselves competing with a free product not long after establishing themselves. As at date of writing, the Bitcoin space even meets several criteria of the “theoretical” perfectly competitive market. Bitcoin’s nature as an open-source, public, encrypted, distributed ledger means that the blockchain guarantees radical transparency, property rights and homogeneity of product, at zero or near-zero transaction and storage cost. The factors of production (labour, equipment, and capital) are mobile to the extent that only a communication link and a power source is required to participate in the ecosystem. Developing on top of Bitcoin requires no permission, and if entrepreneurs have a good enough idea, securing start-up capital is not a difficult barrier to entry to overcome. Information asymmetry, low number of market participants, and externalities from use of non-renewable energy to mine will all be resolved in time, most likely by the end of this decade. The critical thing to note is, although there are relatively few people who own the majority of Bitcoin now, once Bitcoin is spent in the future during the redistribution phase, it is spent forever — there are no reprints. If you want your Bitcoin balance to stay the same or increase, you must be creating value for someone. There is no free lunch with Bitcoin.

A central tenet of your school of thought is open-mindedness, and I encourage you to suspend disbelief and allow yourself to be immersed in high quality Bitcoin content; whether through attending a Bitcoin-only conference, books, podcasts, or even attending your local casual Bitcoin meetup. When meeting Bitcoiners in the real world, you are guaranteed to witness more IQ packed into one small place than you have ever witnessed in your life. Bitcoin was created and fostered by the most radically open-minded, and the development of its technology over time was only possible through radical open-mindedness in the developer community, and of the wider user community once improvements were thoroughly scrutinised and ready to be implemented.

I’m sure that a lot of these arguments have hit home — after all, you personally coined the majority of the arguments I used to present The Case for Bitcoin. It is daunting and confusing to step into such a revolutionary realm, but you will find that if you are willing to radically open your mind, your fundamentals are 100% aligned with Bitcoin’s.

Bitcoin Price Will Always Be Too Expensive if You Don't Believe in Its Revolution

You need to be able to make a decision, and then take action.

By Sylvain Saurel

Posted March 1, 2020

Inlife, there is nothing worse than hesitation. I often see people spend a lot of time hesitating before they finally never take action. These people always imagine that there might be a better time. They wait for the perfect moment, which never comes.

These people somehow make the choice to live with regrets about the actions they might have taken.

With Bitcoin, I have a feeling that a lot of people have been going through the same thing for several years now. When Bitcoin price was $1K, they were reluctant to buy it because they thought Bitcoin was too expensive.

It was the same thing when Bitcoin reached $2K, then $3K, and finally $5K. Many of these people then literally jumped on Bitcoin when it reached $20K at the end of 2017.

Today, Bitcoin is around $8.5K after reaching $10K in early February 2020. This sudden drop in price is once again questioning these hesitant people. At the heart of their hesitation is the same question that comes up again and again:

Is this a good time to buy Bitcoin? Is its price too expensive?

I'm going to disappoint some people, but the reality is that Bitcoin will always be too expensive if you're one of those people who don't fundamentally believe in it.

I will explain why in this story.

A Lot of People Are Thinking About Buying Bitcoin

With the approach of the third Bitcoin Halving, and an excellent beginning of the year for Bitcoin price, many people began to wonder if they were missing the Bitcoin train.

When Bitcoin surpassed $10K on February 9, 2020, many people began inquiring about buying Bitcoin.

The same people who weren't interested in Bitcoin when it was $3.3K at the end of 2018, became interested in Bitcoin when it reached $10K.

How do you explain this strange psychological phenomenon? Quite simply by the feeling of FOMO (Fear of Missing Out).

These people are non-believers who are simply afraid of missing out on the Bitcoin opportunity. They've been thinking about buying Bitcoin for months, even years, but never dare to take action.

Any excuse is good for not taking action now by buying Bitcoin.

Bitcoin would be too complicated if you listen to them. There are risks of losing what you own. There are no guarantees on your Bitcoin like you can have guarantees with your fiat currency stored in a bank account.

This list is far from exhaustive, but is representative of what many people will tell you to justify not taking action by buying Bitcoin.

These People Are Always Waiting for the Best Time to Buy Bitcoin

In addition to these justifications, people who hesitate will tell you that Bitcoin is too expensive. They are waiting for the best time to buy Bitcoin. To these people, I often say the following:

On what do you base your opinion that Bitcoin is too expensive?

When Bitcoin price is $10K, and you choose not to buy Bitcoin, what criteria do you think it is too expensive based on?

Generally, you think Bitcoin is too expensive because its price was $3.3K at the end of 2018. At the end of 2018, you had doubts about the $3.3K price because Bitcoin was in the middle of a very strong and prolonged bear market.

In 2017, when Bitcoin started the year at $900, you weren't even paying interest on it.

Indeed, Bitcoin seemed to you at that time to be simply a system for geeks who dreamed of revolutionizing the current monetary and financial system.

You became interested in Bitcoin when the media started talking about it when its price exceeded $2K in June 2017.

Rather than trying to understand why Bitcoin was a revolution, and how it worked, you simply told yourself at the time that you were going to wait until it dropped below $1,000 to buy it.

And then, Bitcoin's price soared to $10K by the end of November 2017.

At each additional step up, you have been psychologically blocked by thinking that if Bitcoin was worth $900 at the beginning of the year, it was too expensive today when its price was $10K.

When Bitcoin surpassed $15K in December 2017, you finally took the plunge for fear of missing the train. Bitcoin quickly reached $20K in a hurry, and you felt reassured.

The speculative bubble that formed around Bitcoin price as a result of this widespread euphoria burst throughout 2018, and you panicked.

You capitulated and sold your Bitcoin in early February 2018 when its price fell below $10K.

You lost a lot of money. This prevented you from buying Bitcoin again when it was at $3.3K.

There's No Such Thing As the Best Time

Generally speaking, there is no such thing as the best time to take action in life. You will always find a reason to wait. And by the time you do, it will really be too late.

You will take action because you will be affected by what happens, not because you have decided to.

Then you will be in a worse position than if you had taken action right away when you were offensive.

Since there is no such thing as the best time, it is up to you to create the perfect conditions. These conditions are created when you take direct action with a positive mindset.

With Bitcoin, it's exactly the same thing.

There is no better time to buy Bitcoin. Bitcoin wasn't too expensive at $3K, just as it wasn't too expensive at $10K or $20K.

Bitcoin Will Always Be Too Expensive if You Don't Believe in It

In order to be able to judge what a correct price for Bitcoin might be, you need to understand what Bitcoin is. Once you understand how Bitcoin works, and how it is a complete paradigm shift from the current monetary and financial system, you will be better able to judge its price.

You still won't be able to say whether its price is too expensive or not, because no one really can, but you will understand that all your questions about its price are useless at the moment.

Bitcoin is limited to 21 million units. This is true today, and will still be true in 10, 25 or 50 years from now.

There are currently 7.8 billion people on Earth. When there are 10 billion people on Earth around 2050, there will still be 21 million Bitcoins available.

If you believe in the Bitcoin revolution, then you will realize that this is at most 1 Bitcoin for every 476 people on Earth.

That is very small. So the demand for Bitcoin is going to explode. With the extreme scarcity of Bitcoin, you don't have to be an expert in the law of supply and demand to understand that Bitcoin price will literally explode.

An interesting exercise then consists in comparing Bitcoin and its $160 billion capitalization with the valuation of other markets:

- The world's gold stock is the equivalent of $8T
- The global capitalization of the stock market, which reached $73T
- The global money supply that reaches $90T
- The global real estate market reaching $228T as a whole
- The global debt which is astronomically high at $246T

The first thing that stands out is that the capitalization of Bitcoin is currently negligible in comparison to these other markets.

Then, let's imagine for a moment that the capitalization of Bitcoin reaches the equivalent of the global amount of money in circulation, that is $90T.

Applying a simple rule of three, this would give us a price of about $4.2 million for one Bitcoin.

This figure may sound crazy to you, but it clearly isn't if you have complete confidence in Bitcoin and what it is trying to build for the future.

With such a level of confidence in Bitcoin, you will easily be able to take action whether Bitcoin price is $3K or $10K.

On the other hand, if you don't believe in Bitcoin, its price will always be too high, and you will never take action.

Bitcoin Rewards Those Who Truly Believe in It and Take Action

Bitcoin has been advancing at its own pace since its creation by Satoshi Nakamoto on January 3, 2009. It has proven to be a special case since its price is not correlated to any other asset.

Day after day, block after block, Bitcoin continues to move forward in building a fairer and freer world for all in the future.

Launched in complete anonymity, Bitcoin has become in just over 11 years the only credible alternative to the current monetary and financial system.

Bitcoiners are growing in numbers, and even its fiercest opponents are really starting to fear it. This is the ultimate proof that Bitcoin continues to move in the right direction.

Once you've taken the time to understand what Bitcoin is, and why the total paradigm shift it proposes is a revolution, you will clearly no longer have any doubts. You will be able to truly believe in Bitcoin.

If you have complete confidence in Bitcoin, you won't find its price too expensive, and you'll be able to take action to buy it whether its price is $3K, $10K, or even $20K.

If you don't trust Bitcoin, and that is your right, it will always seem too expensive to you.

A psychological brake will always prevent you from taking action, and you may have regrets in the future when you realize that you missed the Bitcoin train.

It's up to you to know what you want to do for your future with full knowledge of the causes.

Bitcoin's Habitats

How Bitcoin is surviving and thriving between worlds

By Gigi

Posted March 1, 2020

As I have argued previously, Bitcoin is a living organism. But where does this organism live, exactly? As with many questions in the world of Bitcoin, exact answers are hard to come by. Living things have fuzzy edges: beginnings and endings are hard to pin-point, differentiation is more-or-less arbitrary, and what was classified as a wolf today might evolve to be a dog tomorrow.

Bitcoin has no rigid specification, no absolute finality, no fixed development team, no final security guarantees, no scheduled updates, no central brain, no central vision, no kings, and no rulers. It is a ***decentralized*** organism, organically evolving without central planners. The lack of any centralization is the source of Bitcoin's beauty, it's organic behavior, and it's resilience.

Bitcoin is everywhere and nowhere, which makes figuring out where this thing lives a daunting task. However, it turns out that there is a space it lives in. Multiple spaces, as we shall see.

The Habitats of Bitcoin

While classifying the habitat of a decentralized organism isn't trivial, we can look at the constituents of Bitcoin to make the task a bit easier. As outlined in the last article of this series, Bitcoin lives across domains, with one foot in the purely informational realm (ideas and code) and one foot in the physical realm (people and nodes).

An awareness of Bitcoin's environment(s) might help to better understand this new form of life. No organism can be meaningfully studied in isolation, and Bitcoin is no exception. As Alan Watts pointed out, one has to be aware of the basic unity every organism forms with its environment.

"For the ecologist, the biologist, and the physicist know (but seldom feel) that every organism constitutes a single field of behavior, or process, with its environment. There is no way of separating what any given organism is doing from what its environment is doing, for which reason ecologists speak not of organisms in environments but of organism-environments." Alan Watts

With that in mind, let's take a closer look at the organism-environment(s) we are dealing with. As outlined above, Bitcoin's ideas and code inhabit one realm, and Bitcoin's people and nodes inhabit another. To stick with tradition, let's call the physical realm "**meatspace**" and the purely informational realm "**cyberspace**" — even if, as always, the lines might be fuzzy around the edges.

The "soul" of Bitcoin, so to speak, lives in **cyberspace**. There, Bitcoin absorbs useful ideas and incorporates them into its code. As with all living things, something is ***useful*** if it helps an organism to survive. While Bitcoin has various self-regulatory mechanisms to react to the environment, new ideas may be necessary for survival if changes are drastic enough.

The "body" of Bitcoin, like all bodies, is living in **meatspace**. Nodes, hard drives, cables, and other things come together in an intricate dance, pushing

around electrons, changing zeros to ones and vice-versa, making sure that Bitcoin's heart beats about a thousand times a week.

Living things have an interest in staying alive, and the Bitcoin organism is no exception. Bitcoin found an ingenious way to ensure that it stays alive: it pays people, as Ralph Merkle pointed out. People — and increasingly, organizations — are incentivized to keep it alive. They shape the physical world to Bitcoin's liking, feed it energy, renew its hardware, and update its software to keep it alive.

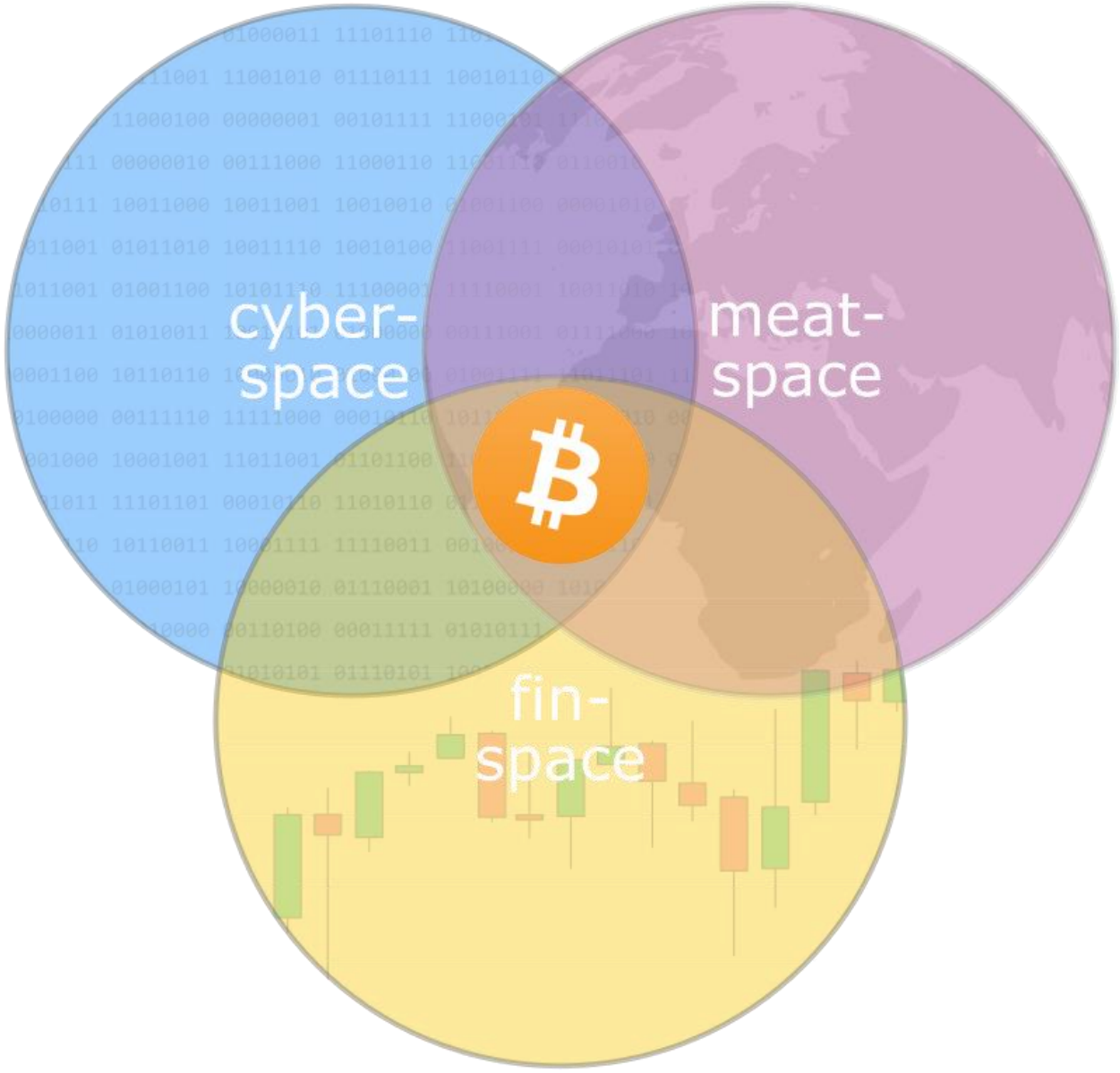
The fact that Bitcoin pays us to keep it alive opens up a third space: a space of financial transactions, value, and mutual beneficial exchange. Let's call this space "**finspace.**"

To understand finspace, we will have to examine the other side of this coin. So far, we only examined the side with an uppercase B: the Bitcoin network. But there is also bitcoin — with a lowercase b — which is the unit of value itself, brought into existence by every copy of the ledger.

These bitcoins, while deeply embedded in the amber of the ledger, are traded worldwide on various markets and marketplaces. And since these bitcoins — and their value — are critical for Bitcoin's survival, we will have to recognize finspace as the third space this strange beast lives in. Note that finspace, strangely enough, is solely inhabited by bitcoin with a lowercase b.

In total, we can identify three distinct environments which the Bitcoin organism inhabits:

- **Cyberspace**: the world of ideas and code.
- **Meatspace**: the world of people and nodes.
- **Finspace**: the world of value and markets; the world of dollars and sats.



Understanding these habitats becomes increasingly important, especially as the climate in one — or more — heats up.

The Climates They Are A-Changin'

The three spaces outlined above — cyberspace, meatspace, and finspace — have different restrictions; different climates, so to speak. In short: they operate under different rules. Once these rules change drastically enough, people will say that "the political climate is heating up" and reports on "the coming financial climate" will be written. Citizens will be unable to speak and act freely. If things change drastically enough, people will rise up in protest, or, if all else fails, flee.

Cyberspace: While we don't have precise words for it, it is obvious that the climate in cyberspace has changed quite drastically in the last two decades or so. The idealistic, utopian ideas which were the foundation of most of the internet were perverted by the advertisement-driven surveillance companies which are the giants of today.

People and politicians are slowly waking up to the strange reality we are living in: the fact that Facebook can manipulate moods and sway elections is as disturbing as the fact that Google knows you better than you know yourself. Edward Snowden showed that the most paranoid netizens were right all along: everyone in cyberspace is under constant surveillance, without suspicion, by default.

While the western world does not immediately ***feel*** the repercussions that come with living in a constant state of surveillance, Chinese citizens are gathering first-hand experience with each passing day.

In the western world, the consequences are advertisements which range from annoying to spooky. In China, the consequences are frozen bank accounts, an inability to buy train or plane tickets, elimination of creditworthiness, automated fines for trivial offenses, and more. Voicing the "wrong" opinion — online or not — can lead to restricted access to schools, hotels, and jobs. And after ruining your life with the flip of a bit you will be publicly named as a bad citizen and the government will take away your dog. If that doesn't sound dystopian enough for your taste I bet that it will be in a couple of years. Remind yourself that this is only the beginning.

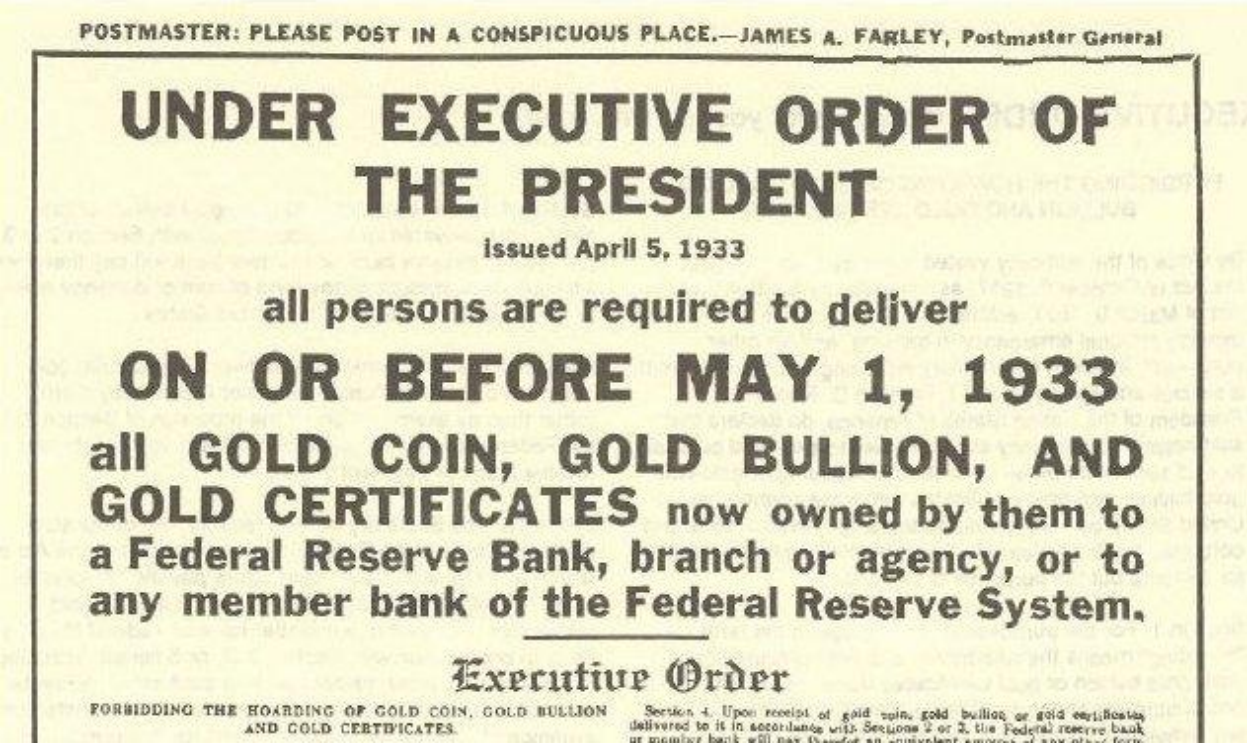
In the "free" world, things are more subtle. Multiple efforts are underway to curb net neutrality, the very cornerstone of the internet. Legislation is being passed which is inherently incompatible with the laws of cyberspace. It seems like the last battle of the Crypto Wars is yet to be fought as politicians are calling for "responsible encryption" and the ban of certain CAD files. Companies are in charge of the speaker's corners of cyberspace and are making arbitrary decisions on what can be uttered by whom and what is off-limits.

Bitcoin knows no borders, no jurisdictions. However, it has to conform to the laws of cyberspace — and if these laws change, e.g. if large parts of the world block Bitcoin traffic and/or the usage of TOR, the Bitcoin organism will have to adapt.

Meatspace: Meatspace climate differs wildly from jurisdiction to jurisdiction. Some bastions of freedom still exist, but once you try to board an international flight it becomes obvious that your right to privacy and your freedom to bring a bottle of water with you are null and void.

Protests across the globe indicate that the powerless are fed up with the powerful, who do everything they can to stay in control and solidify their positions of influence.

History shows that governments do not shy away from using their power. In 1933, Executive Order 6102 was signed, effectively forcing the whole population of the United States to hand over their gold and gold certificates to the government.



POSTMASTER: PLEASE POST IN A CONSPICUOUS PLACE.—JAMES A. FARLEY, Postmaster General

UNDER EXECUTIVE ORDER OF THE PRESIDENT

issued April 5, 1933

all persons are required to deliver

ON OR BEFORE MAY 1, 1933

all GOLD COIN, GOLD BULLION, AND GOLD CERTIFICATES now owned by them to a Federal Reserve Bank, branch or agency, or to any member bank of the Federal Reserve System.

Executive Order

FORBIDDING THE HOARDING OF GOLD COIN, GOLD BULLION AND GOLD CERTIFICATES.

Section 1. Upon receipt of gold coin, gold bullion or gold certificates delivered to it in accordance with Sections 2 or 3, the Federal reserve bank

Yes, seizing bitcoin is way harder than seizing gold — in some cases even impossible. But it would surprise me if those who currently control our money — the governments and central banks of this world — would simply roll over and let Bitcoin march on unhindered. Governments have a monopoly on violence, and they are able and willing to abuse this violence in their own interest.

With Bitcoin, however, people can flee a country with their wealth intact. While this is definitely not easy, and not something I would wish on anyone, it is now possible.

Finspace: Where should I even begin? The current, debt-based financial system has an appetite for printing money which is beyond belief. Quantitative Easing (QE), Negative Interest Rate Policies (NIRPs), currency wars, hyperinflations, and a looming recession are just a few of the recipes of the global instability soup which is currently brewing.

The current financial system seems so far removed from common sense and reality, that all the jargon in the world won't be able to stabilize this house of cards. People know that our money is broken, which is why they flee to buying real estate, stocks, and all kinds of complicated financial constructs to preserve their wealth. In the current system, you have to be an investment expert just to hold your value.

And we haven't even talked about the looming recession, and the virtual inevitability of the next financial crisis yet. Yes, governments might be able to kick the can down the road by printing ever more money. But no road is endless, and the experiment which is fiat money will come to an end, one way or the other.

How bitcoin will react to a catastrophe in finspace is anyone's guess. Some people might flee from their failing fiat currency into bitcoin, using it as a risk-off asset. Others might sell bitcoin to buy something they consider more stable, such as real estate or land. A rising number of people will identify bitcoin as the best money we ever had, shunning other assets and other monies on the quest to stack as many sats as they can.

However it might play out, Bitcoin is the cure for many of the current system's ills. It is hard money which doesn't devalue over time. It is an incorruptible system which forms the basis of a new financial reality.

"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." Ralph Merkle

In addition to the above, it seems to have many indirect effects. It lowers the time preference of those who use it. It incentives users to have better personal and operational security. It incentives individuals and companies to have better digital hygiene. It propels the development of chip manufacturing and encryption technology.

While Bitcoin definitely influences its environments and vice-versa, how Bitcoin reacts to drastic changes is yet to be seen.

Migration

Bitcoin lives on the internet, as Ralph Merkle points out. The internet, however, is not a necessary requirement for Bitcoin to work. Bitcoin is text — pure information — and every system capable of transmitting (and storing) information is a potential habitat for the Bitcoin organism. The internet just happens to be the most suitable habitat which currently exists, since it is the most efficient system to transmit information we have to date.

Cyberspace: The Bitcoin organism *could* migrate to other environments, and multiple efforts are underway which enable Bitcoin to spread to places where

access to Internet infrastructure is limited or non-existent. As of this writing, Bitcoin transactions (and LN invoices) have been sent via radio waves, mesh, and satellite networks — just to name a few. All of these can be seen as Bitcoin conservation efforts, so to speak.

Whether we will see the migration of Bitcoin to another system in the decades and centuries to come depends, in essence, on whether the internet will remain a suitable habitat or not. If the online climate changes drastically enough, we might see the migration to even more resilient, less restrictive environments.

Meatspace: We can already see that mining facilities pop up where energy is cheapest or even stranded. In essence, mining is done where it makes the most sense — economically speaking. The same is true for running nodes. If people can run nodes at low risk and near zero marginal cost, they will. Thus, visualizing Bitcoin on a map, nodes and mining facilities migrate geographically from unfriendly places to friendlier places over time. Unprofitable mining facilities will shut down, profitable mining facilities will go online. The same, again, is true for nodes.

Public bitcoin nodes. Source: /u/SondreB

Increasingly, people will migrate to jurisdictions which are more favorable to their bitcoin holdings. And if you want to start a Bitcoin company, you might also move to a jurisdiction which is more favorable to you and your future business.

Finspace: In the last 10 years, many people decided to buy bitcoin, effectively feeding the Bitcoin organism by investing in it. This capital allocation will

continue as more people understand the nature of this beast, and the ultimate goal of Bitcoin: the separation of money and state.

What investors describe as portfolio balancing and allocation of capital can be seen as a migration of value from worse assets to better assets; from bad stores of value to better stores of value. Bitcoin, being the ultimate asset in terms of portability, verifiability, divisibility, scarcity, and unseizability, will continue to suck up value and grow in the process.

Conclusion

Bitcoin lives at the intersection of three spaces: ***meatspace***, ***cyberspace***, and ***finspace***. These spaces have different laws, different rules, and different climates. To fully understand any organism, we must not only look at the organism itself, but examine the organism-environment holistically.

Because of its decentralized nature, Bitcoin is able to overcome many, if not all obstacles in its environments. It can migrate to favorable jurisdictions in meatspace, use different transportation and storage media in cyberspace, and feed on the instability of other asset classes in finspace.

Whatever the future may bring, Bitcoin is equipped to survive and thrive in the various environments it lives in. It is remarkably resilient — well adapted to survive any coming storm, however perfect it may be.

Further Reading

- Proof of Life by Gigi
- The Sovereign Individual by James Dale Davidson and William Rees-Mogg

Acknowledgments

- Thanks to Jannik and Raph for their feedback on earlier drafts of this article.

Bitcoin's Social Antifragility

By Sven Schnieders

March 1, 2020

Secure Rules

I have argued in the past that the difficulty of changing the rules is one of the most important properties of Bitcoin. Without this security, which is in large part a consequence of decentralization, Bitcoin cannot function as a store of value. For a more detailed argumentation, I recommend reading my essay Mass Adoption of Bitcoin's Values and this Twitter thread:

In this essay, we will take a look at why it is becoming less and less likely that these rules, e.g. monetary policy, are going to change in the future—even though it is already extremely unlikely. The reason is Bitcoin's social antifragility. Unlike some other articles that cover the same topic, we will

focus on the community and developers to find out why the social part of bitcoin's antifragility is the most important one.

Antifragility

The term antifragility was coined by Nassim Nicholas Taleb and is used to describe the property of something that benefits from volatility and randomness. If you ship something which breaks easily, you label it "Fragile, handle with care!". If on the other hand, you ship something robust—a large brick—you do not label it at all. In other words, the brick does not care about volatility. Most people assume therefore that robustness is the opposite of fragility. That is false, the opposite is antifragility. If you ship something antifragile, you label it "Antifragile, handle without care!". The difference is that the robust—the large brick—does not care if it is thrown around; the antifragile ***wants*** to be thrown around—it benefits from volatility. Unfortunately, there is no concrete example of something that gets better by putting it in a box and "mishandling" it; there are however many things in socioeconomic life that work this way.

How the Coronavirus Strengthens the Restaurant Business

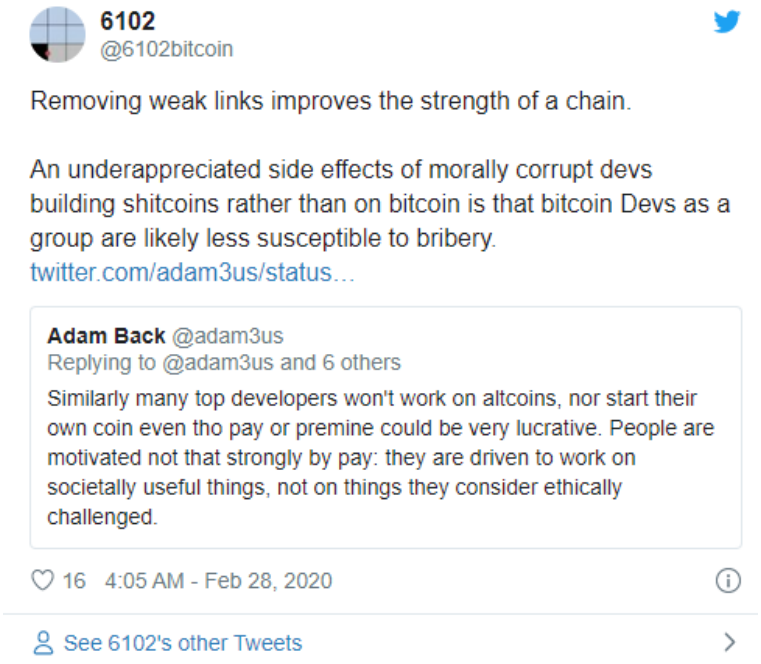
Let's imagine that as a consequence of the recent Coronavirus outbreak, a lot more people eat at home and do not go out (I am oversimplifying the impact here but it is useful to illustrate the point). For this example, we will assume that the revenue of the restaurant business in NYC—all restaurants combined—suffers a decline of 50%. This is obviously bad for individual restaurants; they are fragile and do not like volatility—some of them will go bankrupt. It is however beneficial for the restaurant business as a whole. Why? Because of the survival of the "fittest"; the restaurants that do go bankrupt are the "weakest." They are the ones that are struggling to survive even under normal conditions; the ones with few costumers, too high prices and bad food. After these bad restaurants have gone bankrupt, the average quality of the remaining restaurants is better and there is room for new ones. The reader should be aware that this distinction between "good" and "bad" restaurants is not objective; it is about being well adapted to the local market—delivering what the consumers want. Conclusion: the restaurant business as a whole is antifragile because the individual restaurants are fragile. (For more implications of antifragility and other great ideas, I highly recommend reading all books by Nassim Nicholas Taleb.)

Antifragility of Bitcoin's Community

Bitcoin is profiting from the same antifragility as the restaurant business and NO2X is a great example of this effect. There was a heated debate in 2017 about doubling the block size of Bitcoin which ended in the BCash fork. Those who—wrongly—thought that increasing the block size is a great idea

left Bitcoin for their own chain and most users who thought the same way switched as well. The fact that those people left made Bitcoin stronger as a whole. But what do we mean by saying it is now "stronger"? It means that after the BCash fork, the average commitment of the remaining community to the core values of Bitcoin was stronger. Those who understood the value proposition of Bitcoin—securing monetary sovereignty and liberty—stayed in Bitcoin and this understanding became the new baseline. Everyone who fundamentally disagreed with this value proposition, thinking—wrongly—it is about cheap and fast payments, left Bitcoin.

"6102" and Adam Back have pointed out that the same effect is responsible for making the ***current*** Bitcoin Core developers less susceptible to corruption and bribery; because if they were, they would have already switched to more lucrative "Altcoin" development. The developer community got stronger because the "weak links" left.



Stronger Bitcoin

Bitcoin became stronger through the 2X attack and the community is now more committed to its core values than ever before. As a consequence, a change in the rules that secure the core values is becoming increasingly unlikely.

As always, keep stacking Sats and hodling Bitcoin.

Ten Million Bitcoiners: The Intransigent Minority

By Cory Klippsten

Posted February 21, 2020

Not too many years from now, the number of Bitcoiners in the United States of America will cross ten million. When we hit that milestone, it's game over: Bitcoin wins.

My favorite writer and thinker, Nassim Nicholas Taleb, wrote about "the intransigent minority" in his book ***Skin in the Game***. Here's the concept at work: almost every packaged food product for sale in the U.S. has a tiny ***U*** inside a circle printed outside. Very few U.S. residents require the kosher certification indicated by that ***U***, but it's easier for food companies not to have to make two separate lines for every product, so they generally make everything kosher. The rule, per Taleb: "A Kosher eater will never eat nonkosher food, but a nonkosher eater isn't banned from eating kosher."

For most observed complex systems, the minority contingent required to flip a population to comply with their intransigent view is in the 3–4% range. With a U.S. population of 325 million, 3% is 10 million.

For most observed complex systems, the minority contingent required to flip a population to comply with their intransigent view is in the 3–4% range. With a U.S. population of 325 million, 3% is 10 million.

A fintech fund that's been in the Bitcoin space since 2012 recently ran intense analysis resulting in the best estimate I've seen for Bitcoin ownership. Just 7 million people globally are storing $100 of value or more in the Bitcoin protocol. For round numbers, let's assume half of those people are in the U.S., and that one-seventh of those are above a more significant threshold like $2500. That's just 500,000 U.S. citizens with a meaningful amount of Bitcoin. And of those, what percentage actually understand and care about Bitcoin to the point where they would fight for it? Let's be generous and say 20%.

There are approximately 100,000 Bitcoiners in the United States. This means that ***just to get to "intransigent minority" levels***, we need a 100x increase. This is why adoption dominates all other priorities for Bitcoin.

Bitcoiners have already knocked out so many potential attack vectors and handled so much FUD that there's not much downside risk.

Another concept Taleb references throughout the five volumes of his ***Incerto*** is: Protect Your Downside. Bitcoiners have already knocked out so many potential attack vectors and handled so much FUD that there's not much downside risk left for Bitcoin. But there ***is*** some, whether you handicap it at sub-1%, sub-10%, or more. And by far the most threatening attack vector, in my opinion, would be a concerted effort of the U.S. government at many levels attempting to stamp out Bitcoin in an effort to maintain dollar hegemony across the globe.

Let's be clear: Bitcoin would survive even the most concerted and vicious attack by the U.S. government. It might even thrive, ***Antifragile***-style (another Taleb book), with people around the globe snapping up sats ***en masse*** as they witness the erstwhile hegemon lash out. But it could also play out differently, with a massive drop in network activity and value, thousands of individual lives irreparably disrupted, and the delay of our bright orange future by decades or longer.

This, to me, is unacceptable. That is why I have dedicated my life to recruiting the other 99% of our intransigent Bitcoiner minority here in the United States. There are 100,000 of us already. Help us recruit the other 9.9 million.

The Many Angles of Bitcoin Adoption

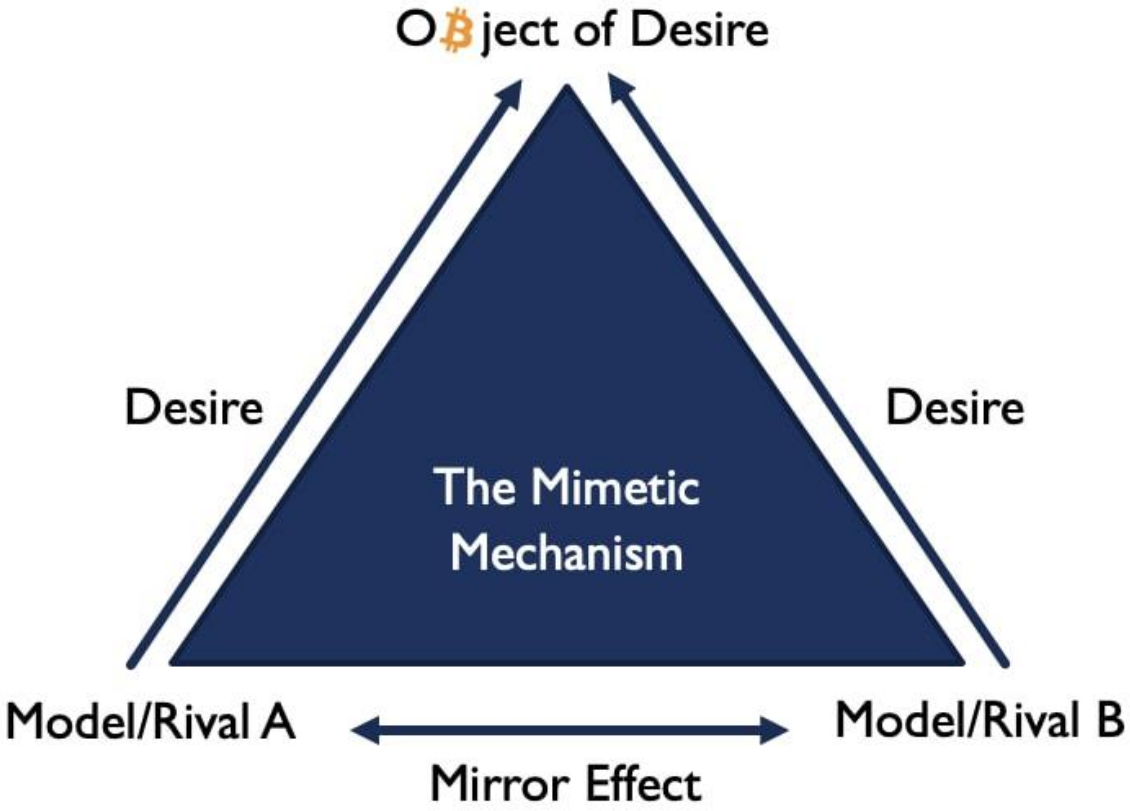
By Phil Bonello

Posted February 12, 2020

It might make sense just to get some in case it catches on. If enough people think the same way, that becomes a self fulfilling prophecy. – **Satoshi Nakamoto, 2009**

The data indicates that Bitcoin ***is*** catching on from a number of angles. As Satoshi pointed out in 2009, this creates a positive feedback loop.

The acceptance and value of Bitcoin is largely based on imitation which can be explored through Rene Girard's mimetic theory. We usually explain why we want something because it fits our unique preferences, or we highlight the objective good qualities something has. But in reality, we are frequently imitating others. We pattern our choices based on another's example. This is also the nature of the monetization process.



This idea of imitation is key to Bitcoin's value. Absent agreed upon frameworks to value Bitcoin, the price ***someone else*** is willing to pay is often

the best signal one has to know what to pay. It's self-referential and what makes Bitcoin's price exceptionally reflexive. Following the picture above, when price rises, Rival A buys Bitcoin. Rival B is imitating Rival A, so Rival B also buys Bitcoin which then leads to Rival A buying more Bitcoin. This also works in reverse. As price falls, Rival A sells which triggers Rival B to sell and so on. This crowd mentality exists everywhere and has been especially true for Bitcoin. Crowds need a reason to exist.

For the Bitcoin crowd, there are many reasons.

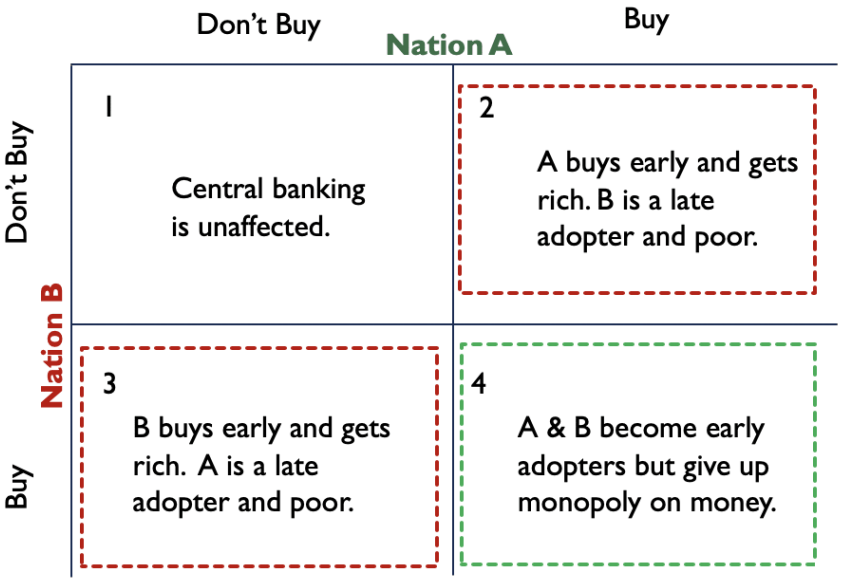
Bitcoin is:

- A prisoner's dilemma for nation states
- Digital gold - a money outside the reach of central banking
- An uncorrelated alternative investment with asymmetric upside
- A generational movement
- A tool for survival, social good, and dissidence, especially in autocratic regimes and hyper-inflationary economies
- A network that is driving the profitability of renewable energy initiatives
- The best performing asset of the decade

Bitcoin Presents a Prisoner's Dilemma for Nation States

To start with the most controversial and least talked about adoption vector, Bitcoin presents a prisoner's dilemma for nation states and their sovereign wealth funds. Of course, nation states would like to maintain control of monetary policy. But they have to participate in the Bitcoin game whether they want to or not.

- **Quadrant 1: All nations agree not to buy Bitcoin**. They can maintain the status quo – central banking.
- **Quadrant 4: All nations buy Bitcoin**. They benefit from price appreciation but lose control of money supply.
- **Quadrants 2 & 3: *Any* nation buys Bitcoin, while others abstain.** Those that abstain may be forced to buy later - the worst case scenario.



This is a forcing function. It only takes one sovereign wealth fund to set this in motion. Once a fund has accumulated its target amount, it simply has to make it known. Not only would this immediately put the fund in profit by initiating a cascade of buying from others, it would force other nations to consider making the same purchase. Nation states will experience intense fear of missing out.

Bitcoin is Digital Gold

Bitcoin is money, a digital gold. As such, the target market is massive. If Bitcoin can achieve the market capitalization of gold, it would see over 50x return on investment. Bitcoin's scarcity, acceptance, and portability make it an object of desire to gold bugs and central banking skeptics.

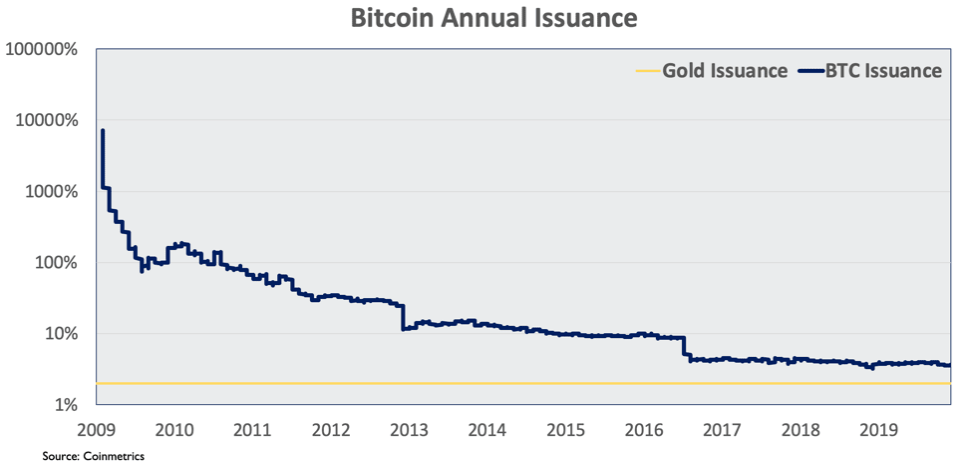
	Estimated Value ($B)	Multiple on BTC
BTC Value	$150	x
10% of Global Gold Value	$770	5x
Global Gold Value	$7,770	52x
Global M1 Money	$34,000	225x
Global M2 Money	$86,000	570x

Source: OnchainFX, Visual Capitalist, CIA 2017

Scarce

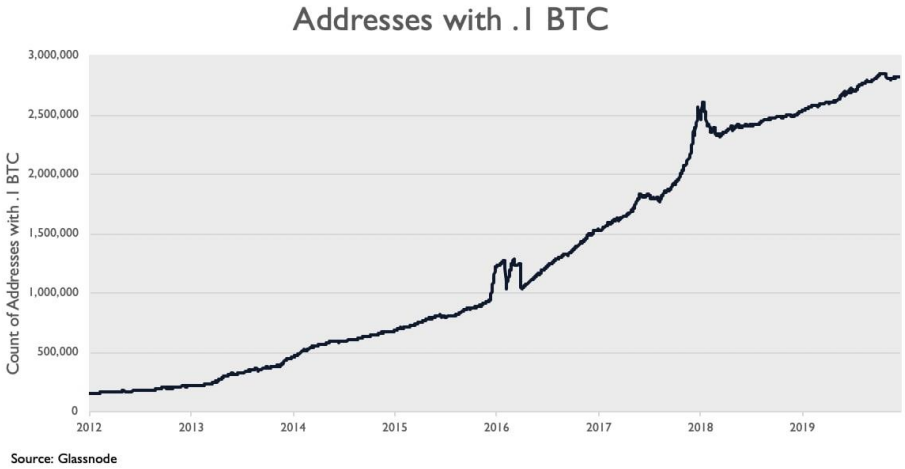
Bitcoin is compared to gold because it's scarce. For thousands of years, gold has been used as a money and store of value because consistently, its annual issuance has hovered around 2-3%. It has maintained its purchasing power. Meanwhile, failed currencies range from Rai stones, to seashells, to copper, to countless attempts at paper money. If a money supply can be increased, it will be increased. Bitcoin has a capped supply of 21 million. The Bitcoin

issuance decreases approximately every four years. Symbolically, 2020 is important because for the first time, we will see the annual issuance be less than that of gold.

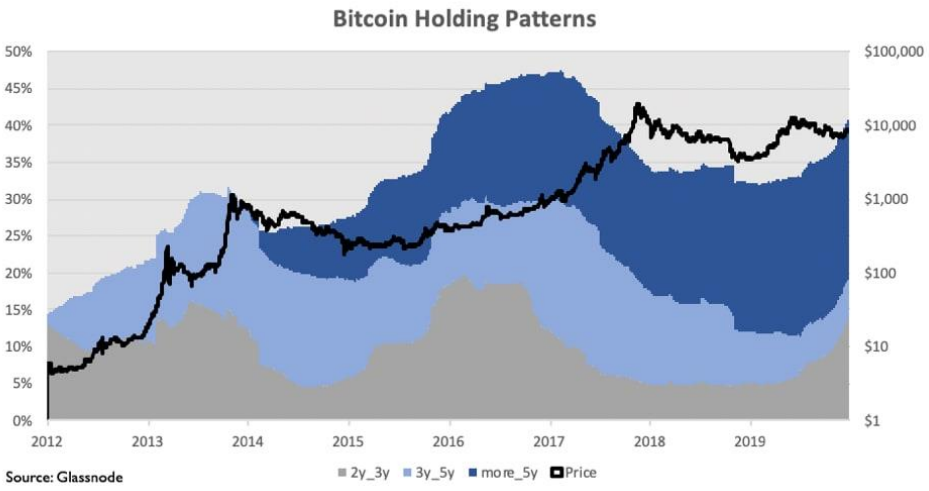


Accepted

Data indicates that Bitcoin that more people than ever are using Bitcoin. This chart illustrates the number of addresses that hold a non-trivial amount of Bitcoin (.1 BTC). This measure allows us to filter out addresses with so-called dust balances. More people than ever are holding Bitcoin, and infrastructure is in place to make it easier for merchants to accept it as payment.

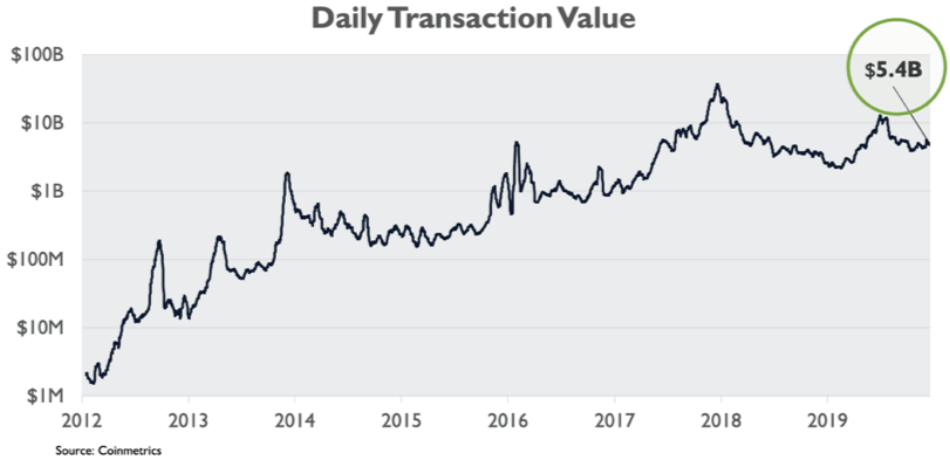


This chart shows Bitcoin holding patterns. Over 40% of Bitcoin has been held for two years or more, and that number is increasing rapidly. We can observe a similar patterns of accumulation before previous bull runs.



Portable

One of the biggest pitfalls for gold is its portability. It's inconvenient for daily use but also expensive to move large quantities. In November of 2019, Poland repatriated 100 tons of gold, about $5 billion. Poland conducted a top-secret mission with a police escort, a helicopter, and a freighter plane for only $5 billion of gold. In a world that's increasingly digital, we need a money that is digital and portable. Not only would the same transaction cost less than $1 and be completed in an hour, but the Bitcoin network handles over $5 billion each day! Over $7.5 trillion has been transferred throughout Bitcoin's history. Bitcoin is portable in a time of rapid globalization.



Bitcoin is an Uncorrelated Alternative Investment

There's $250 trillion in global debt and that trend seems unlikely to reverse. The United States federal government alone has added $10.4 trillion of debt since 2009. Central banks are forced to implement accommodative monetary and fiscal policy in hopes of tempering the debt bubble - $17 trillion in

negative yielding bonds and counting. Investors are using Bitcoin as a hedge against currency devaluation while also decreasing the overall correlation within their portfolios.

Source: Institute of International Finance

Uncorrelated return streams are hard to come by. Bitcoin has been completely uncorrelated in the last five years. Investors have noted this as an intriguing characteristic of Bitcoin. Not only does it offer potential for great returns, but it is uncorrelated to major assets.

Correlation of daily returns from December 2014 - December 2019

	Bitcoin	SPX	Gold	VIX	DJIA	Wilshire US REIT	NASDAQ	High Yield Bonds	Japanese Yen	Chinese Yuan	Canadian Dollar
Bitcoin	1.000	0.052	0.005	-0.049	0.045	0.032	0.038	0.040	0.018	0.041	-0.003
SP500	0.052	1.000	-0.029	-0.794	0.966	0.533	0.950	0.478	0.311	-0.147	-0.214
Gold	0.005	-0.029	1.000	0.048	-0.021	-0.024	-0.030	0.000	-0.348	-0.151	-0.153
VIX	-0.049	-0.794	0.048	1.000	-0.764	-0.436	-0.758	-0.369	-0.275	0.129	0.163
DJIA	0.045	0.966	-0.021	-0.764	1.000	0.498	0.879	0.464	0.316	-0.158	-0.220
Wilshire US REIT	0.032	0.533	-0.024	-0.436	0.498	1.000	0.452	0.258	0.062	-0.030	-0.142
NASDAQ	0.038	0.950	-0.030	-0.758	0.879	0.452	1.000	0.448	0.281	-0.143	-0.152
High Yield Bonds	0.040	0.478	0.000	-0.369	0.464	0.258	0.448	1.000	0.293	-0.209	-0.335
Japanese Yen	0.018	0.311	-0.348	-0.275	0.316	0.062	0.281	0.293	1.000	0.134	0.136
Chinese Yuan	0.041	-0.147	-0.151	0.129	-0.158	-0.030	-0.143	-0.209	0.134	1.000	0.265
Canadian Dollar	-0.003	-0.214	-0.153	0.163	-0.220	-0.142	-0.152	-0.335	0.136	0.265	1.000

Source: Federal Reserve Bank of St. Louis

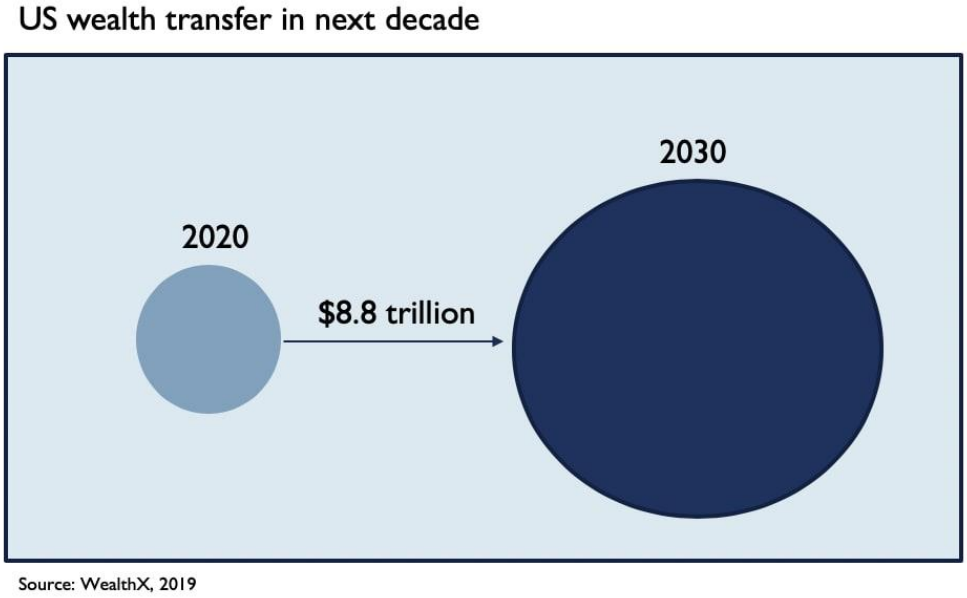
As more investors warm to the idea of Bitcoin as an uncorrelated hedge, career risk will decrease, institutional products will come to market, and firms will have the go-ahead to allocate. It's reflexive.

Bitcoin is a Millennial Movement

Most convincing of all is the interest younger generations show for Bitcoin. They've grown up in a digital world, and they are comfortable with digital money. Gold is the reserve asset of Baby Boomers. Bitcoin is the reserve asset of Millennials. It represents a changing of the guard.

Millennials just became the largest US generation as of 2019 and are soon to be the largest generation in the world. They prefer alternative financial products - mobile banking, robo advisors, prepaid debit cards, emergency lending. They have grown up in a digital world and are comfortable holding money on their phones.

And in the next 10 years the younger generations are estimated to inherit almost $10 trillion. This does not even include the money millennials will earn as they enter their prime working years. This is the tip of the iceberg. Over the next 30 years, estimates indicate almost $70 trillion of wealth transfer.



And millennials are buying Bitcoin like crazy!

The data below shows the top 5 equity holdings as a percent of total assets across generations in Charles Schwab IRAs. Amazingly, millennials hold almost 2% of their assets in Grayscale Bitcoin Trust, a Bitcoin vehicle that often demands over 20% premium to spot. Not only are millennials interested in exposure to Bitcoin, but they are willing to pay a substantial premium.

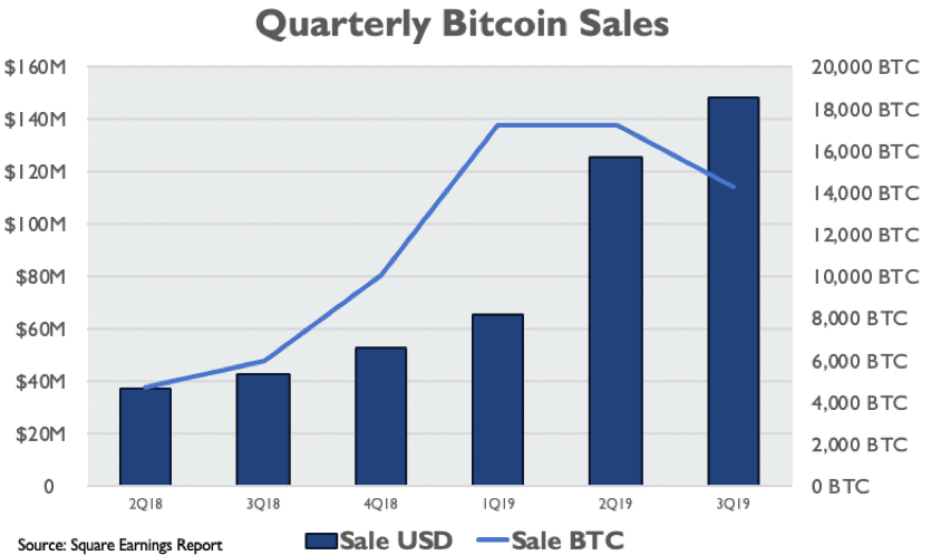
Top 5 IRA equity holdings as a % of total assets held across generations

Millennials	%	Gen X	%	Baby Boomers	%
AMAZON.COM INC	7.87%	APPLE INC	10.52%	APPLE INC	9.91%
APPLE INC	6.18%	AMAZON.COM INC	7.16%	AMAZON.COM INC	5.32%
TESLA INC	3.22%	BERKSHIRE HATHAWAY	2.37%	BERKSHIRE HATHAWAY	2.75%
FACEBOOK INC	3.03%	FACEBOOK INC	2.26%	MICROSOFT CORP	2.69%
GRAYSCALE BITCOIN TRUST	1.84%	MICROSOFT CORP	2.16%	FACEBOOK INC	1.43%

Source: Charles Schwab

As millennials enter their prime earning years and inherit enormous wealth, this Bitcoin buying should increase dramatically. **Square** *"Bitcoin is resilient. Bitcoin is principled. Bitcoin is native to internet ideals. And it's a great brand"* – Jack Dorsey To further illustrate the connection between Bitcoin and millennials, it's worth exploring Square, one of the companies at the center of the trend. Jack Dorsey, CEO of Square and Twitter, is an avid supporter of Bitcoin. And with $3.2 billion in revenue in 2018 (~50% increase YoY), Square's business is growing quickly, especially with younger generations.

- 70% of users are millennial or younger
- 2x increase in first time Bitcoin buyers in Q3 2019
- 2 million merchants use the point of sale product
- 60 million Cash App downloads.



Square is on the path to providing end-to-end financial services for consumer and merchant that represent a massive portion of the population. Expect Bitcoin to be integrated into all of these services in the coming years.

Bitcoin is a Tool for Survival, Social Good, and Dissidence

"Africa will define the future (especially the bitcoin one!). Not sure where yet, but I'll be living here for 3-6 months mid-2020." – Jack Dorsey

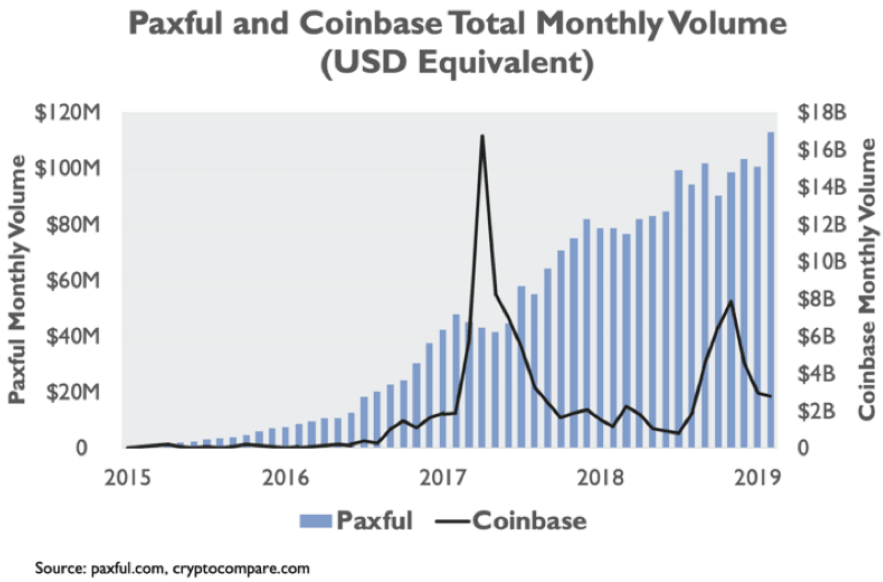
Jack Dorsey also recently made a trip to Africa where he sees substantial opportunity. Africa is home to 7/10 fastest growing economies on earth and 1.2 billion people.

Nigeria also has the highest Bitcoin search volume since 2018. Comfort level with digital products, acceptance of alternative money/financial products, and their intrigue for Bitcoin shows interesting parallels to millennials broadly.

Currently, Africa's GDP is only 10% that of the United States. Generally, Africa isn't burdened by past technological success and is now in the throes of a technological revolution, leapfrogging personal computers in favor of internet connections through mobile phones. It's plausible that we see Africa lead tech adoption over the next two decades.

Because currencies and banking infrastructure have been so unreliable, pre-paid minutes and services like M-Pesa have been used for the last decade to transfer value. Consumers are comfortable with alternative payment systems, simply using whatever works best. And increasingly, Bitcoin is the tool of choice.

This chart shows monthly volume for Paxful vs Coinbase. Coinbase is the most popular US retail trading venue. Paxful is a peer-to-peer online exchange where Bitcoin is traded for direct bank transfers, gift cards, other goods or services, or cash. Paxful doesn't require connection to traditional banking or regulatory infrastructure so it can service unbanked citizens in developing countries or authoritarian regimes. This chart is particularly interesting because it shows that organic demand for Bitcoin as a money is steadily growing while the trading volume on Coinbase seemingly follows price movements.



Necessity is the mother of innovation. It's worth paying attention to how those that ***need*** this technology are using it.

Bitcoin is Driving Profitability of Renewable Energy

Critics opine on the wastefulness of Bitcoin mining. But contrary to popular belief, Bitcoin mining is emerging as a key driver of profitability for renewable energy.

From the perspective of those selling electrical power, Bitcoin miners have become the buyers of last resort. Energy economics in many countries have carved out a serendipitous niche for Bitcoin miners. Governments are forcing a transition from fossil fuels by subsidizing renewable energy. These subsidies have resulted in over-production of renewable energy. This over-production has outpaced transmission capacity. Because energy storage at scale is still inefficient and uneconomical, this forces power plants to sell electricity at substantially reduced prices. This has become a boon for Bitcoin miners and power companies. Miners buy power at a discount by locating themselves near the plants, and the power companies have buyers of excess power that would otherwise go to waste. Unsurprisingly, companies are taking advantage of the opportunity.

In the fall of 2019, two companies announced funding to launch mining operations in the U.S., specifically to capitalize on these dynamics. Layer1 raised $50 million led by PayPal founder, Peter Thiel. The goal is to launch a vertically integrated operation that utilizes wind energy in Texas. Crusoe Energy raised $70 million, $40 million in financing and $30 million in equity. This raise was led by Bain Capital Ventures. Crusoe provides solutions to oil

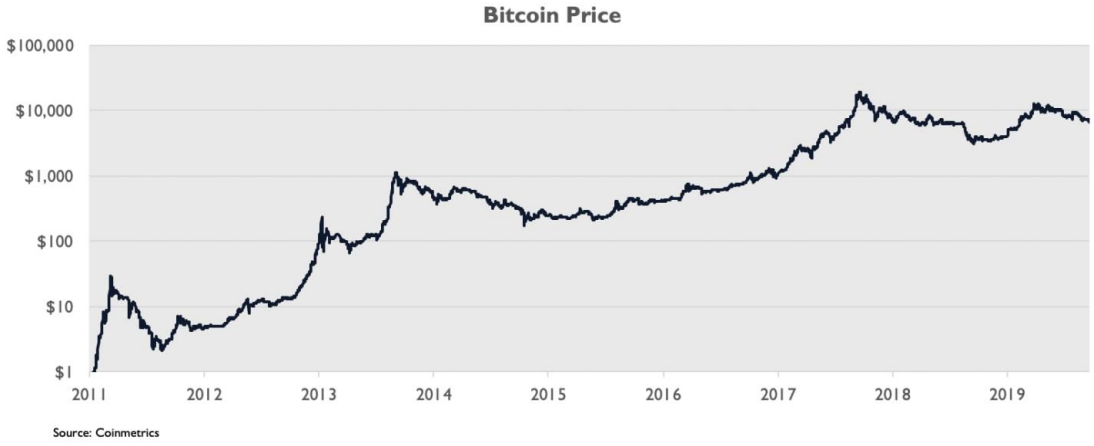
and gas companies to reduce flaring and repurpose the energy for mining and cloud computing.

Environmentalists – from foes to friends!

Bitcoin is the Best Performing Asset of the Decade

Finally, Bitcoin is the best performing asset of the decade. From fractions of a penny to over $9000 today, millions of percent of appreciation all without a central team managing its success.

This price performance is inescapable. If you are paying attention to markets, you know the Bitcoin story. The price increase and the resulting wealth that some have gained, attracts others. Once again, the is reflexive.



Conclusion

Bitcoin is catching on from multiple angles. Sovereign wealth funds are forced to consider the Bitcoin prisoner's dilemma. Gold bugs are forced to consider Bitcoin as a worthy digital counterpart. Institutional investors are forced to consider Bitcoin's low correlation and its status as a reserve asset. Baby Boomers are forced to consider the preferences of future generations. Developed nations are forced to consider the adoption trends in developing nations. Environmentalists are forced to consider the positive impact that Bitcoin mining has on renewables. And everyone has to consider Bitcoin's meteoric rise.

Once more from Satoshi...

It might make sense just to get some in case it catches on. If enough people think the same way, that becomes a self fulfilling prophecy. – Satoshi Nakamoto, 2009

Tweetstorm: On Adversarial Thinking

By Ragnar Lifthrasir

Posted January 12, 2020

A thread/rant on the importance of thinking critically and adversarially about Bitcoin claims and ideas, and the dangers of failing to do so.

This isn't directed at anyone specifically so please don't make it personal. Let's stick to ideas and arguments please

Below is an example of robotic repetition of unquestioned simplistic dogma as a mantra of faith and an excuse for inaction and critical thought.

In this instance it's HODLmonomania. (Yes I HODL and recommend it). The danger of this monomania is what follows from it...

- Don't develop and use @btcpayserver, a self-hosted, open-source bitcoin payment processor to build a circular Bitcoin economy. Just HODL.
- Don't develop and use the Lightning Network to give better privacy for censorship resistant and faster payments. Just HODL.
- Don't build a network of people to informally buy and sell bitcoin to escape the KYC/ AML and surveilled 3rd party Bitcoin exchanges. Just HODL.
- Don't use bitcoin to pay for Bitcoin products and services to spread adoption of bitcoin, create a circular bitcoin economy, and offer an alternative to exchanges to acquire bitcoin. Just HODL.

We can see how reducing all of Bitcoin to one monomania keeps bitcoin from progressing, gives an excuse for inaction, narrows the scope of Bitcoin's purpose and abilities, and discourages rigorous intelligent discourse.

Memes are for humor, not orthodoxy.

Here's an example of an extraordinary claim, that feels good to believe, but lacks empirical support and isn't evaluated with common sense.

If you owned all the BTC currently in circulation, 18,144, at today's price of $8,087, then you'd have a net worth of $147 billion. Jeff Bezos is worth $131 billion. From when he started Amazon & it was worth $0 to today he had a "wealth transfer" of almost the market cap of bitcoin

There's many more extraordinary claims about Bitcoin that require extraordinary evidence, or at least critical thinking, but lack either. These claims have become givens, unquestioned, and widespread.

Some other examples: Lightning Network can replace Visa and MasterCard. Bitcoin solves inequality. Bitcoin will become the world's reserve currency. Bitcoin will end wars. Bitcoin will prevent governments from collecting taxes at a mass scale.

As much as we hope some of these claims come true (I do!) we make bitcoin weaker by burdening bitcoin with unrealistic expectations, setting up bitcoiners for disillusionment, and lulling into inaction and dangerous overconfidence.

Humility is the beginning of wisdom.

To make Bitcoin and ourselves stronger we need to think like the software engineers who contribute to Bitcoin. They peer review, mercilessly seeking flaws. At their tech events they talk about every which way a proposal can fail. They think adversarially. They're conservative

Stressing muscles makes them stronger

Testing & reviewing codes reduces the risk of exploits

Thinking critically about ideas & claims focuses our limited resources on what's realistic & achievable. It also helps us let go of future fantasies to focus on the present.

Tweetstorm: On Cheating

By Dhruv Bansal

Posted March 3, 2020

\1 "Bitcoin is a game we play where we can easily tell when someone is cheating."

When I first saw this (in some ELI5 bitcoin Tweet) I thought it just some pithy phrase.

But over time this simple sentence has come to resonate with me as a profound summary of the bitcoin ethos.

\2 Bitcoin IS a game, but an ***infinite*** one, where the goal is to keep playing – not a finite game where the goal is to win.

"Finite games are theatrical, necessitating an audience; infinite ones are dramatic, involving participants"

Finite and Infinite Games

\3 Like any game, bitcoin is an opt-in set of rules devised by its players.

Once the game has begun, changing rules is tough. Only rules which help players continue playing will survive. And no one is in charge of making changes.

So, like the game of culture, Bitcoin evolves.

\4 Preventing cheating is important in infinite games because cheaters are seeking to win, not to continue play.

Cheating in bitcoin isn't prevented by referees (3rd parties) or parents (the state).

Mathematics, energy & the greed of other players ensures the game continues.

\5 Imagine other games if they were like bitcoin:

- A news industry in which those with the incentive to lie don't because it's more profitable to tell the truth.
- Societies which don't pollute because it's cheaper to be clean.
- Making people free making people money.

\6 Yes, bitcoin is deadly serious with big fortunes, egos, and ambitions in play.

But thinking of it as an infinite game can help engender the playfulness required for creativity, innovation, progress.

To a beautiful game...

So You Think Bitcoin Mining is Wasteful?

By Daniel Frumkin

Posted March 5, 2020

Much has been said in the past couple of years about the amount of electricity consumed by Bitcoin mining. In fact, negative environmental impact has become one of the go-to talking points for Bitcoin pundits to criticize the digital currency.

However, data provided without context can be ***very*** misleading, and this is often the case when journalists write about Bitcoin mining. The total (estimated) energy consumption is indeed quite high, and still growing rapidly as the network hash rate continues to climb. However, the real world impact is frequently misrepresented and misunderstood.

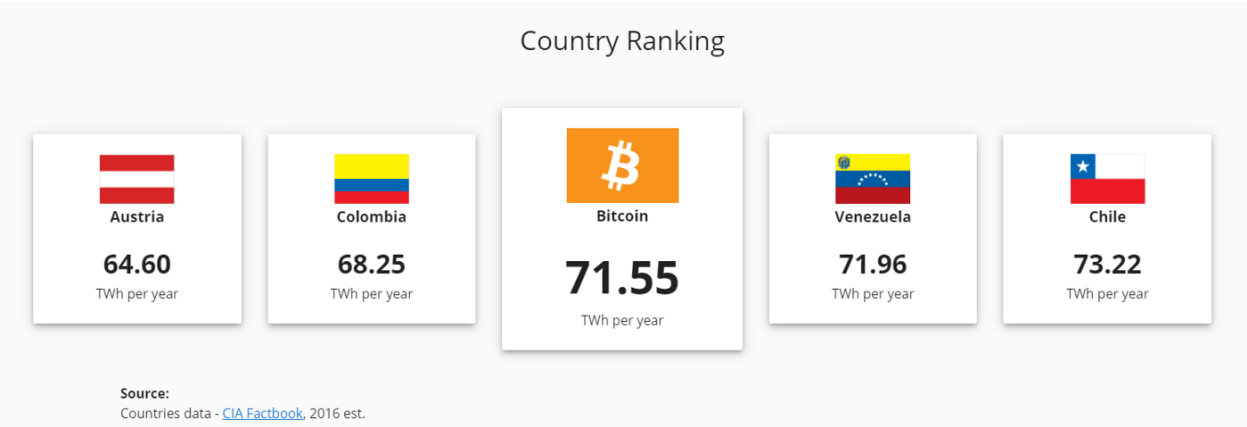
In this article, we'll be comparing the electricity consumption of Bitcoin mining with all of the world's videogame consoles and computers. Then we'll discuss the difference in typical electricity _sources _for the two and their respective environmental impacts.

Let's begin with an update on the most common of comparisons: Bitcoin vs. countries.

Bitcoin's Electricity Consumption Relative to Countries

It became popular around 2017 to compare Bitcoin's total electricity consumption with that of entire countries. To that end, the University of Cambridge created a handy tool called the Cambridge Bitcoin Energy Consumption Index (CBECI) that tracks annualized electricity consumption of Bitcoin mining and makes interesting comparisons to provide some context.

As of November 2019, Bitcoin's estimated energy consumption is in the same range as Colombia, Venezuela, and Chile.



It should be noted, however, that this is still asmall amount compared to the top global electricity consumers: China (5564 TWh per year) and USA (3902 TWh per year).

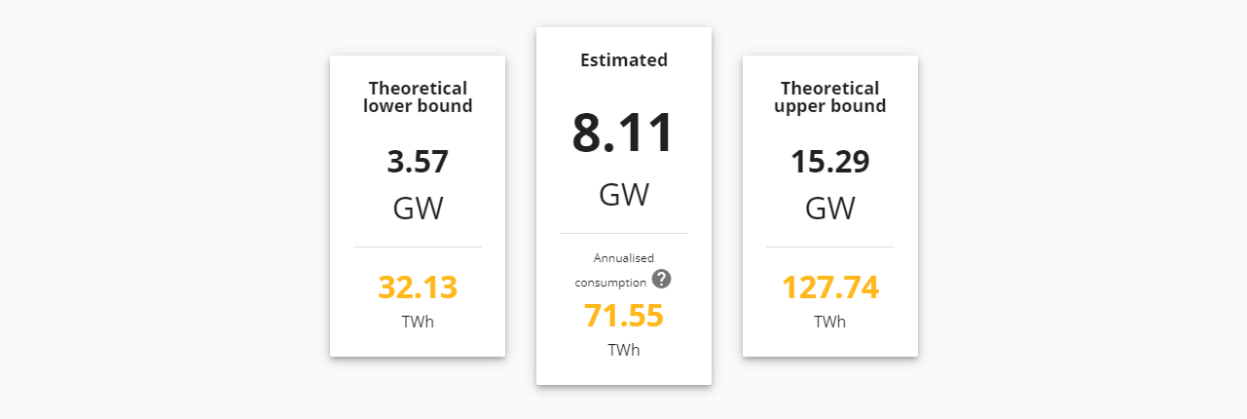
Now let's get to the real comparison we want to know about...

Bitcoin vs. Video Games — Electricity Consumption

First, it's important to clarify that the following calculations are ***estimates*** with potentially high error margins.

Bitcoin mining's energy consumption varies depending on the total network hash rate and the efficiency of each mining machine being used. For example, producing 100 Eh/s with only the newest and most efficient ASICs would consume substantially less electricity than, say, 100 Eh/s with only ASICs from 2017 and earlier.

With that being said, CBECI has a rather robust methodology for calculating electricity consumption, so we feel comfortable using their estimate of **71.55 TWh per year** as of November 2019.

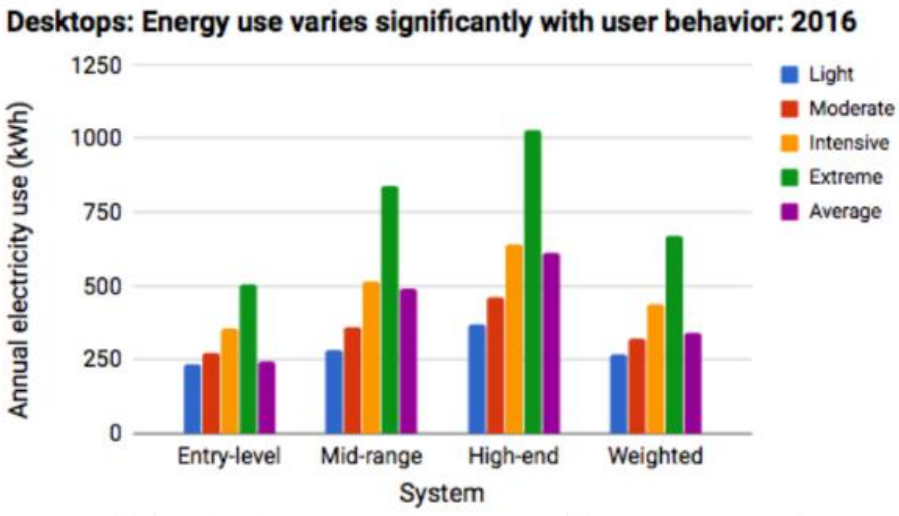


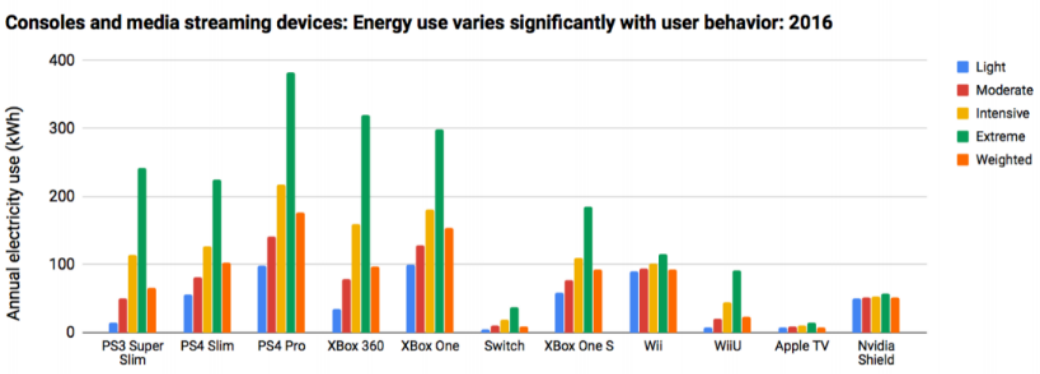
Global electricity consumption of video game playing is substantially more difficult to estimate. For one, there is a large diversity of devices that are

being used for gaming. Consoles such as the PlayStation 4 and Xbox One consume less electricity than high end gaming computers such as a Digital Storm — Velox, so treating all gameplay equally will not be remotely accurate. On top of that, there is the extra complication that gaming consoles and computers don't run 24/7, unlike Bitcoin mining machines.

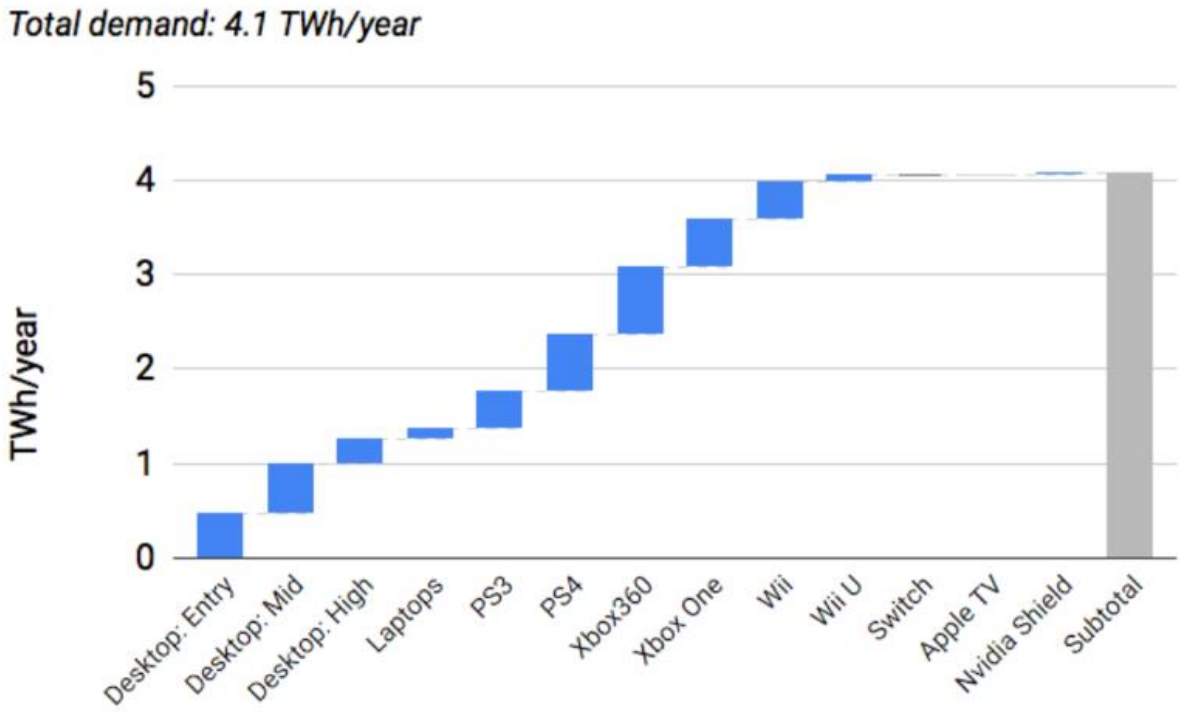
Accurately estimating the energy consumption of video game playing around the globe requires consideration of these factors and many others. In fact, it's well beyond the scope of this simple blog article. Fortunately, a team of researchers at Lawrence Berkeley National Laboratory carried out an incredibly thorough research study on the energy consumption of video game playing in California in 2018. They took into account factors such as the popularity of various gaming systems, their respective efficiencies, typical user behavior, and much more.

You can get a better idea of the thoroughness of their methodology from the graphics below calculating the weighted consumption of a wide selection of gaming systems based on typical user behavior.





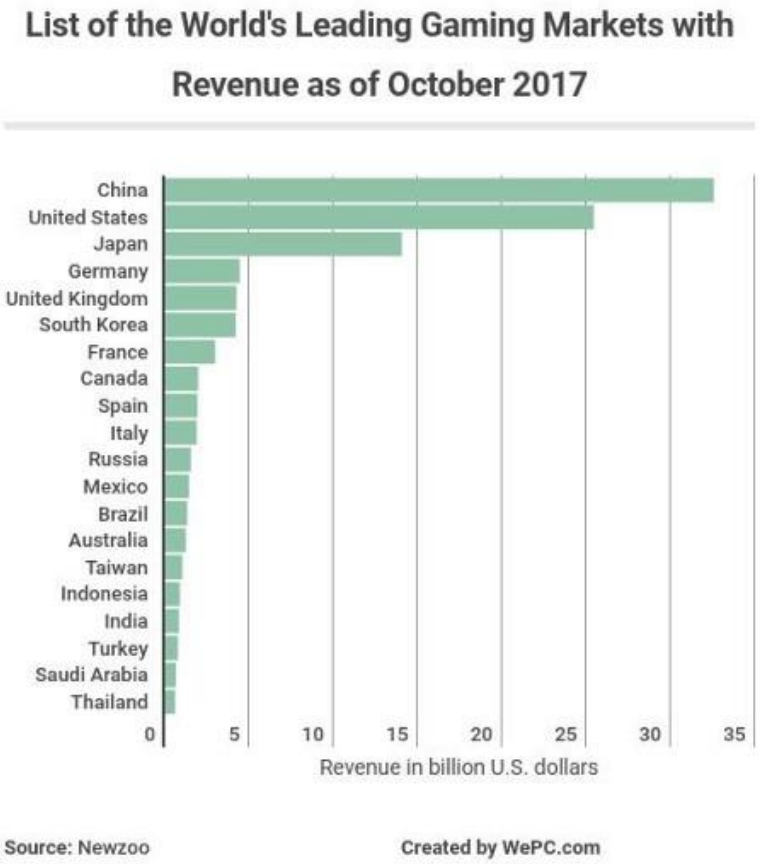
Ultimately, after taking all of this data into account, the research team concluded that the annual consumption of video game play in the state of California for 2016 was approximately ***4.1 TWh per year***.



Now, our only remaining task is to somehow extrapolate that estimate to cover video game playing for the entire world. (This is a good time to reiterate that these estimates have a high potential error margin.)

First, we need to use the estimate from California to come up with an estimate of the total United States consumption. California's population is approximately 40 million people, while the whole of the US population is approximately 327 million. If we assume that the behavior of video game players in the rest of the US resembles California, then we can simply multiply California's 4.1 TWh/y consumption by the ratio 327/40. From that, we get 33.5 TWh/y as the total consumption for the USA.

Next, we'll use data collected by NewZoo and presented in WePC's 2019 Video Game Industry Overview to further extrapolate for the total energy consumption of video game playing worldwide. In this case, data about revenue is far easier to come by than more nuanced data about the number of gamers around the world and their typical user behaviors. (Note that according to NewZoo, "the revenues are based on consumer spending in each country and exclude hardware sales, tax, business-to-business services, and online gambling and betting revenues.")



Considering that the US accounts for 32% of global gaming revenue, we're going to make the (admittedly far from perfect) assumption that it also accounts for about 32% of global energy consumption from gaming. In that case, we arrive to a grand total of **104.7 TWh per year consumed by video game play worldwide.**

So What's the Takeaway?

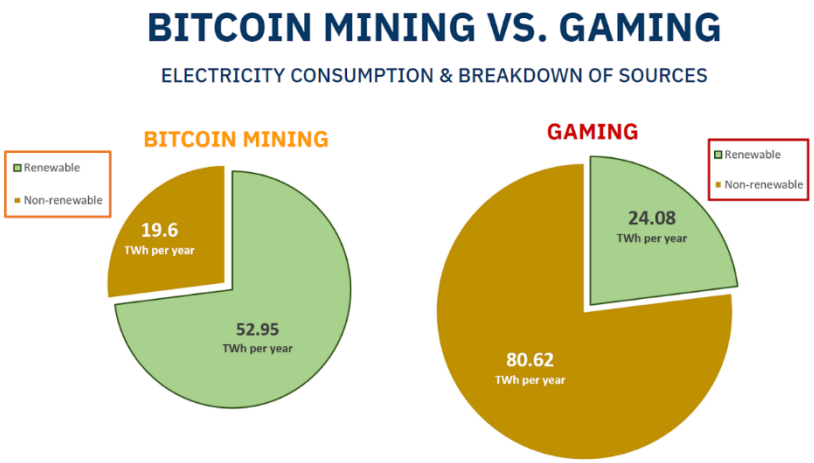
Based on our very rough estimates, we found that the worldwide electricity consumption of people playing video games is **46% higher** than the total consumption of Bitcoin mining as of November 2019. However, since these are such imprecise estimates, the bigger takeaway is simply that the two amounts are pretty close to each other. This provides much better context as to the true scope and impact of modern day Bitcoin mining than comparing the annualized energy consumption directly to small countries.

But it's even more important to understand _where _that energy is coming from. In their June 2019 report, the cryptocurrency investment and research firm CoinShares **estimated that more than 74% of all Bitcoin mining electricity comes from renewable energy sources**. In fact, about 50–60% of the total hash rate comes from Sichuan province in China during its wet season due to the abundance of cheap hydropower there, much of which would otherwise go unused because it is difficult to store and transport. When the wet season is over, many miners move their operations elsewhere to harness cheap thermal and wind power.

The reality is that access to cheap electricity is a necessity in order for miners to compete long-term. With this economic incentive to find the lowest cost electricity possible, many miners have set up shop in rural locations where

excess renewable energy is produced. This is simple supply and demand: the supply in these locations is high, and the demand is practically nonexistent since the excess energy is so difficult to store and transport to urban areas where there are consumers.

On the other hand, the US Energy Information Administration estimated that only 23% of the world's electricity generation came from renewable sources in 2015. Since the majority of video game playing likely occurs in urban areas, it's reasonable to guess that the same 23% figure is a decent estimate for the amount of renewable energy powering gameplay. In that case, we get the following breakdowns.



Explore More

As Den Held explains in his article, Proof of Work is Efficient, "Bitcoin is a super commodity, minted from energy, the fundamental commodity of the universe. PoW transmutes electricity into digital gold." To put it another way, Bitcoin is like the batteries we don't yet have, capable of storing excess energy and carrying its value through time.

Are there any other topics related to Proof of Work and Bitcoin mining that you'd like us to cover? Let us know by leaving a comment below or tweeting @braiins_sytsems @slush_pool.

Stop Treating Bitcoin as Risky. It's a Safer Asset Than Most

By Jill Carlson

Posted March 5, 2020

This article was written by Jill Carlson on March 5, 2020 and was originally published on Coindesk.

People think I got into bitcoin (BTC) because I have a high risk tolerance.

Actually, I got in because I have a low risk tolerance for worst-case scenarios.

Bitcoin is often touted as a risky bet. It is nascent. It has only been around for about a decade. It is poorly understood by mass markets. It is an experiment. It could still fail. All of these claims are true. In many ways, the risk profile of bitcoin resembles that of an early stage startup. Bitcoin appears to be hovering between the trough of disillusionment and the slope of enlightenment. This means that most people continue to view cryptocurrency as kind of crazy. It's a gamble.

THE ROAD TO HAVING BITCOIN UNDERSTOOD AND VIEWED AS A SAFE HAVEN IS A LONG ONE, DEMANDING DEEP INVESTMENT IN EDUCATION.

These dynamics mean that investors often bucket bitcoin as a risk asset. It gets put in the same category as high-growth stocks, high-yield debt, high-beta exchange-traded funds, venture capital investments and emerging markets.

Markets broadly have two modes: risk-on and risk-off. In risk-on scenarios, when markets are confident and things are moving higher, risk assets tend to outperform safe havens. When the markets are risk-off, safe-haven assets like gold, treasury bonds and cash fare better, and are often the only investments trading higher as investors sell out of their riskier positions.

Whether a financial product is a risk asset or a safe haven depends on a number of properties. In some cases it depends on the fundamentals of the asset. Share price is a reflection of the projected future cash flows of the business, which in turn depend on dynamics like customer demand. The dynamics can make companies more or less subject to movements of the markets. In other cases, the categorization of a given asset might depend on supply and demand dynamics. Gold, with its relatively fixed supply and consistent demand from entities like central banks, is resilient to market cycles and downward shocks. In all cases, however, I would argue that what

matters most in understanding asset correlations and behavior is market perception. Do traders and investors view the asset as a good place to hunker down in volatile markets? Or do market participants view the investment as vulnerable to the downside, but also prime to participate in boom cycles?

The markets certainly still seem to view bitcoin as the latter. And as far as the price of bitcoin is concerned, and as far as any market correlations are concerned, that perception is all that matters.

Via Jill Carlson

This perception misses bitcoin's most important properties. Bitcoin is, in many ways, the ultimate safe haven asset. It can be self-custodied, so even when systems of trust and rule of law breaks down, it can be held. It is open and borderless, with relatively liquid markets in every country in the world. It is censorship-resistant, meaning no government nor institution can, practically speaking, prevent investment or transaction in bitcoin. Bitcoin has a fixed supply, much like gold. Bitcoin is digital, which makes it practical to hoard, hold and transport. For doomsday preppers, dystopian sci-fi fans and apocalypse predictors, there is a lot to like about bitcoin.

Yet, if we look at the behavior of the bitcoin price over the last couple of weeks, as concerns over a global pandemic have ramped up, it is clear that bitcoin continues to behave more like a high-risk investment than like the safe haven which it promises to be.

Do the markets have it wrong? Should bitcoin be more correlated with gold than with Apple stock? Maybe. But as John Maynard Keynes put it, "The markets can stay irrational longer than you can stay solvent." The road to having bitcoin understood and viewed as a safe haven is a long one, demanding deep investment in education. What matters is the narrative around the asset, and right now the narrative around bitcoin is that it is an early-stage, high-risk bet. As far as the markets are concerned, that perception is reality.

Reviewing "Modelling Bitcoin's Value with Scarcity" — Part IV: The Theoretical Framework leading to the Error Correction Model

The next step after the shown cointegrating relation between stock-to-flow and market cap of bitcoin

By Marcel Burger

Posted March 7, 2020

Introduction

In my first review of the work of PlanB, I concluded that the relation between stock-to-flow and bitcoin price as pointed out by the author was invalid because the general assumptions of ordinary least squares regression were not met. When two variables are non-stationary and we estimate a regression model, there is a good chance we find highly autocorrelated residuals and a significant value for the coefficient. This phenomenon is well known as spurious regression. But, spurious regression isn't always the case. Sometimes the variables might be cointegrated, which would imply that the estimated relation is super consistent. Nick pointed out that we could very well be dealing with the exceptional case of cointegration and showed that he wasn't able to falsify the cointegrating relationship between stock-to-flow and bitcoin's market cap. After Nick showed that the variables were cointegrated, I verified his findings. Since I still was skeptic, I chose to run the analysis on my own dataset and ran three different cointegration tests to make sure there was no doubt. Even though I expected I would be able to show that at least one of those tests would lead me to reject cointegration, I could not. Initially, I was a bit too fast with drawing my conclusions and as a result I warned people that the model was flawed. So, I offered my apologies in public for drawing a wrong conclusion and engaged in many discussions to explain why the model was eventually right. Because I noticed in those discussions that the basis underneath the material we discuss is poorly understood by most people, I decided to start writing a book that will help people to better understand the econometric concepts we're dealing with. To stay in the loop about that development, I recommend subscribing at www.bitcoinometrics.io to get notified once the book is available. But that's not what this piece is about. This piece is about further development of the model and presenting a framework which helps to understand the

developments. In the process of writing my book I also conduct some academical research. Not only to refresh my mind on time series analysis, but also to check with academical researchers if there were any important developments in that field of research. Nick in his write up already mentioned the Vector Error Correction Model ('VECM') and estimated the coefficients for the model as part of his attempt to falsify cointegration. In my 'hunt for cointegration' I also touched on it without estimating any of the model coefficients, but I ended the article by stating that setting up a VECM would be a nice subject for a follow up article. This is still work in progress, but I like to share a bit more on how we actually get to that point and how to go about.

Model Selection Framework

Usually when one is looking to quantify the relation between non-stationary time series, the first step is to difference the series until a stationary series is found. This is basically the first thing you learn as an Econometrics student when you follow classes on Regression Analysis or Time Series Analysis. But differencing the time series to make them stationary is only one possible direction to come to a solution. And it comes at the cost of throwing away data that might identify long run relationships between the time series.

Another possibly better solution is to test whether the time series are cointegrated. If the cointegration test tells us cointegration exists, we can set up a model that is able to describe both the long run relationship and the short term corrections.

One of the things I noticed in the literature is that it's hard to find a basic method selection decision tree. I like to attack these kind of problems as structured as possible, so that the chance of actually finding meaningful relations increases while you also prevent yourself from misspecifying a model. In my search for a helpful framework, I found this useful article.

The framework as shown below is my slightly adjusted version that is based on the one I found. It will serve as a guide in the steps we will take. All the shapes that contain bold text, show the path we follow in case we like to construct a model to quantify the relation between stock-to-flow and price (or market cap). In the earlier articles (here and here) Nick and I both independently showed that both variables are first order integrated (after applying differencing we end up with a stationary series over time) and that cointegration couldn't be rejected by running different tests.

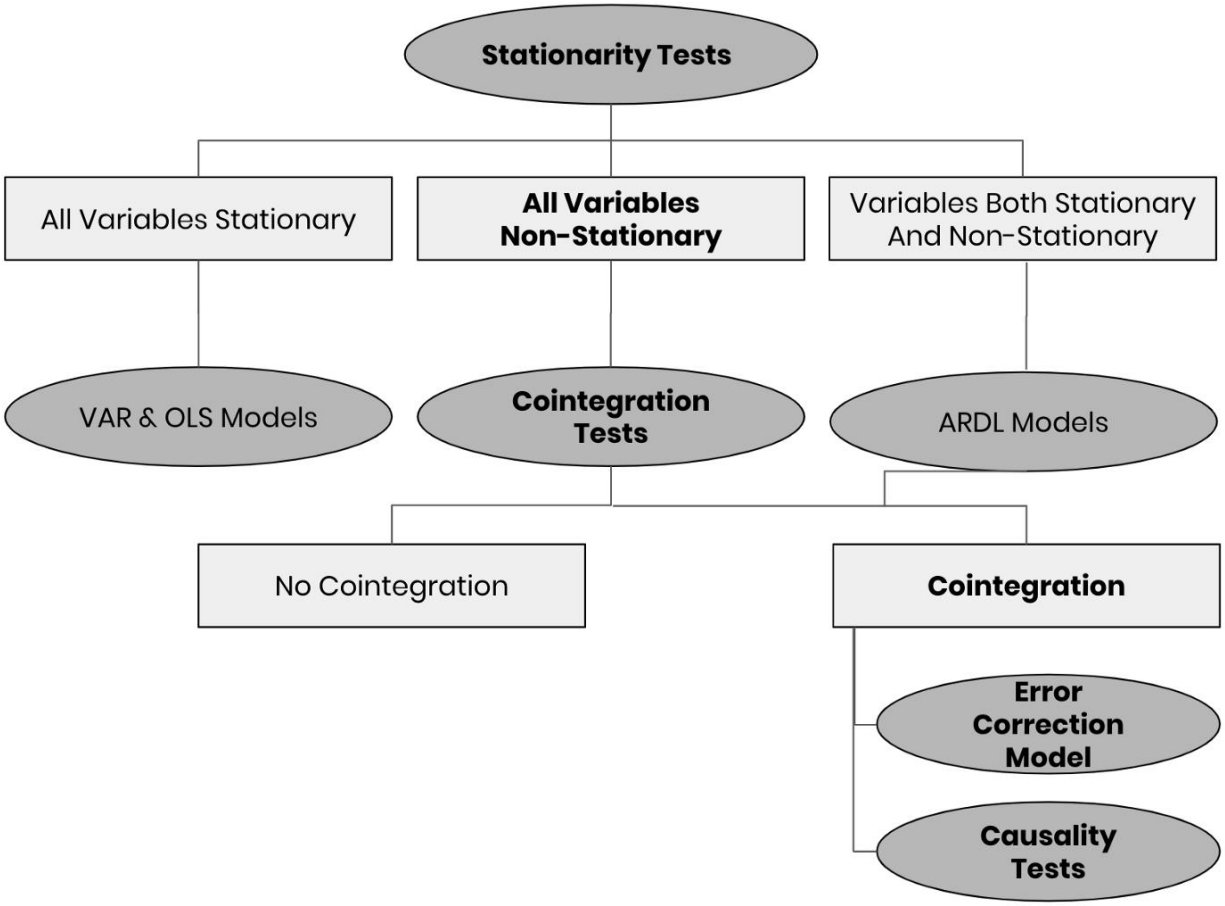


Fig 1: Simplified Model Selection Framework for time series analysis

Note that even though the overview above is far from complete, it offers a useful overview for those models that are often used. Most practitioners who use linear regression models, just go straight to the OLS models without even testing for stationarity. Using frameworks like these would be beneficial to many of them. It also helps people with less of a statistical background to check whether the beautiful model they have been introduced to was indeed the appropriate model to use.

Please also note that this overview is only about model selection and not about estimation of the model. I like to emphasise again that this overview is very simplified.

We found cointegration. Now what?

As cointegration couldn't be falsified, this means that the two variables are linked to form an equilibrium relationship spanning the long run. One of the issues though with the different cointegration tests is that some of them have weaknesses. Johansen (1988) addressed those and came up with an

improved cointegration test model, which is widely applied nowadays and incorporated in many different econometric software packages. Both Nick and I used that test in our model validation and we concluded that the model as introduced by PlanB couldn't be falsified.

If both the variables are first order integrated and there exists a cointegration relationship then we can derive an Error Correction Model. When both variables are put into a vector this can also more generally be referred to as a Vector Error Correction Model ('VECM').

Following the framework

First, I set up all the different equations, and briefly touch upon them. Keep in mind that the long term relation is what matters most in terms of showing us the road, and realise that the short term corrections are modelled to return to the middle of the road. In order to run a full blown analysis we need to define:

- the linear model
- the cointegration representation
- the error correction models for both S2F and BMC
- the models to run causality analysis

Setting up the model equations

If we consider the logarithm of bitcoin market cap ('Log(BMC)') as _Y _and we consider the logarithm of stock-to-flow ('LogS2F') as _X, _then the relationship between the two is written as:

$$Y_t = \alpha + \beta X_t + \epsilon_t$$

Equation 1: The Linear Model

Based on the representation theorem of Engle and Granger (1987), we rewrite the equation to display the cointegrating relationship:

$$\epsilon_t = Y_t - \alpha - \beta X_t$$

Equation 2: Cointegration Representation

Since both variables have their own Error Correction Models, I introduce them here:

$$\Delta Y_t = \alpha_Y + \rho_Y \epsilon_{t-1} + \sum_{h=1}^{l} a_{1h} \Delta Y_{t-h} + \sum_{h=1}^{l} b_{1h} \Delta X_{t-h} + u_{Y_t}$$

Equation 3: Error Correction Model for bitcoin market cap

$$\Delta X_t = \alpha_X + \rho_X \epsilon_{t-1} + \sum_{h=1}^{l} a_{2h} \Delta Y_{t-h} + \sum_{h=1}^{l} b_{2h} \Delta X_{t-h} + u_{X_t}$$

Equation 4: Error Correction Model for Stock-To-Flow

The first expressions at the right hand side of the Error Correction Model equations indicated by α are both stationary white noise processes for some number of lags _l. _In case we look at only at one period lag, the equations become:

$$\Delta Y_t = \alpha_Y + \rho_Y \epsilon_{t-1} + a_1 \Delta Y_{t-1} + b_1 \Delta X_{t-1} + u_{Y_t}$$

Equation 5: Error Correction Model for BMC with one lag.

$$\Delta X_t = \alpha_X + \rho_X \epsilon_{t-1} + a_2 \Delta Y_{t-1} + b_2 \Delta X_{t-1} + u_{X_t}$$

Equation 6: Error Correction Model for S2F with one lag

The coefficients in the cointegration equation are used to show the estimated long term relation among S2F and BMC. The coefficients in the Error Correction Models will provide more information on how deviations from that long term relation affect the changes on them in the next period. In this case ρ measures the speed of adjustment to the long term equilibrium. So, when the model runs away from the long term theoretical price, these coefficients tell us how fast we will return to it.

It's important to note that all equations above on their own, are just equations. I preferred to keep it readable, by not addressing the assumptions over and over again. In order to turn these equations into models we should say something about what assumptions are made regarding the errors. In case we like to use parametric estimation we have to either use 'the weak' or 'the strong' assumptions regarding the error. Under the weak assumptions we only make assumptions regarding the first 2 moments of the distribution, while under the strong assumption we define the entire distribution itself.

Causality Testing and required models

Since S2F and BMC are cointegrated, one of the following statements regarding this relationship will hold:

- S2F drives BMC,
- BMC drives S2F,
- or BMC and S2F drive each other

If S2F and BMC were not cointegrated, there would be no causal relation and the two variables would be independent. Granger (1969) has developed a causality test method that will enable us to determine the direction of the relationship. If current and lagged values of S2F improve the prediction of the future value of BMC, then it is said that S2F Granger causes BMC. And the opposite can be said as well.

The model equations that we build to test for the direction of the relation are shown below:

$$\Delta Y_t = \sum_{i=1}^{n} \alpha_i \Delta Y_{t-i} + \sum_{j=1}^{n} \beta_j \Delta X_{t-j} + u_{1t}$$

Equation 7: Model to test if X Granger causes Y

$$\Delta X_t = \sum_{i=1}^{n} \lambda_i \Delta X_{t-i} + \sum_{j=1}^{n} \delta_j \Delta Y_{t-j} + u_{2t}$$

Equation 8: Model to test if Y Granger causes X

In both cases we are testing the null hypothesis that beta and delta are equal to zero. If beta in equation 7 is equal to zero then X is not Granger causing Y (or LogS2F is not Granger causing LogBMC). And in equation 8 we test for delta being equal to zero.

Estimating the model coefficients

In order to estimate model coefficients we can either choose between parametric or non parametric approaches or some kind of combination of both. As stated by Green:

"Contemporary econometrics offers the practitioner a remarkable variety of estimation methods, ranging from tightly parameterized likelihood based techniques at one end to thinly stated nonparametric methods that assume little more than mere association between variables at the other, and a rich variety in between. **Even the experienced researcher could be forgiven for wondering how they should choose from this long menu.**" As a general proposition, the progression from full to semi- to non-parametric estimation relaxes strong assumptions, but at the cost of weakening the conclusions that can be drawn from the data.

The main reason to use a parametric estimation is that we can infer stronger conclusions (as long as assumptions are respected), because we use strong assumptions w.r.t. the distributions of the variables we analyse. At the other hand, the advantage of non parametric estimation is that we don't need to impose strong assumptions on the distributions of the variables we analyse, but we can just go with their actual distribution. As long as the actual distribution comes close enough to the imposed distribution, I would prefer to go with parametric estimation (like OLS estimation), but when the imposed distribution is not really a good match with the actual distribution, non-parametric estimation is preferred.

What's next?

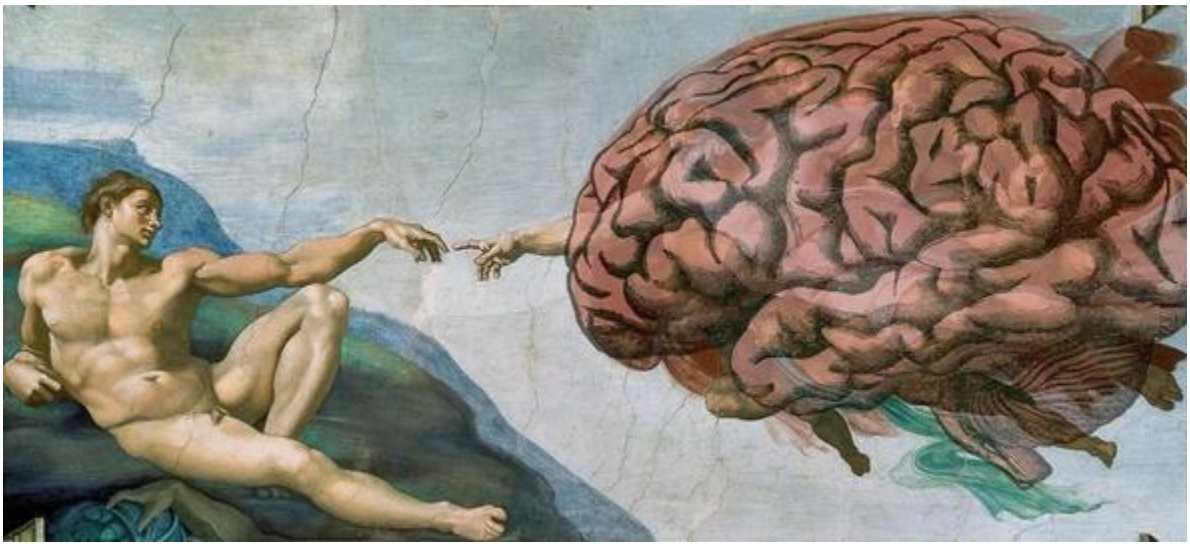
I intended to write a piece on the estimation of the VECM model coefficients, but actual estimation calculations are put on the ToDo list for now. This piece has been in draft mode for a while, so I decided to split up the content into a theoretical part and a more hands on estimation of the parameters. So, next in line is running some actual calculations on different estimation techniques and presentation of the results.

The Moral Philosophy of Bitcoin

Virtuous Habits and the Shameless Bitcoiner

By Prateek Goorha

Posted March 7, 2020



The Mind Behind the Memes

I. Bitcoin-ism

Bitcoin has provided us with a veritable catalog of concepts and ideas. As the essential merits of its framework have become more broadly understood; as ever more services have been developed to leverage its mechanisms for broader objectives; as its ecosystem has matured and become more varied and complex, discourse on Bitcoin has flourished.

Beyond technical concepts, there are simple ideas with astounding memetic resonance that have become tenets for a class of individuals who see themselves as ***true*** Bitcoiners : low time preference; hard money; store of value; #HODL; hyperbitcoinization; #stackingsats; “number go up”; Bitcoin not blockchain; stock-to-flow; digital gold; shitcoins, and a hundred others.

Each of these can, of course, be understood at several levels of comprehension. The same idea can be the basis for an amusing anecdote or meme; a more literary, artistic or even allegorical treatment; or the basis for a serious academic research paper or congressional hearing.

Who, then, is a true Bitcoiner?

Buying Bitcoin or having the loudest voice in the public squares does not make you a Bitcoiner. True Bitcoiners don't merely parrot the memes, they internalize their essential message, exert reason to understand and evaluate their merit and use those lessons to guide their own behavior.

True Bitcoiners don't merely parrot the memes, they internalize their essential message, exert reason to understand and evaluate their merit and use those lessons to guide their own behavior.

Bitcoin's popular memes are mere threads in a larger tapestry. They beguile with their simplicity, but they are pertinent to engaging with a broader unifying moral philosophy: An "-ism" of a kind, if you will.

We grapple and grope at this philosophy with these keywords because they make the ideas they are based upon more manageable for our limited attention spans or desire to acknowledge that we are participating in anything more substantive or revolutionary. Yet, even the keenest thinkers in the course of Bitcoin's history cannot be seen as wanting if they weren't and aren't able to completely unpack its every dimension.

Indeed, you would need to be a polymath of awesome capabilities to understand every aspect of what Bitcoin unleashes. That there ***is*** a larger human story to tell is evident to the extent that we see Bitcoin as exceptional, revolutionary, and unique. It is also why Bitcoin yields insights from eclectic treatments of its influence, including from computer science, anthropology, literature, economics, health, finance, political philosophy, and much else.

Why is this so? Why is it that Bitcoin plucks at so many strings that all seem to resonate with varying degrees within us?

In this piece, I wish to make a first step at tackling this overarching philosophy. It can only be a tentative attempt for I am no philosopher, nor do I think that **The Moral Philosophy of Bitcoin** is the bailiwick of any one individual anyway.

Nevertheless, I do think it is an interesting thought exercise, and one that makes clear that Bitcoin has a larger agenda, not merely for currency, economies or even for society, but in the story of human moral evolution. I make the task more manageable for myself by focusing attention here principally on the ideas of virtuous habits, risk and money, and examining how we can relate some of Bitcoin's popular ideas to them.

II. Virtue and Habits

Our conception of what a habit is differs in an interesting and revealing manner from how it was imagined by ancient philosophers and theologians.

For most of us, a habit is little more than an act or behavior that is regularly repeated and that has a low cost for its initiation. A habit is seen as something that is so intrinsically part of our routine that it assumes the place of an unquestioned norm. It is the default action without even so much as a thought on what the "default" and the "alternative" choice might even represent. The habit resides in our subconscious and, rather automatically, guides our actions and behavior.

This was expressly not the case for the ancients.

Aquinas, for instance, emphasized the idea of deliberative action in making the link between a habit and its virtue. Well before his time, the idea of *karma _had become central to the Aryan religions, Hinduism being the most famous among its several offshoots. To condense karma down to a mere habit sounds absurd, so well-wrapped it is in its initial connotation of deliberative action. Indeed, karma _is* a habit, but it is the habit of taking action in the knowledge of its repercussions in a world that is founded upon an under-girding law of universal causality.

Habit, seen as deliberate action, forces you to place emphasis on its virtue and how it shapes and molds one's mind. Such a habit leads you towards the development of what the Greeks called ***sophrosyne***, and regarded it as an ultimate virtue. Sophrosyne, like karma, is one of those words that defies a ready translation into English, but can be understood as a balance of mind that enables you to be master of your thoughts and action. Aristotle, in his Nicomachean Ethics conceptualized virtue as this balance of mind — as a subjectively-defined mean behavior that avoids extremes.

Arguably, we are all the poorer for having relegated the emphasis on deliberation in our habits. The ancients understood that it was only with the deliberate development of desirable habits that a mature and balanced mind can be developed; a mature mind, in turn, was indispensable to a loftier goal of leading a virtuous life, indeed even to salvation.

What, you may wonder, has all this got to do with Bitcoin?

As it turns out, a great deal. Bitcoin exerts its influence on Bitcoiners most keenly by reclaiming the idea of deliberate action as the basis of a habit, the repetition of which over time reveals its virtue.

The emphasis on burnishing the value of a low time preference, through repeated cycles of volatile markets, requires deliberate action taken to educate and tame the mind. To HODL, while all else around you capitulate is quintessential sophrosyne; HODL is karma to a Bitcoiner.

To HODL, while all else around you capitulate is quintessential sophrosyne; HODL is karma to a Bitcoiner.

Consider another area of life that Bitcoin has reclaimed for Bitcoiners: Risk.

III. Risk

A preference for taking on risk is commonly seen as a necessary condition for courage, fortitude, and manliness. To wit, our modern sensibilities regard courage and bravery as qualities that leave little room for stubborn restraint and inaction.

Yet, courage as a virtue _does _require a mature and reasoned relationship with risky action.

As a matter of fact, Aristotle regarded unthinking courage as a vice, and fear, in certain circumstances, as a virtue to be cherished. Once again, for Aristotle, it was a balance in behavior that shunned excesses in favor of deliberate thought and reasoned behavior that was truly indicative of virtuous courage. This restraint led one towards adopting an imperturbable and centered mind that lived by the principle of a “golden mean” in behavior that avoided the extrema — and was more amenable to achieving excellence of character, or *arete*.

With this Aristotelian basis for ideal behavior, then, let us look a little closer at the risk “profile” of an individual.

In economics, we learn that the curvature of a rational individual’s utility curve reflects the assumptions we make about their behavior. For example, to the extent that it is concave in wealth, the individual is risk averse, and will accept a certain outcome that is worth less than the expected value of a probabilistic outcome.

At first pass, this appears to be a sensible and preferable paradigm for behavior. Surely, the obverse of risk aversion — a preference for risk — where one is willing to pay to participate in the probabilistic outcome is reckless; it is the behavior of a compulsive gambler and is, potentially, ruinous.

However, risk aversion is not necessarily indicative of a virtuous habit of caution that has been cultured with care by a mature mind. Indeed, the acceptance of a certain payoff can be seen as folly when the probabilistic outcome, carefully considered, is more advantageous to oneself, one’s successors or the society one lives in.

Risk-averse individuals in such cases are clearly under-informed and display quite the opposite of a virtuous habit — immaturity, if not outright sloth. At the very least, they are willing to let their fear of failure override their mental faculties.

We arrive, therefore, at much the same sort of critique for risk avoidance as we did for risk preference that would offend Aristotle. Risk-averse behavior

can very easily be born from a virtue-less habit: An automatic predilection for seeking certainty rather than expending the effort of reason to examine and evaluate the complex alternative with its probabilistic outcomes.

There are two qualities that accord with the golden mean of behavior in the face of risk — qualities that are amenable to virtuous habits.

Prudence and Temperance

The expectations of risks materializing in our futures affects us differently to the extent that we have cultivated the virtuous habits of prudence and temperance. True Bitcoiners strive for both.

At the heart of the idea of prudence is our _sensitivity _to the risk. Mathematically, prudence is displayed by a positive third derivative of the utility function. Practically, prudence exists when we have a higher-order appreciation of risk and its effects on our future.

Prudence is a virtue in that it concerns itself with the judicious application of reason. It requires a maturity of mind. It requires the individual adjusting their behavior in the face of a risk rather than reacting directly to the situation. And, it requires adopting a precautionary motive that directs the individual towards accumulating more wealth when faced with a potential risk: precautionary saving is, after all, prudent behavior.

What if the independent sources of risks were to multiply? In such a case, a second virtuous habit, temperance, becomes especially important.

We need to understand that temperance is not some monastic vow. That association of temperance, usually given to it by injunctions placed by religious pronouncements, is unfortunate.

Temperance is an ability to self-regulate one's rate of prudence. In other words, temperance is the rational ability to both increase as well as decrease prudence.

A Bitcoiner, therefore, is a maximalist for the sound reason that, faced with an environment where the sources of risk multiply, temperance requires retrenching within Bitcoin and deliberately reducing exposure to other risks.

A Bitcoiner, therefore, is a maximalist for the sound reason that, faced with an environment where the sources of risk multiply, temperance requires retrenching within Bitcoin and deliberately reducing exposure to other risks.

“Temperance” by Luca Giordano

IV. Money

Every virtue must have a characteristic_mode_ through which the virtue redounds to the edification of the individual and to the benefit of society.

Money possesses several modes that are routinely used to describe its essential functions in society. Money, used in a particular mode, makes it more or less apposite to become the basis for a virtuous habit. It is in our ability to rank-order those modes such that its accumulation is concordant with a habit that exhibits temperance and prudence that virtue can be found.

Bitcoin’s merit as a long-term store of value is derived from strategic human behavior that is informed, disciplined and guided directly by immutable Laws of Nature.

Bitcoin’s merit as a long-term store of value is derived from strategic human behavior that is informed, disciplined and guided directly by immutable Laws of Nature. The cointegrated relationship between hashrate and difficulty acts as an Aristotelian anchor for a Bitcoiner’s habit; it serves as a shared golden mean for sophrosyne behavior.

It is hardly a leap of faith to aver that it is in its role as a medium for the preservation of value that Bitcoin is most conducive to virtuous habits. The reason is not hard to imagine if one considers the overarching role of prudence and temperance.

As a medium of transactional exchange a money cannot readily lend itself to virtue because, in this mode, rather obviously and definitionally, it advocates the ***minimization*** of prudence and temperance. It encourages a higher time preference, discounting the futures of individuals and their successors more heavily.

This difference is of vital importance and Bitcoin developed this thesis for money, in incremental steps, for true Bitcoiners.

V. Finally, yes, Bitcoiners are Shameless

One's engagement in a virtuous habit does not need validation from others. It is a pursuit that is its own reward; a deliberate action undertaken for the benefit it provides in shaping an individual's virtue.

A Bitcoiner should, therefore, seek a detachment from the diversions provided by social, economic and political distractions. This detachment comes at a cost, perhaps of being perceived as close-minded, stubborn and even solipsistic or it may come from being regarded as shamelessly adversarial.

When grounded in the pursuit of virtue, these slings and arrows should not dissuade a true Bitcoiner.

Consider that the philosophy of Cynicism is rooted in three qualities to which a genuine believer aspires:

1. Freedom of speech, or ***eleutheria***;
2. A self-assured indifference, or ***apatheia***, and
3. A desire for self-sufficiency, or ***autarkeia.***

While these qualities are inseparable with the social ethos of Bitcoin's overarching philosophy, Cynicism further roots the achievement of these desiderata with a need to inspire others in society to awaken from their stupor.

The word cynic is derived from the Greek word for a dog for the very obvious reason that the mode by which the Cynic sought to effect change in society was by assuming shameless, convention-flouting and subversive behavior, while living much like a simple ascetic, or just as a common dog might.

So, yes, a true Bitcoiner is shameless.

A true Bitcoiner is shameless.

"Diogenes sitting in his tub" by Jean-Léon Gérôme

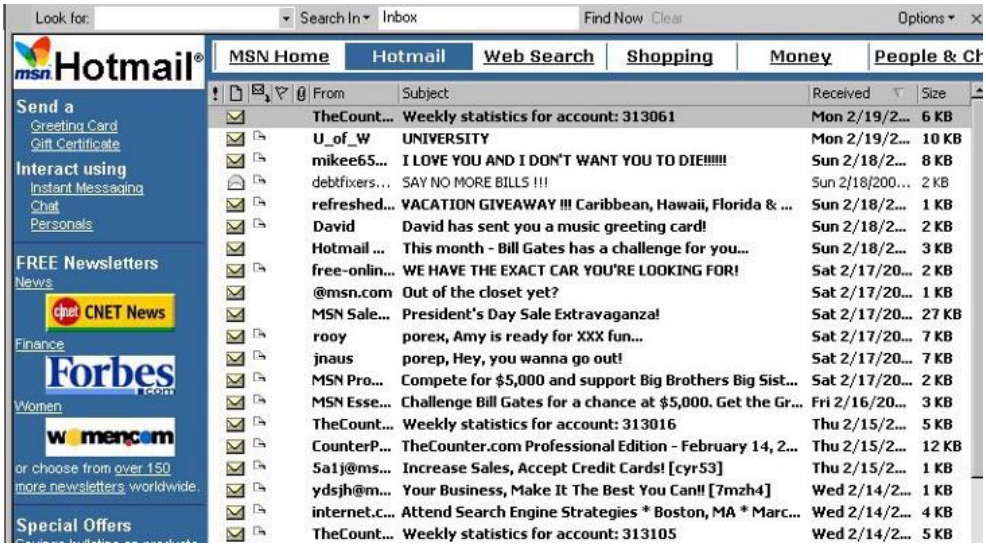
You don't care about, "The Price of the Internet" so ignore the price of Bitcoin

By Beautyon

Posted March 9, 2020

Bitcoin is a very new technology, even though the concept that it brings to life is decades old. The double spending problem has been solved; this means that it is possible to use a digital certificate to stand in the place of money and be sure that no one else can spend that certificate other than you as long as you hold it. This is an unprecedented paradigm shift, the implications of which are not yet fully understood, and for which the tools do not yet exist to fully take advantage of this new idea.

This new technology requires some new thinking when it comes to developing businesses that are built upon it. In the same way that the pioneer providers of email did not correctly understand the service they were selling for many years, new and correct thinking about Bitcoin is needed and will emerge, so that it reaches its full potential and becomes ubiquitous.



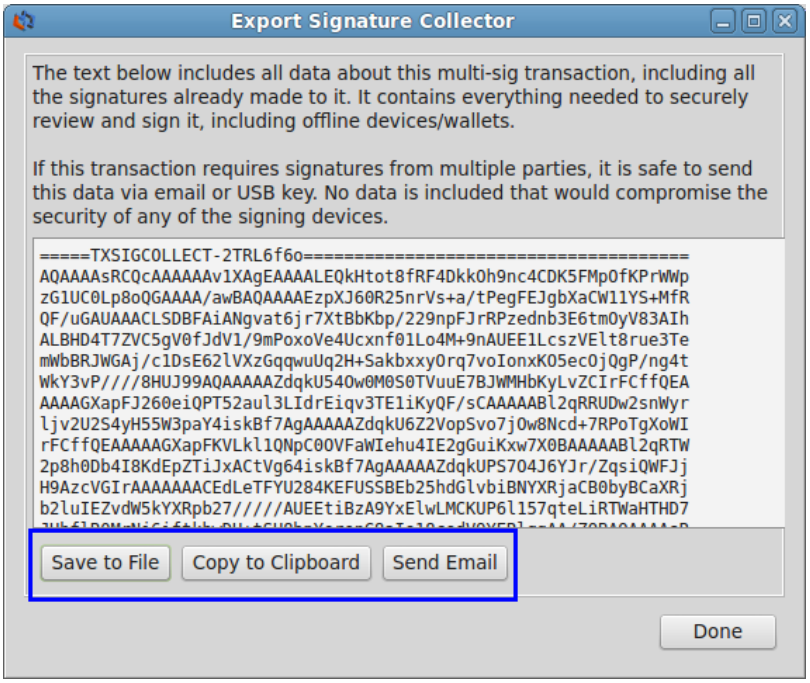
The original Hotmail Interface

Hotmail used familiar technologies (the browser, email) to create a better way of accessing and delivering email; the idea of using an email client like Outlook Express has been superseded by web interfaces and email 'in the cloud' that provides many advantages over a dedicated client with your mail in your own local storage.

Bitcoin, which will transform the way you transfer money, needs to be understood on its own terms, and not just as an online form of money. Thinking about Bitcoin as money is as absurd as thinking about email as

another form of sending letters by post; one not only replaces the other but it profoundly changes the way people send and consume messages. It is not a simple substitution or one-dimensional improvement of an existing idea or service.

As I have explained previously, **Bitcoin is not money**. Bitcoin is **a protocol**. If you treat it in this way, with the correct assumptions, you can start the process of putting Bitcoin in a proper context, allowing you to make rational suggestions about the sort of services that might be profitable based on it.



Every part of Bitcoin is text. It is always text, and never at any point ceases to be text. This is a fact, and as text, it is protected under the free speech provisions of the constitutions of civilised nations with guaranteed, irrevocable rights.

If Bitcoin is a protocol and not money, then setting up currency exchanges that mimic real world money, stock and commodity exchanges to trade in it is not the sole means of discovering its price. You would not set up an email exchange to discover the value of email services, and the same thing applies to Bitcoin.

Staying with this train of thought, when you type in an email on your Gmail account, you are inputting your 'letter'. You press send, it goes through your ISP, over the internets, into the ISP of your recipient and then it is outputted on your recipient's machine. The same is true of Bitcoin; you input money on one end through a service and then send the Bitcoin to your recipient, without an intermediary to handle the transfer. Once Bitcoin does its job of moving your value across the globe to its recipient it needs to be 'read out', i.e. turned *back into money*, in the same way that your letter is displayed to its recipient in an email.

In the email scenario, once the transfer happens and the email you have received conveys its information to you, it has no use other than to be a record of the information that was sent (accounting), and you archive that information. Bitcoin does this accounting on the block chain for you, and a

good service built on it will store extended transaction details for you locally, but what you need to have as the recipient of Bitcoin is _services _or _goods _not Bitcoin itself.

Bitcoin's true nature is as an instant way to pay (despite not being money) anywhere in the world. It is not an investment, and holding on to it in the hopes that it will become valuable is like holding on to an email or a PDF in the hopes it will be come valuable in the future; it doesn't make any sense.Of course, you ***can*** hold on to Bitcoin and watch its value go up, and its value _will_go up, but you need to have guts to weather the violent waves of selling and buying as the transition to an all Bitcoin economy gets under way. Remember also, that businesses that have a need to store Bitcoin need to be concerned about its value if their models are open ended and are exposed to the market. "Closed Circuit Bitcoin" models have control over everything and never need to worry about prices at exchanges. They can do all their business moving an unlimited amount of fiat with just a few Bitcoin.

Despite the fact that you can't double spend them and each one is unique, Bitcoins have no inherent value, unlike a book or any physical object. They cannot appreciate in value. Mistaken thinking about Bitcoin has spread because ***it behaves like money***, due to the fact it cannot be double spent.Misrepresentation of Bitcoin's true nature has masked Bitcoin's dual nature of being digital and not double spendable.

Razzles. They start as a candy, and then end as a gum. Before you chew them, which are they? A candy, or a gum?

Bitcoin is digital, with all the qualities of information that make information non scarce. It sits in a new place that oscillates between the goods of the physical world and the infinitely abundant digital world of information, belonging exclusively to the digital world but having the

characteristics of both. This is why it has been widely misunderstood and why a new approach is needed to design businesses around it.

All of this goes some way to explain why the price of buying Bitcoins at the exchanges **doesn't matter for the consumer.** If the cost of buying a Bitcoin goes to 1¢ This doesn't change the amount of money that comes out at the other end of a transfer. As long as you redeem your Bitcoin immediately after the transfer into either goods or currency, the same value comes out at the other end no matter what you paid for the Bitcoin when you started the process.

Think about it this way. Let us suppose that you want to send a long text file to another person. You can either send it as it is, or you can compress it with zip. The size of a document file when it is zipped can be up to 87% smaller than the original. When we transpose this idea to Bitcoin, the compression ratio is the price of Bitcoin at an exchange. If a Bitcoin is $100, and you want to buy something from someone in India for $100 you need to buy 1 Bitcoin to get that $100 to India. If the price of Bitcoin is 1¢ then you need 10,000 Bitcoin to send $100 dollars to India. These would be expressed as compression ratios of 1:1 and 10,000:1 respectively.

The same $100 value is sent to India, whether you use 10,000 or 1 Bitcoin.The price of Bitcoins ***is irrelevant to the value that is being transmitted***, in the same way that zip files do not 'care' what is inside them; Bitcoin and zip are dumb protocols that do a job. As long as the value of Bitcoins does not go to zero, it will have the same utility as if the value were very 'high'.

Bearing all of this in mind, it's clear that new services to facilitate the rapid, frictionless conversion into and out of Bitcoin are needed to allow it to function in a manner that is true to its nature.

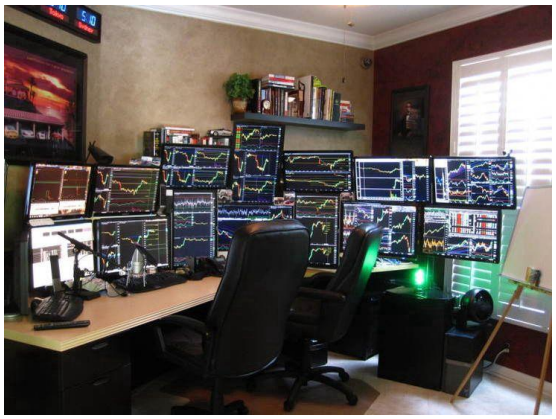
The current business models of exchanges are not addressing Bitcoin's nature correctly. They are using the Twentieth Century model of stock, commodity and currency exchanges and superimposing this onto Bitcoin. Interfacing with these exchanges is non-trivial, and for the ordinary user a daunting prospect. In some cases, you have to wait up to seven days to receive a transfer of your fiat currency after it has been cashed out of your account from Bitcoins. Whilst this is not a fault of the exchanges, it represents a very real impediment to Bitcoin acting in its nature and providing its complete value.

Imagine this; you receive an email from across the world, and are notified of the fact by being displayed the subject line in your browser. You then _apply _to your ISP to have this email delivered to you, and you have to wait seven days for it to arrive in your physical mail box.

The very idea is completely absurd, and yet, this is exactly what is happening with Bitcoin, for no technical reason whatsoever.

It is clear that there needs to be a re-think of the services that are growing around Bitcoin, along with a re-think of what the true nature of Bitcoin is. Rethinking services is a normal part of entrepreneurialism and we should expect business models to fail and early entrants to fall by the wayside as the ceaseless iterations and pivoting progress.

Bearing all of this in mind, focusing on the price of Bitcoin at exchanges using a business model that is inappropriate for this new software simply is not rational; its like putting a methane breathing canary in a mine full of oxygen breathing humans as a detector. The bird dies even though nothing is wrong with the air; the miners rush to evacuate, leaving the exposed gold seams behind, thinking that they are all about to be wiped out, when all is actually fine.



Day traders speculating on Bitcoin from home cause the price to oscillate. Its an artificial signal that has nothing to do with demand for Bitcoin and its circulation as an economic tool to facilitate commerce.

Bitcoin, and the ideas behind it are here to stay. As the number of people downloading the client and using it increases, like Hotmail, it will eventually reach critical mass and then spread exponentially through the internet. When that happens, the correct business models will spontaneously emerge, as they will become obvious, in the same way that Hotmail, Gmail, Facebook, cellular phones and instant messaging seem like second nature.

In the future. I imagine that very few people will speculate on the value of Bitcoin, because even though that might be possible, and even profitable, there will be more money to be made in providing easy to use Bitcoin services that take full advantages of what Bitcoin is.

One thing is for sure; speed will be of the essence in any future Bitcoin business model. The startups that provide instant satisfaction on both ends of the transaction are the ones that are going to succeed. Even though the volatility of the price of Bitcoin is bound to stabilise, since it has no use in and of itself, getting back to money or goods instantly will be a sought after characteristic of any business built on Bitcoin.

The needs of Bitcoin businesses provide many challenges in terms of performance, security and new thinking. Out of these challenges will come new practices and software that we can only just imagine as they come over the horizon.

Finally, when there is no more fiat, and the chaotic transition zone between fiat and Bitcoin has been abolished, then everything will be priced in Bitcoin, and there will be no volatility, because no one uses anything other than Bitcoin to buy or sell. If you know any chemistry, this will be like a reaction's reagents reaching equilibrium; you can shake it and stir it all you like; the reaction is over, and you're left with the inert product. Right now, compared to the amount of fiat in the world, Bitcoin can expand and contract very rapidly over a large range, because it is small in volume. It can expand to what for many is an unimaginably high price, and then shrink down again. As it gets bigger and accumulates more mass (its price expressed in fiat), these fluctuations will become smaller and smaller. Through all of this, Bitcoin remains exactly the same; it is its users that are publishing numbers as a signal to react upon.

If you like the content and feel so obliged to send some love via BTC donations you can do so at the address below:↴

1BhmrHqe6utNARK3xvTDX3pnGrPAL9GcK

The Bitcoin Diaspora, A Confederation of Tribes

By Joe Rodgers

Posted March 11, 2020

Introduction

"There is no Bitcoin community" - Everyone

This is the battle cry of true-believers and deniers alike. There is no CEO, PR, or speaker for Bitcoin. Bitcoin is decentralized, so there is none of that. So why do people get triggered so easily when people utter the phrase "Bitcoin community"?

Surely there is something, but what is it?

During Bitcoin's short existence, it has grown from a small cryptography email list to a globally traded money with a $100B+ market cap. How can something like this happen with no "Bitcoin community".

Surprisingly, there is "no Bitcoin community" but there is a Bitcoin diaspora, a confederation of tribes.

To fully understand this social phenomenon, we must have a basic understanding of these concepts: **diaspora, tribes, specialization and disciplines, and confederation**. This will not satisfy all critics, but the aim is to present a mental model we can use when describing all individuals and communities that use Bitcoin.

What is a Diaspora

A quick search on the internet will yield many different definitions for diaspora. Traditionally, the word has been reserved for describing the dispersion of Jews beyond Israel but it is now commonly used to describe the scattering of people away from their homeland.

While traditional diasporas are rooted in the physical world, the Bitcoin diaspora is rooted in the digital world. Over time, we have witnessed the transformation of the Bitcoin diaspora into a hybrid of both physical and digital worlds.

From the beginning of Bitcoin's creation, users were geographically scattered but shared a common digital home via the Cryptography Mailing List.

The original cryptography mailing list members eventually scattered to join other digital communities and even made joined communities in the physical world via meetups, conferences, business, and educational institutions. Once Bitcoin users made the jump to connect in the physical world, the Bitcoin diaspora transformed from being digital to a hybrid diaspora, which is a special characteristic of this social phenomenon.

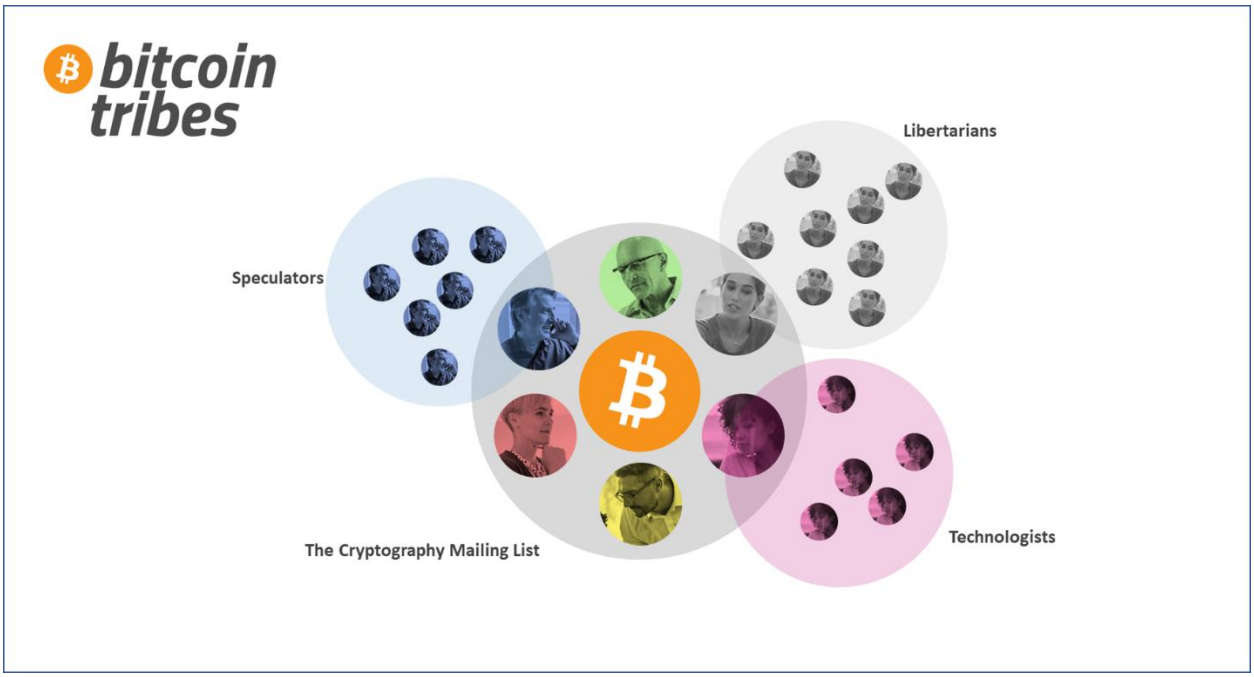
As their numbers grew, so too did the Bitcoin diaspora voice and influence. Finally, a natural tribe would form which we'll get to in the next section.

A great example of this scattering is their infiltration within Libertarian circles. For decades, Libertarians fought for sound money and more liberty, and for decades they cheered for a return to the gold standard and limited government. Libertarians never had a way to bring change because they needed permission from the state. Then along came Bitcoin. Some core principles of Bitcoin are sound monetary policy and it's permissionless nature. Diaspora members began to infiltrate libertarian circles and share their domain knowledge of Bitcoin. Libertarians soon discovered those core monetary principles and found they were in alignment with theirs. As a result, we now have a blossoming knowledge base centered around Bitcoin and Libertarianism.

The scattering of the Bitcoin diaspora has resulted in countless physical and digital tribes. As the diaspora continues to grow and mature, we will see more organization and representation.

Tribes

Tribes come in all shapes and sizes but share common characteristics. Tribes are connected people that share an idea. Tribal needs are communication and a way to share ideas. As tribes mature natural leadership begins to form. Leadership delivers better organization and communication.



One of man's most powerful survival mechanisms is to be a part of a tribe. The opportunity to give and to receive from a tribe of like-minded individuals and to learn from a leader give him a sense of fulfillment. But man is not satisfied with one tribe, he desires to be in many. That is why you probably are a member of many social networks, organizations, and smaller groups.

The Bitcoin diaspora began as a single tribe with a small group of members in the Cryptography Mailing List, but naturally, the members shared and explored the idea of Bitcoin. From that moment, tribes began to form groups outside the mailing list.

As mentioned earlier, a popular example of a tribe is the Libertarian Bitcoiners, but there are many more great examples. One of the earliest tribes that are still around today is the Bitcoin Talk forum. This was the early place where Bitcoin ideas were shared and sharpened. Wild speculation, how-to's, and fud were all hashed out within this tribe. There are more than 30 local meetups for Bitcoin, many developer communities on GitHub, and Bitcoin tribes are forming across every social network.

The expansion of Bitcoin tribes is a powerful example of Bitcoin's network effects. The scattering is a positive feedback loop as Bitcoin is strengthened as the network grows and tribes grow the network.

Specialization and Disciplines

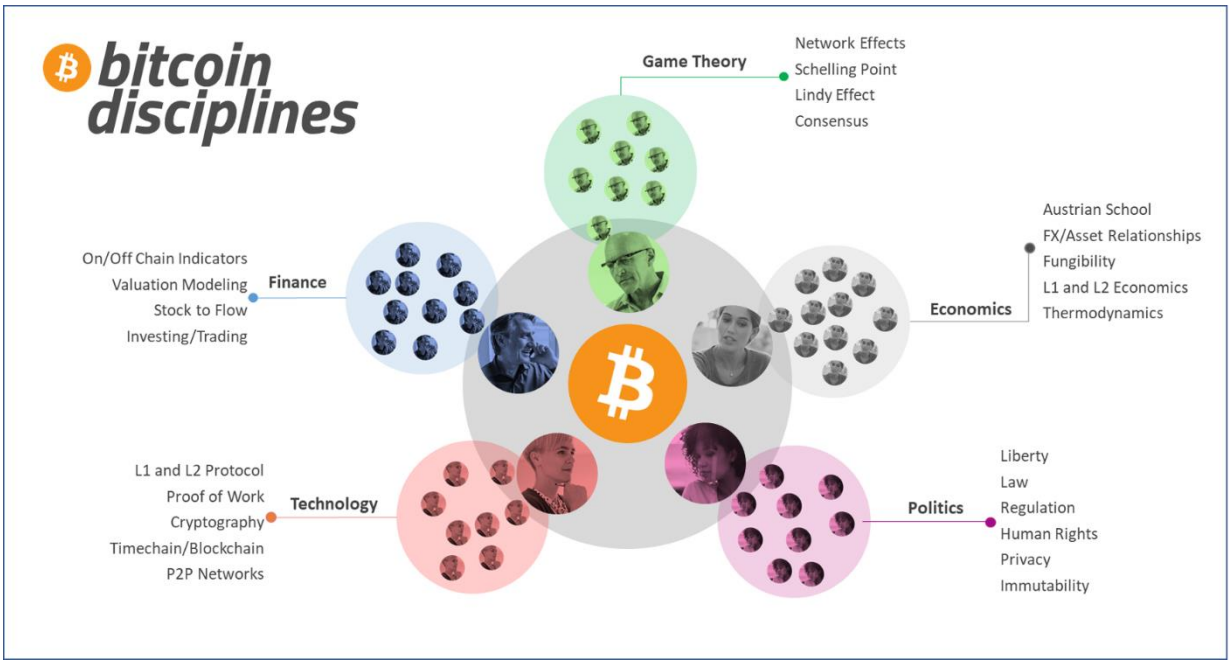
When mankind leaps forward, it's the result of new knowledge. New knowledge is the product of specialization which occurs when productivity is focused along different skills. Since Bitcoin is decentralized, advancement relies on the shoulders of the tribes and tribal members. Since tribal members are free to work on whatever they choose, this leads to more specialization because they can focus their energy where they are most productive.

Within a specific tribe, there is domain knowledge which makes tribes a breeding ground for specialization. Tribal members peer review, share, critique, and advance knowledge specific to their tribe. This process is another example of a positive feedback loop for Bitcoin. Tribes develop specialization, which adds to the overall value of Bitcoin.

Once a person with domain knowledge got their mind on Bitcoin, they tended to see the world through a new lens, and this outcome was specialization.

"I believe that Bitcoin is a mirror - it reflects who you are; it reflects your beliefs." Gigi

Domain experts began crafting new ideas and narratives around Bitcoin. Over time, this specialization has led to the deep study and exploration of Bitcoin which has produced various Bitcoin disciplines. Bitcoin disciplines are branches of knowledge dedicated to understanding Bitcoin.



Disciplines are like schools within a university. They encompass an overall idea or school of thought and have deep focus areas that add to the understanding of that discipline. As you can see from the chart, Bitcoin disciplines are developing along conventional schools of thought, however, specialization is developing which further the understanding of how Bitcoin relates to that discipline.

Once the Bitcoin diaspora scattered out beyond the cryptography mailing list, Bitcoin was exposed to people with different areas of expertise. Tribes formed which led to specialization and disciplines. This all happened organically and is another example of how the Bitcoin diaspora is influencing the world.

These disciplines might look familiar at first glance, but once you dig into the writings, code, and other knowledge created, you will find that Bitcoin is changing us far more than we are changing it.

Confederation

Let's now dig into the final aspect of the Bitcoin diaspora, confederation. The most useful definition of confederation is an organization that consists of several tribes united in an alliance. History has many examples of tribal confederations from the Iroquois to the Mayans. Each tribe had its values, norms, and leaders, and they found strength in an alliance.

The tribes of the Bitcoin diaspora are like these native confederations of the Americas. Although there are no formal alliances in the Bitcoin confederation, tribes and tribal members all share a belief in this informal alliance.

But what forges this alliance? That is the beauty of Bitcoin. It means many things to many people. For some, it is as simple as sound money and for others, it is their path to riches. Interpretation is up to the individual, but it can be summarized as **a shared desire for Bitcoin to succeed**.

The strength of the confederation is in the tribe and tribal members and vice versa. This is another example of a positive feedback loop.

- As individuals are on-boarded to tribes →
- those tribes create more specialization →
- which benefits the confederation →
- which brings more value to bitcoin →
- Loop repeats

Through scattering and specialization, the diaspora has spawned many tribes that share ideas, norms, and values, and they all work as an informal confederation.

Conclusion

The Bitcoin diaspora has already changed the world and will continue to bring positive changes to humanity. With each epoch, new waves of innovation and users join the Bitcoin diaspora. As new technology is unlocked, this will bring in more areas of study and new disciplines.

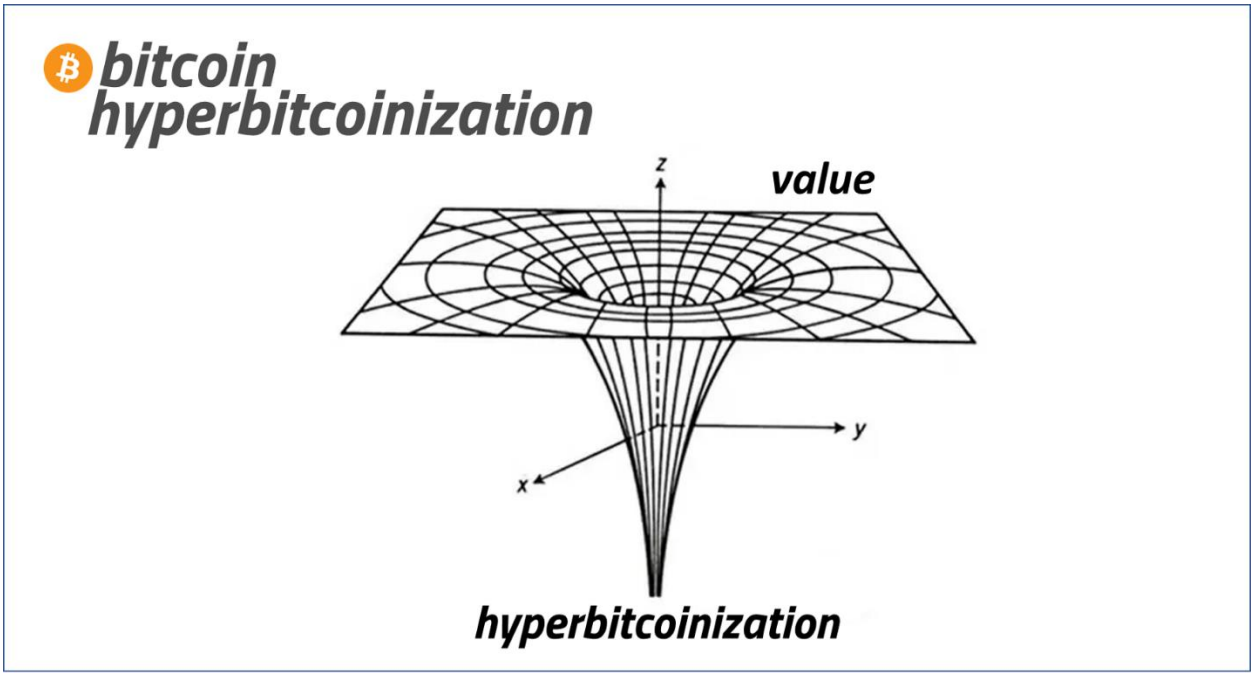
Tribal communication will change rapidly over the next decade as VR and AR technology is brought to the mainstream. Already today, we are seeing primitive Bitcoin meetups in VR. As VR technology is improved, this will unlock new levels of human communication and collaboration. Tribes will continue to meet in the real world, but VR will become more and more common and eventually will be the norm. Better tools will lead to the better communication of ideas and more rapid specialization.

Over the next decade, we will see the creation of many new tribes. Some will be unthinkable because they will be dedicated to technology not yet created. Today, we are witnessing new tribes being developed such as the Bitcoin Artists and the Bitcoin Religion.

There are already Bitcoin Artists, but they are just now getting organized. This tribe is already spreading the ideas of Bitcoin through art and is on the cutting edge of technology creating digital and physical art the world has never seen or imagined.

The Bitcoin Religion is an emerging meme within the Bitcoin diaspora. While this might be laughable to some, this is rapidly becoming a more common idea within existing Bitcoin tribes. As more ideas are created and shared around Bitcoin religion, the tribe will find itself. It too will bring value to Bitcoin through self-betterment.

The Bitcoin diaspora will continue to scatter as Bitcoin makes its way into more and more areas of study and human life. Tribes will organize and the confederation will be strengthened. This will ultimately lead to hyperbitcoinization.



Eventually, we will reach a point of hyperbitcoinization which is when Bitcoin is the global currency. This will trigger a switch in mindset for humanity. Humans will no longer think with shorter time preference. Human action will be shifted from inflationary money as a store of value to deflationary money as a store of value. This will make all human actions weighed with longer time preferences. Once hyperbitcoinization is achieved, the Bitcoin diaspora will be the global human tribe, because Bitcoin will be the global currency.

In the hyperbitcoinization period, there will still be tribes of innovators working to improve Bitcoin and their discipline, but for the common man, it will be an afterthought. The common man will use Bitcoin and act with a longer time preference. He will be changed by Bitcoin. He will become a better man.

Thanks

Thank you, David, for your early conversation and review. Thank you, Gigi, for your review and encouragement.

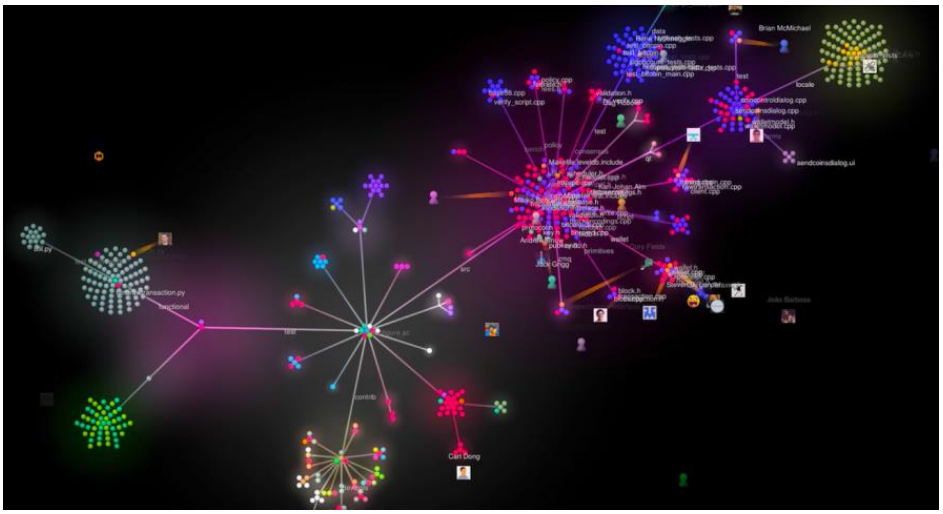
Supplemental Resources

- Satoshi Nakamoto Institute
- bitcoin-only
- 21 Lessons
- Lopp's Bitcoin Resources
- WORDS Bitcoin Journal

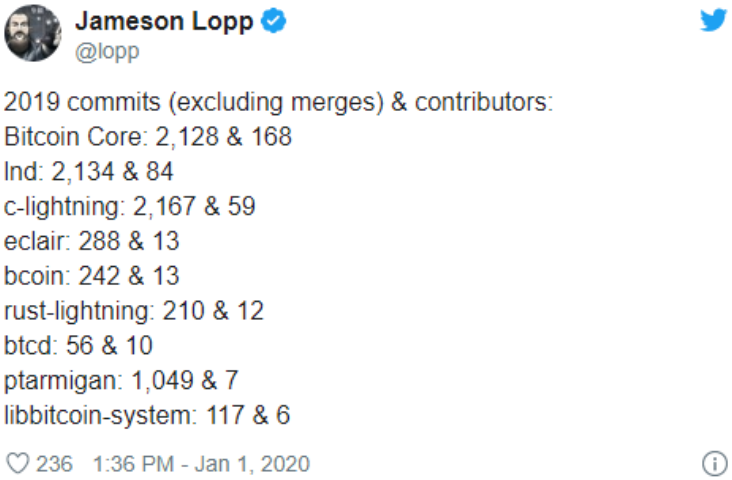
Bitcoin Core Contributor Challenges

By Jameson Lopp

Posted March 14, 2020



Bitcoin Core is an open source project that is the schelling point for development of the Bitcoin protocol; it is often referred to as the "reference implementation" because it is by far the most mature Bitcoin software with more contributors and activity than any other implementation by far. While it has changed names and even platforms several times, it is the original organization started by Satoshi Nakamoto.



But Bitcoin Core isn't like most open source projects. It's mission critical software than is relied upon by many individuals and enterprises in what has grown to be a $100+ billion network. Bitcoin Core is not developed in the same manner as your average consumer software; it's more akin to aerospace engineering. The stakes are high and tolerance for even the most minor failure is incredibly low due to the potential for catastrophe. If you speak to Core contributors who have been participating for many years, they tend to agree that the quality control of code review and testing has increased enormously over the past decade.

As such, the bar has been raised for anyone who wishes to have their code merged into the repository.

If you wish to better understand the dynamics of how Core operates as an organization, check out Who Controls Bitcoin Core? I also have several guides about contributing to Bitcoin Core linked in my educational resources.

Pull Request Stats

Note that in late 2011 the Bitcoin project migrated from SourceForge to Github - for simplicity I'm ignoring any rejected PRs that occurred during the SourceForge era. It's not clear to me if it's even possible to find them. At time of writing, Bitcoin Core has:

- 337 open PRs
- 8,431 closed merged PRs
- 4,014 closed unmerged PRs

Thus 32% of pull requests end up being abandoned / rejected (or re-proposed differently.)

Merged Pull Request Stats

Thankfully it's quite simple to query git to aggregate stats for the code that made it into the repository.

```
$ git log –no-merges –all –pretty=tformat: –numstat | awk '{inserted+=$1; deleted+=$2; delta+=$1-$2; ratio=deleted/inserted} END {printf "Commit stats:\n- Lines added (total): %s\n- Lines deleted (total): %s\n- Total lines (delta): %s\n- Add./Del. ratio (1:n): 1 : %s\n", inserted, deleted, delta, ratio }' -
```

Based upon all historical commits (excluding merge commits):

- Lines added (total): 2,167,565
- Lines deleted (total): 1,483,481
- Total lines (delta): 684,084
- Added / Deleted ratio (1:n): 1 : 0.6844

Unmerged Pull Request Stats

But now we need to figure out how many PRs have been closed without being merged!

We've already determined that there are a little over 4,000 unmerged PRs at time of writing. But how many lines of code would these PRs have changed if

merged? GitHub has an API for that, though perhaps there's a library that can help us use it more easily! Let's give PyGithub a shot...

After a bit of trial and error, here's what I came up with: https://gist.github.com/jlopp/5aa87ed33e97ad58f54ace65e9b0ece3

Unfortunately, while Github's UI allows us to filter out merged pull requests, it appears the API does not. So we need to iterate over all 12,000+ PRs to count the lines of code from the unmerged ones. It turns out that Github limits API calls to 5,000 per hour, so this operation requires us to throttle the script to spread itself out across 2+ hours.

The Results

After iterating all rejected pull requests from Bitcoin Core we find that there were:

- 9,011,209 total rejected added lines of code
- 6,279,435 total rejected deleted lines of code

That's 15,290,644 rejected lines of code changed vs 3,651,046 accepted!

Which means that as of time of writing, only 19% of proposed changed lines of code have been accepted into Bitcoin Core.

Top Contributor Stats

What if we drill down a bit more to the individual level? Clearly some contributors are better than others at navigating the (often arduous) process of seeing a proposal through to completion.

- *Wladimir van der Laan - 88% PR merge rate* 737 merged PRs 104 unmerged PRs
- *Pieter Wuille - 87% PR merge rate* 600 merged PRs 90 unmerged PRs
- *Marco Falke - 85% PR merge rate* 733 merged PRs 133 unmerged PRs
- *Matt Corallo - 77% PR merge rate* 290 merged PRs 88 unmerged PRs

What about notable contributors who have stopped contributing after scaling contention?

Jeff Garzik - 58% PR merge rate 88 merged 63 unmerged *Mike Hearn - 57% PR merge rate* 8 merged 6 unmerged *Gavin Andresen - 80% PR merge rate* 180 merged 43 unmerged

Gavin's stats are high but I wondered if that was due to his early involvement and if there was a noticeable trend leading toward his departure. It turns out there is indeed:

2012: 91% PR merge rate (49 out of 54 PRs) 2013: 86% PR merge rate (60 out of 70 PRs) 2014: 81% PR merge rate (29 out of 36 PRs) 2015: 59% PR merge rate (10 out of 17 PRs) 2016: 0% PR merge rate (0 out of 5 PRs)

Did Gavin become a worse programmer over the years? That seems pretty unlikely. Rather, I suspect that this is evidence of Bitcoin Core's quality standards increasing in rigor.

Takeaways

- Bitcoin Core has high standards; a significant portion of code changes are abandoned or rejected.
- There's evidence that supports the theory that code standards have increased over the life of the project.
- It appears that a PR rejection rate of under 70% is a sign that a contributor will get frustrated and stop contributing.

There's certainly opportunity to dig further into this phenomenon, but I think this is a good start!

A Treatise On Bitcoin And Privacy Part 1: A Match Made in the Whitepaper

By Giacomo Zucco

Posted March 18, 2020

Introduction

How one's focus can shift in just two weeks! While today everybody in the Bitcoin space seems more concerned with price fluctuations in response to the global financial panic (understandably so), it's important to remember perennial issues that never go away, like the importance of maintaining your privacy when you transact in bitcoin. Throughout this month especially, we've been hearing reports of KYC/AML-compliant exchanges freezing user accounts due to suspected use of CoinJoin software (more on that later), followed by yet another case of a famous and respected early Bitcoin proponent promoting his new illiquid altcoin as something that "will replace Bitcoin, which isn't private enough!"

If you want to take a short break from global pandemics, financial meltdowns and price volatility, here's an attempt at analyzing claims, facts and context of this latest "Bitcoin drama." To begin with, in Part 1 of this two-part series, we'll start by looking at the fundamental relationship between Bitcoin and privacy by going back to the beginning with the whitepaper. Then, in Part 2, we'll focus on some the ways that Bitcoin privacy is being maintained and improved upon — and strike down a few "red herrings."

Money Needs Privacy

Bitcoin is designed to perform monetary functions, and money needs a strong separation of personal identity from specific monetary units and transactions in order to work sustainably at scale. There are at least two fundamental components to this separation.

Deniability

We could call the first component "deniability." This describes the possibility for an individual using a monetary tool to credibly deny any connection with it later on.

The reason for this is that money has been developed to facilitate individual saving and voluntary exchange among people. But the positive-sum game of voluntary exchange is not the only way to increase one's wealth: The other

way is the negative-sum game of violent confiscation. As the sociologist and political economist Franz Oppenheimer brilliantly put it, there are two different paradigms for wealth acquisition within societies:

“These are work and robbery: one’s own labor and the forcible appropriation of the labor of others. I propose in the following discussion to call one’s own labor and the equivalent exchange of one’s own labor for the labor of others, the economic means for the satisfaction of needs, while the unrequited appropriation of the labor of others will be called the political means.”

While the temptation to resort to political means is always present in extended social contexts, it becomes particularly strong when money is involved: The same features that make money an especially good tool for exchange and for storing economically acquired wealth make it also particularly interesting as a target of confiscation — and as a way to store politically acquired wealth.

Individuals exchanging and storing money are more easily and more often targeted by political rent-seekers, since it’s most efficient to rob them than to rob participants in simple barter or insulated hermits who don’t exchange at all. Quite often political organizations prefer to present confiscation as conditional upon the specific type of exchange engaged in by the victim: taxes, imposts, tolls, tariffs, tributes, fines, bribes, penalties, excise duties, protection money, etc.

Privacy in communication is important, and economic exchanges are among the most important, sensitive, private and potentially dangerous forms of communication in adversarial environments. Money talks. Somebody whose financial and commercial life is completely exposed runs a higher risk of suffering robbery, blackmail, kidnapping or political expropriation.

For all these reasons, it becomes paramount for economic agents to be able to detach their own public identity from the specific monetary transactions they have taken part in and, thus, to be able to deny such connection.

Fungibility

The second component is called “fungibility.” By this, we mean the possibility for an individual receiving a monetary tool to safely ignore any connection between that tool and any particular individual or use case it interacted with in the past.

Fungibility is more an economical category than a political one: It basically means that any random amount of money is practically indistinguishable from any other, thus making the validation cost for a money receiver way lower. One $50 bill is as good as any other, and you don’t need to know who

has used it in the past in order to accept or use it as payment today. Indeed, if a receiver had to evaluate the history of every individual unit before being able to assess its value, verification costs would increase exponentially.

Ironically, one of the relatively recent trends of "Know Your Customer" regulations around the world is, indeed, that money was mostly adopted as a way for merchants to avoid knowing (and trusting) their customers! Customers are already somehow required to "know their merchant," since they have to trust them about the quality and the dependable delivery of the product or service they purchase. But merchants, when they scale up from trivial systems of barter or credit to actual markets, use money to be free from the burden of knowing all their customers. "KYC" regulation is just a political control tool marketed with a paradoxical expression which exudes economic illiteracy.

This isn't an ideological problem but a functional one: A good cannot easily pass over many hands (as a monetary good is required to do) if every current receiver has to verify the entire political status of every previous owner in order to know how much political risk (including persecution, censorship, taxation, debt) he is actually inheriting. Non-fungible goods can't work as money.

Some goods are ideal for mitigating both deniability and fungibility problems: "bearer instruments" which don't carry the personal information of previous owners, making it easy for everyone to deny having been involved in any specific transaction.

Bitcoin: Born for Privacy

Satoshi Nakamoto created Bitcoin as a tool for privacy. The entire cypherpunk quest, which Satoshi was an active part of and which the Bitcoin experiment is the coronation of, was all about personal and financial privacy. Most of the early messages and publications by Satoshi (including the famous whitepaper, which devotes a paragraph to it) are heavily concerned with its privacy features.

The first consideration made in the whitepaper about privacy is that centralized online payment intermediaries are easy targets for regulation. As such, it is easy to push these intermediaries to actively mediate disputes and thus to make most transactions reversible. This requirement, as a consequence, forces merchants, scared by risks of chargebacks, to be very "wary of their customers, hassling them for more information than they would otherwise need." Merchants get pushed back to the "KYC paradox" once again. Being decentralized and impossible to regulate, Bitcoin cannot be forced to actively mediate disputes. For this reason, Bitcoin transactions

can quickly become irreversible, making any inquiry into the personal identity of a payer absolutely redundant and unnecessary.

The second consideration concerns the fact that Bitcoin's base layer (the "timechain," developed to avoid double-spending without the need of a trusted third party) requires the publication of every settlement transaction, thus limiting the chance to apply the traditional "privacy through obscurity" technique of centralized providers. This limitation is mitigated by the anonymity of the cryptographic public keys, which are intended to be used only once, without any association with identities to work. In Satoshi's words, "The traditional banking model achieves a level of privacy by limiting access to information to the parties involved and the trusted third party. The necessity to announce all transactions publicly precludes this method, but privacy can still be maintained by breaking the flow of information in another place: by keeping public keys anonymous. The public can see that someone is sending an amount to someone else, but without information linking the transaction to anyone. This is similar to the level of information released by stock exchanges, where the time and size of individual trades, the 'tape,' is made public, but without telling who the parties were."

Privacy and Trust: All or Nothing

An interesting feature of this transparent setting, discussed by Satoshi and by many other early Bitcoin contributors and researchers, is the all-or-nothing nature of its privacy guarantees. A trusted third party can, indeed, promise to keep your sensitive information safe from potential kidnappers, robbers or stalkers, while still being forced to provide any detail to more powerful political entities (nation-states with their tax agencies, financial authorities, secret services, etc.).

In a (pseudo)anonymous but public setting, it's safe to assume that in every case where the latter type of adversary is able to access sensitive financial information, the former type will find a way as well. When somebody's privacy on the timechain is broken, it is broken to the benefit of all snoopers with an internet connection: governments, bandits, hackers, business competitors, personal enemies, haters, ex-spouses, etc. This should serve as a strong incentive for users to protect their "on-chain" deniability, thus protecting fungibility for all.

Bitcoin base-layer transactions, on the other hand, already show perfect fungibility internally. What this means is that, although every transaction is public, there is no public data about who, within a certain transaction, was in control of the private keys that spent a specific input, or who is now in control of the private keys that will spend a specific output.

Bitcoin's rules assure us that the total amount of satoshis spent with all the inputs is equal to or less than the total amount of satoshis "locked" in all the outputs (transaction can't create inflation, they can only leave out "blockspace fees" for miners). But there's technically no way to be sure, from public timechain data alone, if a transaction with 10 inputs and 10 outputs is moving satoshis from one payer to ten payees, or from two payers to one payee, or from one entity to himself. Of course, some probabilistic inferences are possible, based on heuristics and common patterns, but nothing can be proven with public timechain data at the individual transaction level.

While having one or more entities controlling the outputs is trivial, having more entities controlling the inputs is a little bit trickier, requiring some real-time coordination among all the payees before the transaction gets broadcasted. Luckily, though, the atomicity of Bitcoin transactions is such that this process doesn't require any trust among different, unknown payees.

The Fungibility Factor

This fungibility feature of Bitcoin transactions has been part of Bitcoin's design since the very beginning, but its privacy implications were explicitly pointed out by different contributors only later on. Finally, in 2013, the label CoinJoin was created by Gregory Maxwell, to refer to the best practices a bitcoin wallet should implement in order to fully leverage such preexistent internal fungibility. Many variants of the technique have been proposed over time (PayJoin, JoinMarket, CoinSwap, P2EP and Zerolink implemented in wallets Wasabi and Samourai), all with the same goal: taking advantage of the fundamental fungibility of the protocol.

Another dynamic with the potential of boosting Bitcoin's privacy is its layerization. Upper layers of the protocol stack, like the Lightning Network, don't need to use the timechain to confirm every single transaction; rather transactions are only used as "anchors" to open and close "contracts" enabling payments elsewhere. Satoshi already imagined such kinds of "payment channels" early on:

"The parties hold this tx in reserve and if need be, pass it around until it has enough signatures. [...] They can keep updating a tx by unanimous agreement. The party giving money would be the first to sign the next version. If one party stops agreeing to changes, then the last state will be recorded at nLockTime. If desired, a default transaction can be prepared after each version so n-1 parties can push an unresponsive party out. Intermediate transactions do not need to be broadcast. Only the final outcome gets recorded by the network. Just before nLockTime, the parties and a few witness nodes broadcast the highest sequence tx they saw."

This did not turn out to be the exact way payment channels have been introduced (it was flawed), but they are now a common tool for many Bitcoin users. They can be used directly or collectively via routing. While often presented as a "scalability" solution, the Lightning Network and, in general, Layer 2 techniques have the big privacy advantage of massively reducing the amount of public information available on the timechain.

Starting Off on the Wrong Foot

Of course, it was not trivial to implement privacy best practices in everyday bitcoin wallets and tools. First of all, while reducing the amount of information leaked on-chain, Layer 2 techniques and CoinJoin often increase the amount of network-level information to manage and protect (mostly because of the need for real-time interactivity, up-to-date lists of reachable peers, publicly available liquidity, etc.). The Lightning Network, in particular, was not really easy to bootstrap until a protocol upgrade was adopted by users in late 2017.

While CoinJoin, unlike the Lightning Network, was possible to implement in theory since day zero (although with many practical challenges regarding coordination, liquidity and amount obfuscation), most actual bitcoin wallets didn't bother to find a way to do it. By not doing so, they consolidated a dangerous trend: The large majority of on-chain transactions were considered as created, signed and broadcast by one single entity, in complete control of the private keys associated with all the inputs. Bitcoin transactions started to be seen as always one-to-one or one-to-many. Thus, one of the most effective fungibility features of the protocol hasn't actually been turned into a wallet best practice until very recently, even though it has always been available.

But there's more, unfortunately. Other, simpler best practices, included in Bitcoin's design as trivial defaults, have been mostly ignored by tool builders who have been less concerned with privacy and more focused on user experience during the early years. One obvious example is address reuse. Satoshi's words about the anonymity of public keys were written under the assumption that users would generate a one-off address every time they received bitcoin, which would then be discarded after it's spent again and never reused. (Maybe the word "address," itself, wasn't a good choice after all, being often linked to permanent references: email, IBAN, ecc.; while the word "invoice," now used for Lightning Network transactions, would have been a cleaner choice.)

Implementing this design was not entirely trivial either (especially before the introduction of HD wallets which made it easier to re-derive thousands of keys with just one "master" backup). So we ended up with massive reuse of

static addresses, decreasing the entropy and facilitating analysis and deanonymization. Users started to link the same address to their profiles on forums, social networks and blogs. For many early users, making a payment meant giving the payee a complete overview of all their past and future financial life in Bitcoin.

Another major incident was the proliferation of “light clients”: applications unable to download, validate and store the timechain directly, but able to store private keys and query other nodes (in the best cases, a trusted third party, like a wallet provider; in the worst cases, random nodes, in so-called “SPV wallets”) for the validity of the transactions involving the corresponding public keys. Besides creating a systemic risk in terms of security, these clients become a common hazard in terms of privacy.

Some other minor implementation best practices have been initially overlooked by tool providers in this regard (including privacy-oriented coin selection, merge-avoidance, change management, etc.), but, for the most part, these three practices represent the basis for the heuristics employed by “chain-analysis” companies hired by eavesdroppers to spy on Bitcoin users.

As of today, most of these problems have brilliant technical solutions and modern tools that implement them. But it’s difficult to push the best practices (which sometimes present small but existent coordination costs) in an ecosystem already “drugged” with easy, if dangerous, shortcuts. And privacy, as they say, loves company: Even if you have the best tools and follow the best practices, it doesn’t really help if you are the only one doing so (in fact, it may even hurt by making your efforts stand out in comparison, putting you under the spotlight).

In Part 2, we’ll look at some of the techniques that are threatening our privacy as bitcoin users, common misconceptions about privacy, and finally, how innovations in Bitcoin are going to make privacy more secure and easier to maintain.

A Treatise On Bitcoin And Privacy Part 2: Don't Be Misled By Red Herrings

By Giacomo Zucco

Posted March 18, 2020

In Part One of this treatise, we examined the fundamental relationship between Bitcoin and privacy by going back to the beginning with the whitepaper. In spite of some excellent privacy preserving options that have been available to users since those early days, we seem to have taken a few wrong turns. But to fix it, in order to make Bitcoin's privacy "great again," we must be able to distinguish between real privacy and red herrings that can only lead us further off the path.

Fiat Gateways Lead to Privacy Graveyards

Bitcoin is an effective system to transfer and store wealth, but that wealth has first to "enter" the system somehow, very often coming from fiat money. (Of course, you can also earn satoshis directly in exchange for goods and services you provide, instead of buying them with fiat.)

Fiat-enabled bitcoin on-ramps (often known as "cryptocurrency exchanges"), acting as liquidity bridges, created huge privacy problems in Bitcoin. In order to manage fiat, exchanges will have to use traditional bank accounts. In order to get those, they have to meekly accept all the rules, conditions and limitations banks require. Traditional fiat banks, in turn, will pass over the extremely complex and heavy "compliance" burden they received from governments and regulatory agencies, including that concentration of economic illiteracy called "KYC/AML regulation."

So, fiat-to-bitcoin bridges will almost always end up demanding a scary amount of personal information from their user, linking that information to a few deposit and withdrawal addresses (often incentivizing continuous reuse) and then even hiring "chain-analysis" companies in order to follow, trace, tail and stalk all the previous and following economic activity on-chain.

Why Chain Analysis?

The first and most important reason for doing so is because these on-ramps are scared to lose the privilege of having a fiat bank account. Bitcoin was, is and will always be considered a "borderline" reality by governments and government-sanctioned legal cartels like modern fiat banks. Thus, it's realistic

to assume they would close down operative accounts to any exchange which couldn't guarantee the same level of financial surveillance that fiat banks routinely enact.

For this reason, fiat-enabled gateways not only keep promoting wrong and dangerous uses of the Bitcoin protocol, discouraging security best practices and hiring "chain-analysis" spy companies: They often even go to great lengths to publicly praise "KYC/AML" nonsense regulations and to push the narrative that "Bitcoin is completely traceable," marketing some probabilistic assumptions as "legal proofs" and ignoring even the existence of the fundamental privacy features of the protocol.

For a while now, these businesses have been freezing or confiscating users' accounts because of what theoretical "chain-analysis" heuristics (dishonestly promoted as "facts") suggest these users may have been doing way before or way after their interaction with the exchange, basically trying to break fungibility in Bitcoin.

We often see this happening for activities that aren't even explicitly considered illegal in the specific jurisdiction under which they happened: online gaming, adult services, political campaigns, etc. Anything considered even remotely controversial has been depicted as forbidden, and any statistical guess about "on-chain" activity, based on common patterns and typical tools, has been depicted as "proven."

Of course, there's nothing really proven in "chain-analysis" heuristics, so the spy companies arbitrarily decide how many "on-chain hops" to look for, arbitrarily assuming who is doing what. Even assuming that such heuristics are correct (they have never been 100 percent reliable, and they are less and less so each day, while Bitcoin developers build better tools and Bitcoin users start employing best practices), this behavior is unacceptable. It is the digital equivalent of your physical bank sending private investigators to follow your every move for days after you withdraw cash at the ATM, and then freezing or confiscating your bank account entirely if that PI comes back with a report that says that "you may have," with some probability, engaged in controversial actions with that cash.

More recently, this shady behavior has extended beyond some generically controversial activities engaged by "somebody somehow connected with customers" to encompass even the very act of trying to use Bitcoin's security and privacy best practices!

Closing the Blinds

In January 2020, a company that operates a regulated exchange froze a customer's account once they discovered possible hints that somebody, possibly the customer himself (but after some "hops" following the withdrawal transaction, that is, not even directly), was using a wallet enabling privacy best practices. Again, imagine your physical bank sending a private investigator to follow your steps for days after you withdraw some cash at the ATM, and then freezing or confiscating your bank account if that PI reports that says that "you may have," with some probability, closed your shutters at home, or pulled your shower curtains while naked, or put a lock on your personal journal, or used HTTPS within your web browser!

Furthermore, the specific message to the customer was tragically hilarious: It said that the business "can't condone activities such as peer-to-peer (sic!) mixing or gambling." All this while talking about Bitcoin, which is literally a peer-to-peer protocol whose transactions can natively work as mixers, and coming from a business that operates in cryptocurrency trading, which some consider not that different from gambling!

Don't Fall for Red Herrings

There have been many reactions from Bitcoin users and analysts to these dodgy examples of behavior, many of which are based on logical fallacies or straight-on distortion of the facts. A classical example is the absurd notion that "Bitcoin users should not use privacy best practices, because that's dangerous."

Red Herring #1: "Being Private Will Get You Into Trouble"

The pseudo-argument goes something like this: Since some overzealous business may use unreliable heuristics to accuse you of adopting privacy and security best practices that they have arbitrarily defined as "unacceptable," possibly freezing or even confiscating your account, or flagging it as "suspicious," you should just stop using those security best practices and move to insecure alternatives instead. In other words, to use our physical bank example, since your bank might flag your account if the PI they sent after you comes back with a report that says that you may have, with some probability, used some privacy best practices a few days after a cash withdrawal, you should just stop closing your shutters while home, or pulling the shower curtains while naked, or putting a lock on your personal journal, or using HTTPS within your web browser.

This is nonsense, of course. If anything, it's **not** using privacy and security best practices that would turn out to be extremely dangerous — not just for your financial safety but also for your physical safety. Reminder: Bitcoin's privacy is all-or-nothing! Once a business is able to attach your physical identities, not

just to an on-chain address but also to all the future and past history connected with it, all it takes is a little leak (by the business itself, by its spy-contractors or by one of the countless government agencies which will receive and pass along that information) to direct very dangerous enemies to your doorstep.

Incidentally, the pseudo-argument is flawed more fundamentally as well: Even if you were so reckless as to decide to trust this third party with a complete account of your future and past transactions, in spite of the risk to your physical security (and that of your loved ones), you may achieve the very same result just by sending it the cryptographic proofs of all the inputs you ever signed (either on-chain or on upper layers), allowing the meddling gateway to read through each of your CoinJoin or Lightning Network routing — all without giving up generic privacy best practices. You are still risking a leak, but at least you are not giving every random guy with an internet connection an easy way to deanonymize and stalk you (and others you interact with).

Red Herring #2: "If You're Just Using Bitcoin to Invest, You Don't Need to Worry About Privacy"

Usually this red herring comes with some distorted vision of Bitcoin's utility. "If users just want to invest in bitcoin as an uncorrelated financial asset with some disinflationary features," they say, "then they don't need privacy at all." This pseudo-argument is severely flawed.

Here's the bad news: Gold was, for many many centuries up until 1933, a typically "uncorrelated financial asset with some disinflationary features" that people in the United States and elsewhere could invest in. But then came Executive Order 6102. Gold was confiscated all across the nation, and all the investors who didn't protect their privacy (which was especially hard with "paper gold," kept in custody by trusted third parties eager to comply with the order, but also pretty hard with actual physical gold, difficult to hide in large amounts or to smuggle across a border) had to give it to the government.

A good general heuristic is this: If you are a privileged "first-world" investor, with a good KYC identity, and you are looking for some kind of investment that is politically uncontroversial now and likely to remain that way, then you will soon be able to access that type financial product from you favorite fiat bank. If that describes you, don't even concern yourself with complex stuff like private keys, blockchain fees, addresses: leave the real protocol to real users. Just call your good old bank over the phone and ask to buy some "bitcoin-flavored risk": certificates, futures, ETNs, ETFs, CFDs, etc.

If, on the other hand, you are not as privileged (like the majority of the world population today, which doesn't have a KYC-friendly identity), or if you think that the financial asset you seek is a bit controversial today already or likely to become so in the future, then you will eventually need some very strong privacy techniques to acquire it and to safely store it, since "legally compliant" exchanges, brokers and marketplaces will do everything they can to keep you out of it or take it from you.

Red Herring #3: "Just Use a Magical 'Privacy Coin!'"

A second typical reaction, even more absurd, is to suggest "privacy altcoins" as a "solution" to this problem. A regulated exchange will flag your account if you use best practices such as CoinJoin, or Lightning Network, or address-reuse-avoidance. Then, instead of bitcoin, just use some illiquid bitcoin-clone whose design has been altered in such a way that it's said to offer "more fungibility," right?

The superficial problem with this approach is that such "magic privacy coins" don't actually exist in the real world. On one hand, that's because most of the changes marketed as "privacy improvements" are either entirely fake or greatly exaggerated. They also tend to come with serious trade-offs which make these clones otherwise unusable at scale over the long run (usually including a completely centralized development process, trivial to compromise).

On the other hand, even if such a coin were to exist, from a technological point of view, it couldn't work in practice from an economical point of view. Remember: Privacy loves company. A huge chunk of the bitcoin economy and its users would have to move to the very same bitcoin-clone as you. Otherwise, your transactions will have a lower liquidity and a smaller anonymity set, regardless of how perfect and sci-fi-worthy the privacy tech you are using is.

More on These Magical Privacy Coins and Why They Are Useless

The Bitcoin + Privacy-Coin Combo Fallacy

There are variants of this red herring which are based on some kind of "bimetallic standard" idea: Those proponents will suggest that you use bitcoin as your fundamental store of value (which centralized illiquid clones can't be for obvious economic reasons), and then add a particular "privacy altcoin" for privacy in transactions.

Of course that can't work in most real-world scenarios. Assuming that the payer and the payee both use bitcoin as a long-term store of value, the payee

would have to move satoshis from his personal storage solution to some kind of market (regulated or not, it doesn't really matter here) with the same privacy issues as any other bitcoin transaction; then exchange those satoshis for altcoins on some low-liquidity shared order book with very low privacy; and then move the altcoins over their native system with a low anonymity set to an address provided by the payee. Then the payee would have to repeat the same steps in reverse.

The privacy guarantees of the whole process would be, overall, way lower than a normal bitcoin transaction performed following the best practices. Of course, these guarantees can be increased if either the payee or the payer "batch" many transactions in one big altcoin reserve, exchanging satoshis only once, way before or way after the single individual transactions. But this would require the altcoin to be a reliable store of value for long periods of time — which illiquid and centralized bitcoin-clones (often crippled by unbalanced trade-off choices between privacy features and other very delicate aspects) can't be.

The deeper problem with this approach is that, even if feasible, it would become completely useless pretty quickly. The very same reasons that convinced some regulated exchanges to actively discourage or even prevent their customers from adopting privacy best practices on Bitcoin, would readily convince the very same exchanges to just delist any "privacy-focused" bitcoin-clone. The "smaller" the altcoin, the weaker the incentive to list it. The "bigger" the altcoin, the stronger the regulatory pressure to delist it. It's as simple as that.

The "Mandatory" Privacy vs "Opt-In" Privacy Fallacy

Some weak attempts at steel-manning this approach focus on the distinction between **mandatory privacy** and **opt-in privacy**. "With Bitcoin," the altcoin proponents say, "you are not forced to use the fungibility features at the protocol level, so it's easy for the exchange to ask you not to use them. But with my altcoin, you have no choice, so the regulated exchange will also have no choice but to allow you to use them."

Again, this is nonsense; it's not true that a privacy feature can ever be "mandatory at the protocol level."

As the history of Bitcoin teaches us, it's mostly about tools: Even when the base protocol includes strong fungibility capabilities, if the most widespread tools don't leverage them, then people will simply not use them. They'll just resort to using whatever is easy and available, even if that mean adopting bad practices instead.

It doesn't matter which protocol you use: If the tools are inadequate, so is your privacy. Just as you can have a bitcoin wallet that is incompatible with CoinJoin and that forces address reuse, you can also have a monero wallet that leaks confidential information about amounts and always constructs "ring-signatures" between every single user and himself. If such a wallet is widespread, spy companies can assume such behavior as common and build de-anonymization heuristics.

Of course, altcoin proponents may just build and market tools that actually use the privacy features already present in their clone at the protocol level. But then again they would need just as much time, money and effort that is required for building and marketing tools that actually use the privacy features already present in Bitcoin at the protocol level.

What Really Matters: Incentives

A more useful distinction to examine is the one between privacy features that are economically **convenient** to use and privacy features that are **costly** to use. The perfect (bad) example would be that of "shielded transactions" in the altcoin Zcash: Since they take way more space inside blocks, and way more computation time to be verified and signed (making this last action almost impossible on a light client), economic incentives push the already-few users of the coin to "unshielded" transactions, which are just an outdated version of the traditional bitcoin ones.

As a **direct** effect, many users will think they have "more privacy" when this process, in fact, makes tracking and deanonymizing far easier.
An **indirect** effect will be that the very few users who do decide to pay the extra cost for "shielded" transactions will find themselves within an even smaller anonymity set, ending up exposed instead of protected.

An opposite example would be the Lightning Network on Bitcoin: Since block space is expensive, users often have strong economic incentives to switch to payment channels to save fees, reducing the "timechain footprint" to just opening and closing channels.

Same Old Story

Ultimately, it's not surprising at all that some of the most vocal proponents of the "CoinJoin is risky because your account will get flagged" narrative turn out to be also promoters of new, illiquid "privacy" altcoins, which they hope to push to profit from "pump-and-dump" schemes. Same old story: "Bitcoin's fees are too high: buy my low-fee altcoin!" or "Bitcoin signatures aren't quantum-proof: buy my quantum-ready altcoin!" or "Bitcoin's smart contracts aren't flexible enough: buy my Turing-complete altcoin!" or "Bitcoin is not fungible enough: buy my privacy altcoin!"

Solutions Are Coming

Are there real solutions and ways to mitigate the threat that regulated exchanges pose to the privacy and the security for Bitcoin users, beyond the red herrings? Yes: many.

The ultimate solution, albeit very slow, will eventually come from the evolution of the market. While more and more resources will leave the fiat world to enter Bitcoin over the years, more and more parts of the bitcoin economy will move from fiat gateways to satoshi-denominated trades among users. Gateways will still be important, but gradually less so, making their bargaining power lower and lower over time. Fiercer competition will also help: People will be happy to leave meddling PI-hiring banks who force them to keep shower curtains open if they have alternatives.

More Tools

Another mitigation will come from the evolution of Bitcoin tools. While more and more modern wallets will make it harder to reuse addresses or merge inputs, and easier to coordinate CoinJoin rounds, regulated exchanges will have a harder time forcing their customers to use only old, outdated or inferior wallets instead.

Lightning Network

Yet another mitigation will come from the adoption of the Lightning Network. Since block space in the base layer will become more expensive, users will be strongly incentivized to route transactions over payment channels instead. It will be harder for regulated exchanges to arbitrarily ban customers due to a probabilistic link between the satoshis they deposited or withdrew on the Lightning Network, especially when the latter will be ubiquitous, thanks to economic incentives.

Protocol Upgrades

Additional improvements may possibly come from the next protocol upgrades in Bitcoin, especially the one called "cross-input Schnorr signature aggregation." This upgrade will make coordinating with several different parties within CoinJoin rounds extremely convenient, from an economical perspective.

Decentralized Exchanges

Another hope comes from the idea of decentralized exchanges (DEXes). So far, they suffer from liquidity limitations and their security remains tricky: While the Bitcoin "leg" of any trade can be easily trust-minimized, the fiat leg remains ultimately trust-based, making complex and expensive escrow mechanisms necessary. (In turn, escrow mechanisms tend to prove very difficult to decentralize effectively.)

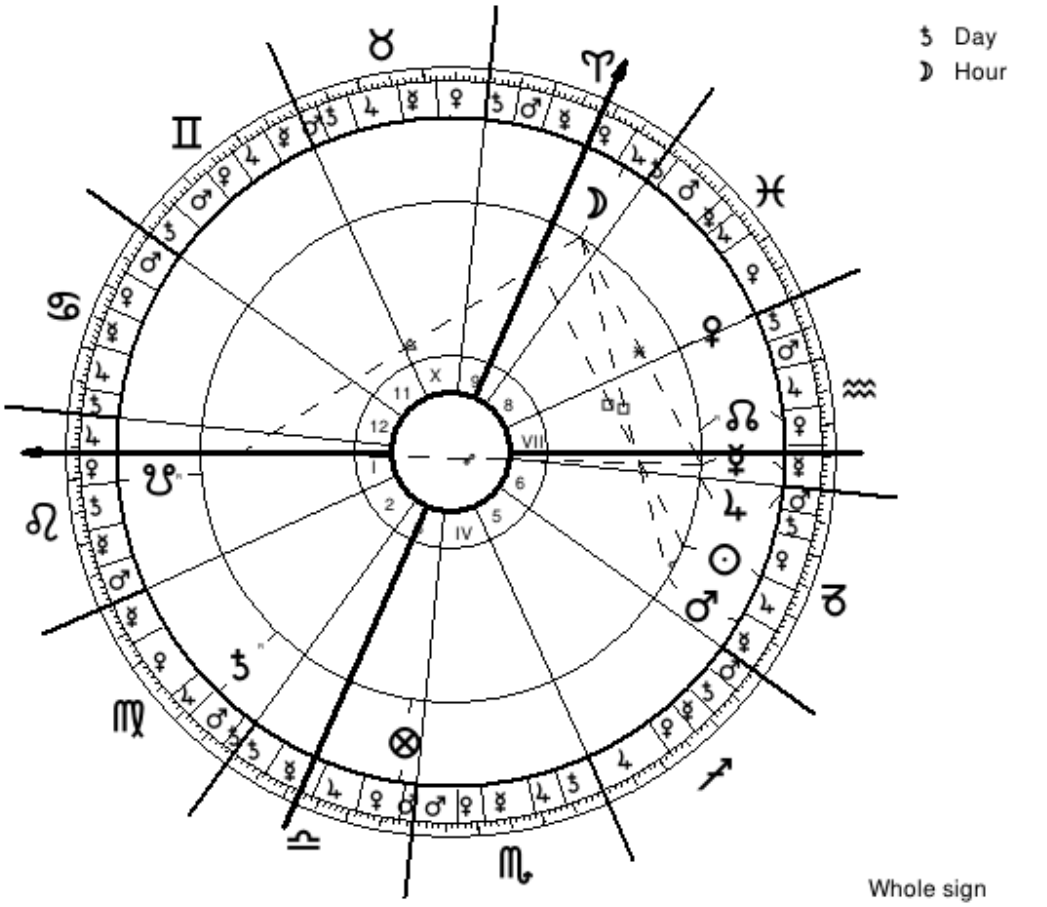
Your privacy is in your hands — just keep calm and be diligent. Don't submit to dangerous privacy violations. Don't reuse addresses. Use CoinJoin. Close your shutters when you're at home. Pull the shower curtains when you're naked. Put a lock on your personal journal. Use HTTPS when surfing the web.

In the end, Bitcoin fixes this.

The Astrology of Bitcoin

By Coeli Astrology

Posted March 18, 2020



Bitcoin is undoubtedly one of the most interesting developments in both the financial and technological sectors in recent times, presenting a radical alternative to traditional centralised banking, and claiming to act as a digital alternative to gold. As would be expected with such a radical development, it has met with vehement opposition and fervent support in near equal measure, with detractors claiming it is another case of tulip mania, while supporters claim it is the most significant financial development since the adoption of legal tender, forecasting Bitcoin to replace all centralised forms of currency and usher in a new era of decentralised trade and decentralised banking.

Aside from the financial and technological factors, Bitcoin is also incredibly fascinating from an astrological perspective, with a birth chart that is equally

interesting to learn about as the currency itself. Many pieces have been written on the chart of Bitcoin, some from the perspective of “modern astrology”, but also some from the perspective of traditional forms of the art such as Jyotisha or Hellenistic astrology, including a very interesting piece on the application of Zodiacal Releasing to the development and price action of the cryptocurrency.

In this piece we will present a thorough analysis of Bitcoins birth chart though a house by house survey, highlighting the real world manifestations of each placement, focusing on the price movement, technology, and public perception of the cryptocurrency. A second article will soon be published detailing the application of Zodiacal Releasing and some other predictive techniques to the development of Bitcoin.

We will begin our investigation by examining the foundational strength of the chart, through the lens of the triplicity rulers of the sect light, the lot of fortune, the ascendant, and the medium coeli

Triplicity rulers of the Sect Light

The triplicity rulers of the sect light can give us a good indicator of the overall strength of the nativity, along with providing us some information on whether early/later life will be the more positive part of the natives life. In the case of Bitcoin, the prognosis here is not a positive one.

The first triplicity lord, Jupiter, is in fall, placed in the Capricorn, the sixth house, in the terms of Mars. The second triplicity lord is the Sun, also in the 6th House, albeit in the terms of Jupiter. The participating triplicity lord is Saturn, which is placed in Virgo, (2nd house) in the terms of Mars.

None of the planets are particularly well placed, meaning that the nativity has a poor foundation of strength from the perspective of this technique. We can see here an early indication that Bitcoins fate will be subject to many reversals, and the charts foundational strength will be weakened.. This does not, of course, completely deny success to the currency, but it is a strong debilitating factor in the chart, and will give more weight to the negative predictions made for the currency.

The Ascendant and Midheaven are also placed in Fire signs, so the judgement on the strength of the triplicity lords of the sect light will extend to these points also, making for a very poor prognosis on the foundational strength of the chart.

Triplicity Rulers of Lot of Fortune

Aside from these three points, it is important to also examine the Triplicity Rulers of the lot of fortune, as this too has a significant influence over the strength of the nativity. Vettius Valens says that if the rulers of the sect light and other points are poorly placed, well configured triplicity rulers of the lot of fortune can sometimes salvage success for the nativity. In the case of Bitcoin, the triplicity rulers of the Lot are much better placed than the rulers of the sect light, with Venus (secondary ruler), and Mars (Co-operating Ruler) both in exaltation and their preferred sect. The primary triplicity lord, the Moon, is also reasonably well placed, both in the birth chart and on the other days of the Moon.

From this we can see that all three triplicity lords of the Lot are all relatively well placed, which will go a long way towards compensating for the glaring weaknesses revealed by the triplicity lords of the sect light. It is written that the triplicity lords of the Lot being well placed can often make the native lucky in life, and attain high rank through fortuitous circumstances. Bitcoin was certainly made at a “fortuitous” time, following on from a global recession, when faith in fiat currency was at a low point. It could be argued that the strength of the Lot is one of the reasons why Bitcoin always seems to bounce back when it seems as if all hope is lost, and that even the most extreme crises experienced by the currency thus far have always been followed sooner or later, by an equally extreme recovery.

These techniques serve as a tool for determining both the severity of the difficulties in the life of the native, and also the heights of success indicated by the chart. From our analysis here it can be inferred that the “baseline” condition of Bitcoin will not be very positive, however it may achieve sudden, albeit short lived, success from time to time. A cursory examination of the history of the currency will prove this to be true, as the price of Bitcoin is constantly subject to both rapid increases and decreases in price, with the price fluctuating by up to 20% a day in some cases. For assets such as stocks or precious metals, such fluctuations are virtually non-existent, with even the most extreme fluctuations in price seldom exceeding 10% in a day, generally occurring in times of crisis or global financial upheaval.

First House

BTC has the Descending Node in the first house, and this placement has proven to have an incredible influence over the currency, and as with all placements in the first house, has had a profound impact on the nature of the nativity.

There are no precise predictions given in any Hellenistic texts for the Descending Node in the first house, with this placement being notably absent from Rhetorius the Egyptians significations for the nodes in the

houses. This does not, however, stop us from gaining valuable information from this placement, as we are aware of some core principles of the descending node which we can use to make forecasts for its placement in the houses, even when no specific information is given.

In the case of Bitcoin, the “dissipating” and “reducing” effects of the node have manifested through the currency being decentralised and split into countless different pieces, the descending node acting directly on the ascendant here in a most interesting fashion. Free of the limitations of the human form, the descending node has much more leeway here to manifest its effects, and has quite literally dissipated the very being of Bitcoin, offering a striking example of a pure, direct manifestation of the node’s effects.

The node is aspected by neither benefics nor malefics, so its effects will not be “filtered” by the influence of any planets. The only planet in aspect is Mercury, which is making a sign based opposition to the node here. The impact of the node in this case certainly has a Mercurial character, with the effects of this placement pertaining largely to finance and technology.

The dodecatemoria of the ascendant can also tell us interesting things about the nativity, often pointing out an area of particular focus in the life of the native, or one of symbolic importance. In the case of Bitcoin the dodecatemoria of the ascendant is at 10 Libra, in the terms of Mercury. The third house of communication is a very appropriate placement for an entity such as Bitcoin, with the terms of mercury bringing the financial/technological significations into play. Not a revelatory placement, but a good example of the accuracy of this lesser known technique.

Second House.

The second house in Bitcoins chart is Virgo, with the out of sect malefic, Saturn, placed here. The second house will be quite important for Bitcoin, given that its primary function is to be a store of value and financial asset. Having Saturn here does not bode well at all for the fledgling cryptocurrency, with the house containing the out of sect malefic usually pinpointing an area of difficulty in the life of the native.

Aside from being out of sect, Saturn has no triplicity Rulership here, and is in the terms of Mars. It is however, receiving an opposition from Venus, which will be expected to produce some difficulties. It also sends an Antiscia to Aries, the sign of Saturn’s fall, which will be another weaking factor for the planet. We will delve into this Antiscia placement in more detail later, for now we will note that it will have an adverse effect on the condition of Saturn. The trine from Jupiter, Mars and Sun will improve the planets condition somewhat, making the difficulties forecast by this placement much more manageable.

The prediction for Saturn in the 2nd is for illnesses and great reversals of fortune, along with the native often being an “agitator of great public disturbances”.

There is also the prediction for the native to “waste their inheritance”. This forecast is quite interesting in the case of Bitcoin, as the mysterious “father” of the currency, Satoshi Nakamoto, has almost 1 million BTC in a wallet which remains untouched to this day. There are numerous theories as to what will happen to these Bitcoins, some say that Bitcoin SV founder Craig Wright is Satoshi, and he will sell all of the Bitcoin one day in an effort to make Bitcoin SV the number one cryptocurrency. Others say that the wallet is lost, and it will never be opened. Others still say that Satoshi will only use the wallet in an emergency.

Whatever the case, astrology would point to a reversal of some sorts resulting from this wallet, as it represents the “inheritance” of Bitcoin, being an asset withheld from the currency by its founder(s) for future purposes.

We can see here that Saturn has most certainly delivered on its promises with regards to reversals, with btc being one of the most volatile assets on the market today, subject to huge fluctuations in price, often dropping by more than 10% of its value in a single day. The illnesses and injuries have manifested as the many hacks and security issues which have plagued Bitcoin from the beginning, with the Mt Gox hack being a notable example here.

The agitator of public disturbances is another signification which is clear for all to see, with huge regulatory concerns, along with a bad reputation among many members of the public proving to be recurring issues for Bitcoin.

The effects of the ruler of this house in the 7th will be seen through the forks that have emerged from Bitcoin, and the infighting between the founders of the currency. Bitcoin Cash is the primary example of this.

The planet which rules the second house can also give us a hint as to the likely cause of any losses of income/employment are likely to be for the native. With Mercury as ruler of the second we can expect mercurial subjects such as technology, finance, and writing to be some of the contributing factors to any losses of income experienced by Bitcoin, and it is quite obvious that this has proven to be true. The only non-obvious result of this placement is the difficulties experienced by Bitcoin as a result of the countless hit pieces that have been published by journalists and critics of the cryptocurrency, which have contributed to many “losses of income” in the case of Bitcoin.

Third House

The third house of Bitcoin chart is Libra, and it contains the Imum Coeli, meaning it will also signify fourth house matters, along with any placements

here having the strength of an angular planet. While there are no natal placements here, we can see the antiscia of Venus placed here, a very auspicious placement having both domicile rulership and angularity. What we can infer from this placement is that hidden matters, and the "foundation" of the currency will both be points of strength. The "foundation" here will manifest as the brilliant technology and team working behind Bitcoin, along with the large base of support that the currency has. The hidden matters will manifest as the currencies ability to avoid regulation, and benefit from much of the clandestine activity associated with BTC in its early years, when it was the currency of choice amongst deep web drug dealers, and also many international crime gangs. Another obvious manifestation of the hidden significations here is the currencies security and cryptography, two decidedly fourth house matters which have proved incredibly beneficial for Bitcoin, and are perhaps two of the greatest strengths possessed by the currency. It would also be expected that the currencies "parents' will be another point of positive focus in its development, and this has proved to be a complicated matter, as will be shown later. However we can most certainly say that Bitcoin's founders were very talented and innovative people, who equipped the currency with the technological foundation which would prove to be a key influence in propelling the currency to the heights which it has experienced in recent years. Venus here would also suggest a good old age, however this is less certain, due to some other placements, and also taking into account that we are dealing with an Antiscia here, which will reduce the strength of all predictions made.

Fourth House

The fourth house is Scorpio and contains no major placements, having no natal planets, antisica, dodecatemoria, or even contra antsica. The ruler of the 4th is Mars, in the 6th house, which would indicate death abroad in the case of a human nativity. In the case of Bitcoin its "death" is very likely to occur abroad, as most of the money flowing in and out of the cryptocurrency comes from outside of Ireland. This will, however, not be a very strong forecast, as you generally want a prediction to be mentioned three or more times before you are certain of it happening.

Fifth House.

The 5th house is Sagittarius, and while it does not contain any natal planets, it does contain the Anstica of Jupiter, Sun and Mars, along with the Dodecatemoria of Jupiter.

Turning our eyes first to Jupiter, we see that these placements are hugely positive for the greater benefic, with the Antiscia and Dodecatemoria having

domicile rulership in Sagittarius, a potent combination that greatly strengthens what is one of weakest natal placements in the chart.

Jupiter in the 5th promises the native wealth, honour, and health, along with a position of power and prominence. As this is a night chart, and we are dealing with "secondary" placements, we can expect these predictions to be reduced in intensity, however they do serve as key astrological indicators of the incredible success enjoyed by Bitcoin, and show us how what seems like a very weak planet in the chart, can make some very positive predictions given its hidden strength revealed to us by the Dodecatemoria and Antiscia.

The Sun is also well placed here, having triplicity rulership, along with being conjunct Jupiter.

A key consideration in judging the condition of these points will be the superior square they receive from Saturn. This aspect changes what would have been a very positive placement, into one promising difficulties and setbacks to accompany all the good fortune predicted by this configuration. The square from Saturn will have a limiting and reversing effect on the predictions here, facilitating the negative side of fifth house matters, such as losses from speculation, to manifest in the life of Bitcoin.

It seems that no matter what way you look at things, all the positive predictions and placements of Bitcoin are hampered by the influence of the greater malefic, something that has proven true time and time again over the lifetime of the cryptocurrency so far. All of its amazing price rallies were followed by severe rapid declines, and regulatory efforts from governments and banks have been a thorn in the side of Bitcoin for many years. Even in discussions about the currency online and in person you will notice the influence of Saturn, for every fan of BTC there is a detractor, for every John McAffee there is a Peter Schiff, the malefic influence of Saturn always rearing its head as soon as the Jupitarian optimism shows its face. This is not to say that either side is right or wrong, it is merely an observation from the "perspective of Bitcoin" as if it were a native. In the context of an individual chart, the malefic influence will be experienced always from the natives perspective, not necessarily from the perspective of "the other".

The effects of Saturn in superior square will be somewhat offset by Venus making an inferior square to the placements in this house. This will not eliminate the impact of Saturn, but it will soften it somewhat. For Jupiter, this placement will be strong, as it has both term and house rulership. For the Sun it will be above average, as it has triplicity rulership and is in the terms of Venus. For Mars it will be average, as it does not have term or triplicity rulership.

We cannot of course, pass over the firth house without mentioning the associations of this place with gambling, speculation, and financial gains. The plethora of placements here will signal that these factors will be highly significant in the development of Bitcoin, and given the strength of these placements, it would be expected that this will be a very positive area for Bitcoin, and this has most certainly proven to be true. The meteoric rise of Bitcoin from being a fringe item of curiosity, to one of the most talked about financial assets in the world, was hugely influenced by speculation, and the reputation of the currency as an easy way to make a quick buck.

This was most clearly illustrated in recent years by the bull run of 2017, and the associated mass hysteria that accompanied it. People with no prior interest in trading or cryptocurrency were now flocking to Bitcoin, seeing it as somewhat of a golden goose which would deliver them to wealth and financial freedom. It cannot be denied that this speculative interest proved hugely influential in the development of Bitcoin and was largely responsible for the astronomical rise in prominence that the currency experienced over the past few years.

These placements offer us a striking example of the power of the antisica and dodecatemoria, as without examining these hidden placements, we would have little idea on the astrological root of how fifth house matters such as speculation came to have such a profound impact on Bitcoin, and how many Jupitarian matters came to have such a positive effect on the cryptocurrency, even with Jupiter so poorly placed natally.

Sixth House

Capricorn is the sign of the 6th house, and it contains a three planet conjunction of Mars, the Sun, and Jupiter. It is the most active house in the chart in terms of natal placements, and as such is key to unlocking the astrological secrets behind this enigmatic cryptocurrency. We see that Mars is earliest in the degrees of the sign, and as such will be the planet with the most influence over the predictions of this house. Mars is quite well dignified here, being in the sign of its exaltation, the house of its joy, and in sect. The Sun is less well dignified, being out of sect and having no triplicity rulership. It is however, in the terms of Jupiter, which will strengthen its condition somewhat. Jupiter is the least well dignified of the three, being in fall, and in the terms of Mars. Jupiter is however, quite close to the DSC, and as such will be strengthened in condition, along with having more capacity to influence the nativity given its angularity. This increased influence will be a mixed blessing for Bitcoin, as we have seen in the past where the expansion and optimism of Jupiter has gotten out of hand, leading to unsustainable growth followed by a very dramatic fall. On a side note, the boom bust cycle of Bitcoin is a good illustration of the polarity between Jupiter and Saturn, the

boom showing the expansive qualities of Jupiter, while the bust shows the reversals and restrictions so characteristic of Saturn.

We have a prediction for this particular three planet conjunction in another article, taking Firmicus Maternus' forecast for the combination, and putting it in the context of modern times.

"The positive effects of this conjunction are that the native is predicted to achieve success in the fields of business or politics, with an important job in the civil service also possible. Some natives may rise from an average position early in life to one of high status, with the help of powerful people.

The negatives of this conjunction are that the native is likely to be involved in difficulties, dangers, and reversals. Sometimes these difficulties will arise from their dealings with powerful individuals, other times from familial issues or betrayals. In some instances these difficulties can lead to criminal charges. The scale and magnitude of these issues will be determined by the condition of the planets and overall nature of the chart."

We can see quite clearly in the case of Bitcoin that all of these predictions have proven true, showing that even though these predictions made by the ancient authors are generic, they are also very accurate, and should not be discounted when judging a chart.

All planets are receiving a trine from Saturn, and a sextile from Venus. The trine from Saturn will be a very positive aspect to have for the planets, as they will benefit from the oft forgotten benefic capacity of Saturn, feeling the influence of the god of the Satya Yuga. This influence will bring an even greater capacity for organisation and hard work than already exists in this placement, with the nature of Mars effects being the most notably enhanced by this aspect. In the case of Mars, the trine from Saturn will reinforce the "controlled aggression" of Mars in Capricorn, upgrading what was the equivalent of a disciplined military force, into an elite special operations unit, as organised and efficient as they are powerful and deadly.

The sixth house is commonly associated with hard work, slavery, and toil. The manifestations of this in the case of Bitcoin will show up in "Bitcoin mining". Bitcoin mining takes a lot of computing power to solve problems, computers acting as "virtual slaves" in this context.

Jupiter itself in the 6th house makes an interesting prediction for the native to be a goldsmith or silversmith. Bitcoins aspirations to become the digital gold standard offer us an illustration of how these effects can manifest in the case of a non human entity.

The sun brings a spotlight onto the topic of mining, making it one of the standout features of Bitcoin, leading it to be widely recognised by the public,

even amongst those unfamiliar with Bitcoin. The positive effects of Mars are clear for all to see here, as the hard work of mining has brought success to Bitcoin and attracted many to the currency in the first place, offering a profitable means of attaining BTC, while improving the security of the currency. Jupiter brought scale to these enterprises, expanding them greatly. The effects of this expansion could prove difficult for Bitcoin, as many miners may cease operation if the price gets too low, and over time it becomes less and less profitable to mine, in this case Jupiter being in fall would be the cause of such a series of events. The negative press coverage about the environmental impact of upscaled Bitcoin mining could be seen as the negative side of having Jupiter in fall with the Sun in the 6th house.

The symbolism of this configuration extends to the ordering of the planets. As the earliest planet in the configuration, Mars will have the strongest influence over the placement. We see this in the orderly, tactical, and forceful manner in which Bitcoin is mined, many computers performing equation after equation as they work towards solving the block. We can even see the Martian influence in the temperature of the computers, as they heat up from the demands of the mining process. Following Mars is the Sun, the Sun representing the moment of “intuitive apprehension” when the equation is solved and the block is completed. Lastly we have Jupiter, this represents the financial reward at the end of the work, the gold rich ore at the end of the tunnel. As Jupiter is a de facto angular planet, this is the most important moment of the process, where the work done under the earth by Mars moves towards its emergence above the horizon. In a traditional mine, Jupiter would represent the loader bringing the ore up to the surface for processing.

This house is perhaps the most symbolically significant of the whole chart, presenting the whole process of Bitcoin mining to us in the space of 30 degrees, a truly magnificent example of the rich symbolism you can find buried in a birth chart.

Seventh House

Given the decentralised nature of Bitcoin, we would expect the 7th house to feature strongly in its chart, and feature strongly it does, with Mercury placed here in its own terms, and with triplicity rulership in the sign of Aquarius. Having Mercury here brings many “partners” for Bitcoin, in the form of the thousands of people who own some of the currency. Being in an air sign such as Aquarius is a perfect fit for an entity such as this, whose existence is purely virtual in nature, the nebulous qualities of the air element made plain for all to see here.

Joining Mercury in the house of partnership is the Ascending Node. The effect of the node here will be to increase and potentiate the “promiscuity”

indicated by Mercury, leading to the thousands of “partners” which Bitcoin has accumulated over the course of time. The Ascending Nodes effects vary considerably depending on the aspects made to it by other planets, with benefits promising good predictions from the node, while malefics will promise bad predictions. In this case, the node is not receiving any aspects whatsoever from benefics or malefics, with Saturn, Jupiter, Mars and Venus all in aversion. The interaction of the Ascending Node with Mercury is somewhat unknown, with very few references made to this in the ancient texts. There are a number of cases where the node is said to interact well with Mercury, but these are quite specific, and do not tell us much about the principle behind the interactions of the pair.

One other signification of the ascending node given by Vettius Valens is that it can have a destructive influence on the topics of the house in which it is placed, and it would appear that this is the case for Bitcoin, albeit not in the sense of decentralised partnerships, but on the partnerships of its founders. There was, as alluded to previously in this piece, a major falling out in the Bitcoin community, which led to the formation of Bitcoin Cash. While there are other placements which further indicate this, the effects of the ascending node would have been a significant contributing factor towards the dissolution of this particular partnership.

Eighth House

The eighth house, the house of death, inheritance, and other people’s money, would be expected to be amongst the most positive in the case of Bitcoin, given that Venus, the beneifc of sect is placed here in Pisces, the sign of its exaltation. It is also the 11th house from Fortune, (“the place of acquisition” as it was referred to in the ancient texts) and as such it will have a strong influence on the capacity of Bitcoin to make money.

Venus has both triplicity and term rulership here, making it very well dignified, however it is also receiving an opposition from Saturn in the 2nd, which will be highly debilitating for the planets condition, and cause a number of difficulties pertaining to 8th house matters

Aside from the natal placement of Venus here, there is also a significant number of dodecatemoria placements, with Venus, Mars and Mercury all having their dodecatemoria located in this house. The deodecatemoria of Venus here is a very positive placement, being equally well dignified as its source planet. Mars dodecatemoira is also well dignified here, having triplicity rulership and being in the terms of Venus. The dodecatemoria of Mercury however, is nowhere near as well dignified, being in fall in Pisces and having no triplicity rulership here.

The dodecatemorias are all receiving an opposition from Saturn, which will not bode well for their condition, or their predictions, even if their essential dignity is quite strong. Mercury's dodecatemoria is also in aversion to its source planet, which is a debilitating factor for both placements. Mars is in sextile to its dodecatemoria, which is a good sign, and strengthens the expression of both placements.

The combination here of Venus, Mercury and Mars is an interesting configuration, as it makes a number of predictions which are very applicable to Bitcoin. Mercury and Mars together will usually add a streak of corruption/criminality to the nativity. This can be seen from the multiple legal issues that Bitcoin has experienced, along with its utlisation by drug dealers and other forms of criminality. The opposition of Saturn has seen much of these cases being found out and punished. The rules and regulations which many governments and organisations have imposed on Bitcoin are another manifestation of this placement, with Saturnian entities quite literally coming into opposition with the Martian-Mercurial nature of the cryptocurrency.

Venus is right at 0 degrees of Pisces, and as such it will have a commanding influence on the configuration of placements in this house, and this is clear from the manner in which Bitcoin has adapted to these issues, always coming out on top despite the many difficulties in its path, and with any issues pertaining to its corruption largely being smoothed over due to the strong Venusian influence at work early in the degrees of Pisces.

The Venusian influence here, when combined with Mars and Mercury, will also make much of the financial gains made by Bitcoin be squandered, and dissipate quickly. In a human nativity it would often manifest as the native being wasteful of money, in the case of Bitcoin it has led to much of its good fortune being short lived, often due to buyers being over exuberant and bringing the currency to price levels which did not reflect its true value.

The location of Venus here will predict that Bitcoin will benefit from unexpected sources of wealth, or from the death of others. The death significations could be taken as the currency benefiting from the death of physical money, or fiat currency, or from the "death" of the economy experienced during a recession. Bitcoin has most certainly benefited from the slow death of physical money, with more and more people using digital services such as Revolut in Britain and Ireland, and the Cash-App in America, society has become more open to alternative, digital methods of payment, and the concept of a digital currency is becoming more and more palatable to consumers.

Having the benefic of sect in the place of acquisition shows us one of the key astrological factors behind the incredible financial success enjoyed by Bitcoin since its inception. The currency was once valued at $0, and at its peak was

valued at nearly $20,000 dollars. Its ability to make money clearly being one of the most positive aspects in the life of Bitcoin, and finding suitable representation in the birth chart.

Of course we cannot ignore recent developments in the price of Bitcoin, with the currency experiencing a significant fall in value in tandem with the huge crash hitting traditional assets in recent weeks. Many will point to events such as this and ask why is Bitcoin not benefiting from the “death” of the financial system? To this I would respond that what we are witnessing here are the effects of the opposition of Saturn to the 8th house, while also pointing out that we are currently in the initial stages of a global recession, and the markets are likely to continue to suffer as things progress over the coming years, so we cannot make judgements on this matter just yet.

In the follow up article to this piece, we will see that Bitcoin is set for a significant period of growth in late April and late June, so the forecast made by the 8th house may still prove true, we will just have to wait a while to find out.

Ninth House

The Ninth House in the chart of Bitcoin is Aries, and it contains the Moon, along with the antiscia of Saturn. The Moon was in the waxing stage at the time Bitcoin came into being, so it will interact relatively well with Saturn, very well with Jupiter, and interact poorly with Venus and Mars.

(It is due to the Moon becoming more “diurnal” as its light increases, and more “nocturnal” as its light decreases that it interacts in this way.)

The Moon’s conjunction with Saturn’s antiscia here will be a hugely weakening factor for the planet, as Saturn is the malefic of sect, in the sign of its fall.

The Moon has no triplicity rulership here, which will further weaken its condition, however it is in the terms of Jupiter, which will somewhat improve its condition, especially given that it is waxing.

As always with the Moon, its aspects are crucial in determining its condition, along with its status on the 3rd, 7th, and 42nd day after the natives birth, along with the condition of the eclipse, full and new Moon nearest to the birth.

The Moon is receiving a superior square from Jupiter, the Sun, and Mars, bringing a mix of positive and negative effects on its condition. The superior square from Jupiter will be greatly strengthening for the Moon’s condition, while the square from Mars will be very harmful to its condition. Given Mars is closer to a degree based aspect with the Moon than Jupiter, we can say that

on the whole, these aspects will weaken the condition of the Moon, however the reduction in strength will be greatly reduced due to the influence of Jupiter.

(Even if Mars is well placed as it is in this chart, it still interacts poorly with the waxing Moon, and is still a malefic planet, so it is safe to say that its effects will still be damaging.)

The movement of the Moon must also be taken into account when determining its predictions. In this case the Moon is moving from Mercury to Mars, with the archetypal manifestation of this configuration being a powerful and feared military/political leader, who ends up making serious mistakes in their career, resulting in them being overthrown and going into hiding/being killed.

After adapting this archetypal prediction to the case of Bitcoin, are presented with a strikingly accurate prediction. It is a rebellion against the existing financial system, an anarchistic alternative to the state controlled centralised financial system currently in place. It is feared by governments and banks, with these institutions creating rules and regulations designed to restrict and oppress the cryptocurrency, and stop it from toppling the ivory tower of centralised control which they have built around the financial system.

The forecast made by this configuration does not bode well for the future of Bitcoin, with the predictions strongly indicating a dramatic reversal in career, as the Moon moves from Mercury to Mars, travelling towards destruction. Given that the Moon is waxing in the chart of Bitcoin, these predictions must be taken very seriously, and strongly indicate that Bitcoin will experience a very dramatic downfall at some point or another, the precise timing of such an event will be discussed in the second article in series.

The ninth house also contains the midheaven, which means that the career and public perception of Bitcoin will also be largely determined by the ninth house. The placement of the Moon here is very interesting. The Moon symbolises the masses, change, and the “rational” faculty of our intelligence* (the sun representing the intuitive faculty), and all of these factors feature heavily in the development of Bitcoin. “The Masses” come into play through its decentralised nature, requiring the cooperation of all Bitcoin holders to maintain the decentralised ledger, and also through the influences of the masses on the price action of Bitcoin, their emotions and actions changing rapidly, just as the lunar cycle. The rational mind significations materialise in the technological nature of Bitcoin, and the importance of programming in the currencies development. There are few fields that place a greater demand on rational intelligence than programming/technology, and given the Moon’s placement with the midheaven it is no surprise that these two fields feature heavily in the development of Bitcoin.

**This association does not, by any means, come from "modern astrology", but from Rene Guenon, who makes the connection between the Moon and the rational intelligence in his book "Symbols of Sacred Science". The Moon has "reflected" light, and in our case this represents the rational "reflection" on the intuitive knowledge of the Sun. The Sun represents direct, intuitive knowledge, while the Moon represents the rational "reflection" on this.*

Having the Midheaven located here will also put a 9th house filter on the career of Bitcoin. We can see this through the topics of foreign countries, travel, and governments featuring strongly in Bitcoins career. It is truly a global currency, being used in almost every country in the world, and payments can be made in seconds between people on opposite sides of the world, with no exchange rates, and very low fees. Governments have also featured heavily, albeit in a negative sense, imposing rules and regulations on Bitcoin and hampering its growth. It could be said that "religion" (the word taken in the modern, western, context) has also featured heavily in the career of Bitcoin, with the currency having somewhat of a cult following, and the mysterious founder Satoshi Nakamoto being regarded as somewhat of a "messiah" by many of the currencies supporters. Much could be said on this, but the article is long enough as it stands.

Interestingly, the rising time of Aries in this chart is around 3 years, a very early rising time which suggests that in this case we can expect the early years of the currency to be hugely important for its development, and for much of the "career" related predictions to manifest quite early on in the life of Bitcoin. This has proven true, as the currency enjoyed a rise to prominence around the 3 year mark of its development, with a number of important events taking place around this time, along with a rapid rise to prominence. During this time period the currency most certainly lived up to the changeable forecast made for its career by the presence of the Moon on the midheaven, with both the price action and development of the currency going through phases of both unprecedented growth, and unprecedented decline.

Tenth House

Bitcoins 10th house is Taurus, and it contains the lot of fortune, along with the dodecatemoria of Saturn and the Moon. Saturn's dodecatemoria will not bode well for 10th house matters such as career and public perception, with the out of sect malefic importing restriction, reversals, and difficulties to matters signified by the 10th house. Saturn is also in trine to its dodecaemoria, which will be an indicator of strength for Saturn.

The Moon's presence here will be much more positive for Bitcoin, the Moon having its exaltation in Taurus. The dodecatemoria of the Moon however, is in

aversion to its source planet, which will debilitate the planets condition somewhat, off-setting some of the benefits accrued from the Moon being in exaltation here. The conjunction of Saturn's dodecatemoria will also prove difficult, although these difficulties will be mitigated by the Moon being in exaltation in Taurus, and also by its waxing condition, as the waxing Moon interacts well with saturn. The Dodecatemoria of the Moon is also receiving a trine from Jupiter Mars and Sun, a sextile from Venus, and a trine from Saturn. The trine from Jupiter and Saturn to the waxing Moon dodecatemoria is an incredibly auspicious configuration, however the aspects from Venus and Mars are less auspicious, given that these planets interact poorly with the waxing Moon. Venus and Mars do however, respectively make a sextile and trine to the Moon, which will mean that much of the negative effects of their aspect will be eliminated.

We see from this placement the extent of the influence exerted by the Moon on Bitcoins career/public perception. The predictions have certainly held true, with Bitcoins reputation and fortune waxing and waning, subject to the ebb and flow of the tides of public opinion. The Lunar influence having a near archetypal manifestation on the "career" of Bitcoin.

Eleventh House

The Eleventh house contains the dodecatemoria of the Sun, which will prove to be a mixed placement. While the 11th is an excellent house for any placement, the Sun is in aversion to this point, meaning that it will not be an overly auspicious dodecatemoria. The Sun in the 11th however will bode well for Bitcoin's public perception, success, and financial outlook, promising success to be delivered in these areas over time.

The contra antiscia of Jupiter, Sun and Mars are also here, which will improve the condition of all these planets, given that they are in one of the most favourable houses in the chart. It is an interesting placement also in the fact that it makes a connection between "friends" (11th house) and the sixth house matters of work. This can be seen through the Bitcoin miners being faithful allies to Bitcoin over the course of time, always keeping their machines running to maintain the strength of the network, even when matters were not looking very promising for the future of Bitcoin.

Twelfth House

To end on a mind numbing note, there are no planets, dodecatamorias, antiscia or contra antiscia here, making this the least active of all the houses in Bitcoins chart, and revealing next to nothing about the cryptocurrency. It is a positive sign to have no placements here, and the ruler of the Twelfth in the

9th (with the MC) may indicate legal issues and problems with government, but not much can be said other than that.

With that we have reached the end of our analysis of the birth chart of Bitcoin. Why it is by no means exhaustive, it has revealed a lot about the astrological roots of many of the unique characteristics of Bitcoin, and provided an interesting case study of applying basic techniques used for human nativities, to non human entities such as Bitcoin. It is a case where many of the predictions translated remarkably well, even though their designated purpose was the birth charts of humans. More proof, if we ever needed it, that the forces symbolised in the birth chart permeate every single layer of material reality, including the virtual ones.

In the next article on the astrology of Bitcoin, we will examine the Zodiacal Releasing periods of the currency, along with taking a cursory look at some other predictive techniques as they apply to the case of Bitcoin. Many will have been disappointed that there was not much information in this article with which you could make money from, however your disappointment will vanish upon reading the next piece, as Zodiacal Releasing has proved incredibly effective in predicting the price action of Bitcoin in the past, and will serve as a valuable addition to any traders toolbox, so watch this space!

Bitcoin: A Bold American Future

Reimagining America's National Security Approach

By Conner Brown

Posted March 23, 2020

America's future is in question. Public and private debt are rising to record levels and economic growth remains stagnant. Despite unprecedented fiscal and monetary intervention after the financial crisis, results have been disappointing. The American people do not need accounting tricks or more debt, but true innovation. Thankfully, Bitcoin provides a way forward.

Instead of falling behind other developed nations, America should lead the world in embracing this monetary evolution and reap the benefits for years to come. With bold action and investment, Bitcoin will secure American dominance into the 21st century. This article will lay out the American case for Bitcoin across multiple dimensions—creating a modern day gold rush to lift our country out of debt and into prosperity and safety.

As a framework for discussion, I'll be using America's most recent National Security Strategy as a guide to demonstrate how Bitcoin should considered fundamental to America's ***National Security Innovation Base***.[1] Bitcoin will help:

- Rejuvenate the Domestic Economy (NSS p.18)
- Lead in Research, Technology, Invention, and Innovation (NSS p.20)
- Embrace Energy Dominance (NSS p.22)

Let's begin with our current financial outlook.

The Dangerous Game of Debt

The United States' financial position is dire. Federal Reserve Chairman Powell recently referred to our financial outlook as "an unsustainable path."[2] The Congressional Budget Office confirms this warning. "Because of the large deficits, federal debt held by the public is projected to grow, from 81 percent of GDP in 2020 to 98 percent in 2030 (its highest percentage since 1946). By 2050, debt would be 180 percent of GDP—far higher than it has ever been."[3]

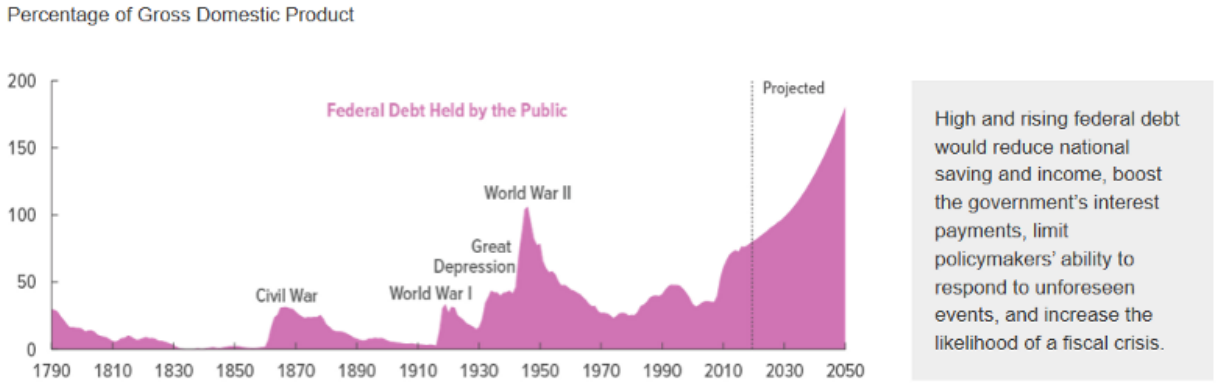


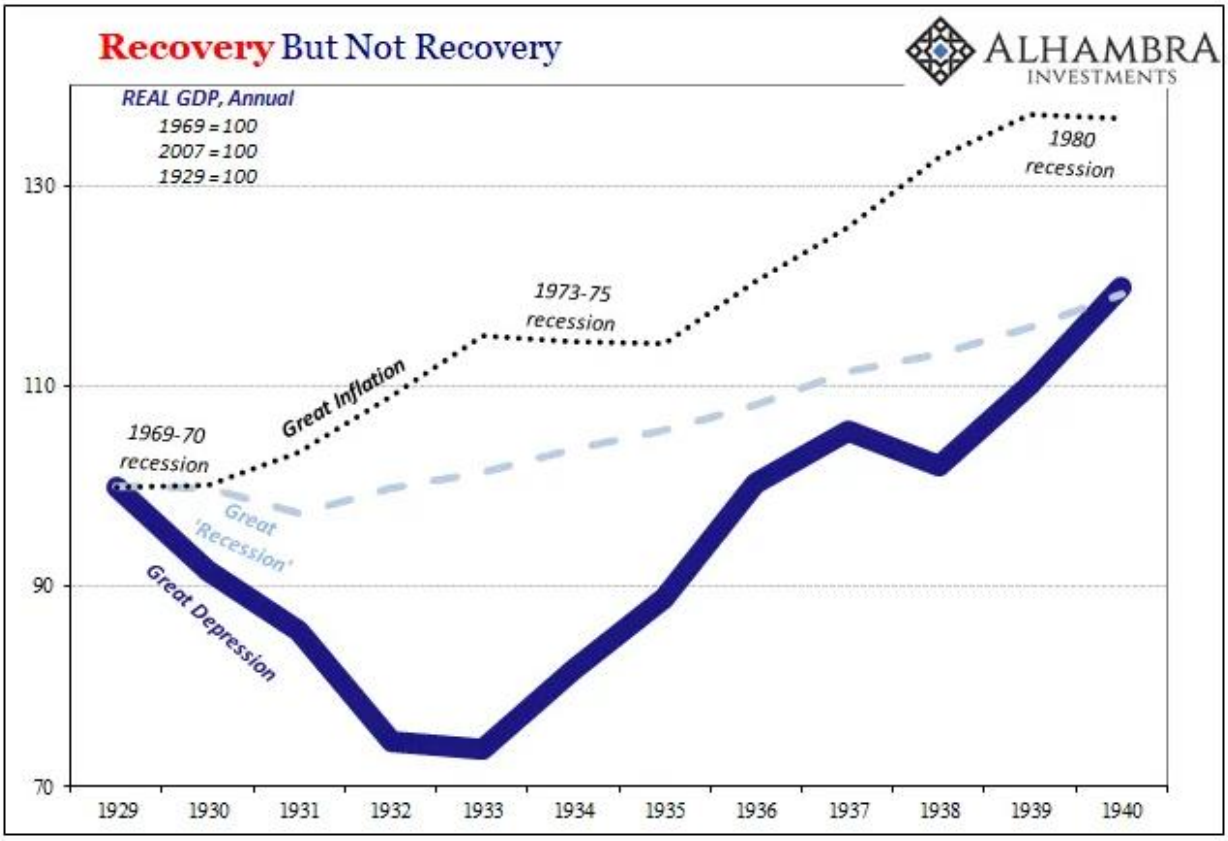
Figure from CBO's latest Annual Report.

Federal debt is only part of the story. Debt levels are unprecedented across multiple areas of the economy. Municipalities, private debt, corporate debt, and ballooning future liabilities add up to astonishing levels. A recent report by AB Bernstein calculated U.S. total indebtedness to be close to **a whopping 2000% of GDP.**[4]

To make matters worse, these numbers depend on America's decade of expansion to continue indefinitely. As Hoisington Investment Management noted in a recent letter to investors, "deterioration in economic conditions would lead to a quick worsening in the [debt to GDP ratio], pushing the debt ratio further into uncharted waters, even without new fiscal measures that would likely be enacted in such circumstances."[5] With declining global

growth and heavy impacts from COVID-19, this position is close on the horizon.

Papering over our problems with debt cannot continue. Hoisington further noted, "the declining marginal revenue product of debt reconfirms that excessive debt usage is triggering the law of diminishing returns, which results in weaker growth in real GDP."[6] Our approach is self-defeating. With such high levels of debt, our economic growth is lagging significantly behind previous recoveries. We simply will not be able to borrow our way out of this.



America's GDP recovery following the three worst recessions of the last century. Chart by Jeff Snider.

The consequences are serious. Not only will an increasing debt burden harm the prosperity and well-being of average Americans, our debt will heavily impact national security. The 2018 National Defense Strategy held: "without sustained and predictable investment to restore readiness and modernize our military to make it fit for our time, we will rapidly lose our military advantage, resulting in a Joint Force that has legacy systems irrelevant to the defense of our people."[7]

"The force does not get hollow by the flip of a switch, but by inadequate resourcing."— Adm. William E. Gortney

Across all services, our military is experiencing "force degradation resulting from many years of underinvestment…and the negative effects of budget sequestration (cuts in funding) on readiness and capacity."[8] These findings led the 2018 Military Strength Index to rate American military readiness as "marginal" across all divisions of the armed forces.[9]

The U.S. Air Force fleet is the smallest, oldest and "least ready that it's been since its founding in 1947", with the average plane being in service for over 30 years.[10] Our Navy's capabilities to build, upgrade—and most importantly—repair ships are quickly falling behind.[11] Other crucial American capabilities, such as deterrence, are also in question. On average, our ICBMs are 40 years old as China and Russia are building state-of-the-art infrastructure.[12]

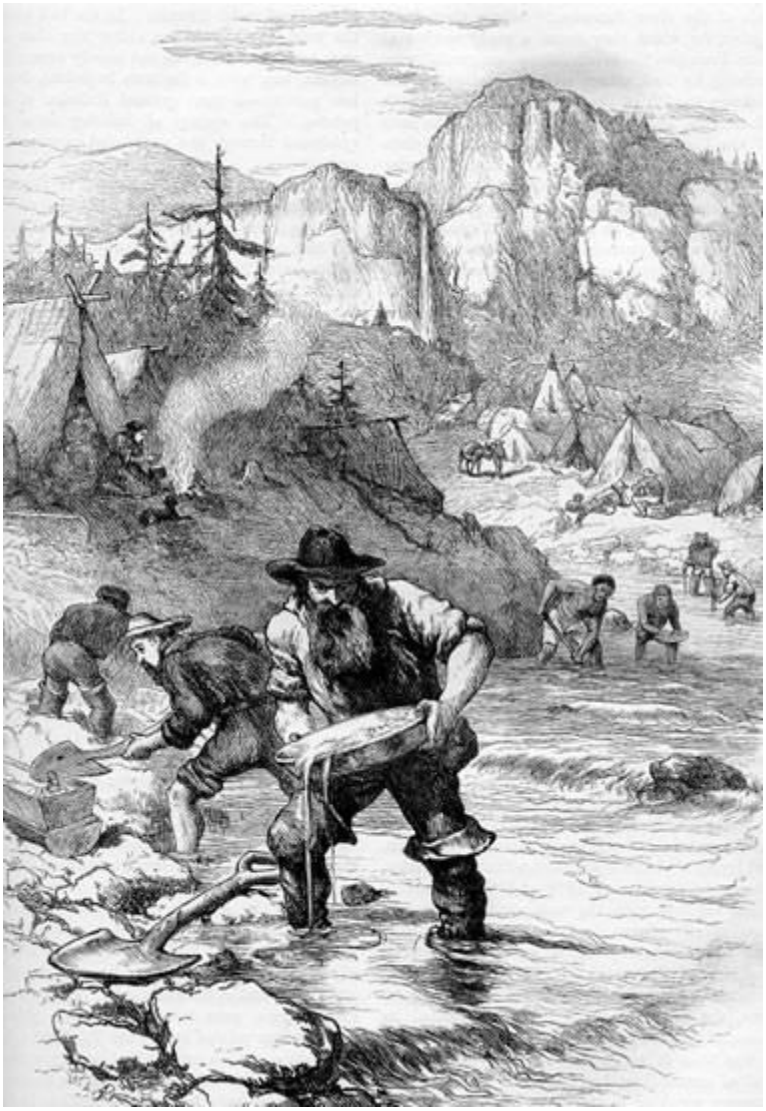
While it is commonly known that America has the largest military in the world, the reality is our forces and infrastructure are aging. Other great powers are able to build on new foundations, while America will need significant resources to repair, maintain, and modernize legacy systems with decades of technical debt. To make matters more complicated, America's forces play an unparalleled role in protecting trade routes, international stability, and global crisis response.

The last financial crisis brought us deep military budget cuts through sequestration. If the United States does not solve its debt problem, a future round of much deeper cuts is inevitable.

To keep our global influence strong, we must take action now. Ever-increasing debt will only accelerate our economic decline and hollow out our security capabilities on all fronts.

Remembering the Golden Years

While deeply unsettling, America's financial position is neither unprecedented nor hopeless. Dr. Lacy Hunt notes that America had another similar episode in the 1830's where Americans took on large amounts of debt to finance early steamship lines, canals, speculation and over-consumption.[13] This ultimately ended with the financial crisis of 1837 and brought on a recession that lasted for several long years. But suddenly, "a very fortuitous event occurred…the discovery of gold in California."[14]



The gold rush—an unexpected opportunity—pulled the U.S. out of financial distress and generated strong demand for our burgeoning transportation sector. New research refers to this period as "America's First Great Moderation."[15] The 1848 gold rush created unmatched economic success in American history with 16 years of strong, sustained growth. As Americans scrambled for gold, this period marked a "transportation revolution" with strong gains in productivity from expanding roads, canals, railroads and global shipping routes.[16] New technologies paved the way for this innovation such as more powerful steam engines, faster railroads, and the telegraph.[17]

This initial windfall also brought secondary effects throughout the economic foundations of America. Greater labor connectivity and transportation efficiency led to major gains across multiple sectors such as ship building, manufacturing, international trade, and agriculture.[18] Such developments brought in large amounts of foreign investments in American companies, further extending the cycle of stable economic growth.[19]

The external nature of the gold rush was key—internal solutions of more debt would have only worsened the ongoing financial malaise. The gold rush thus provides an excellent blueprint for how a fortuitous event can spur critical changes across an economy. Bitcoin, a remarkably similar external stimulus, can do the same for America today.

The Bitcoin Redemption

America needs to spark a second gold rush. Just as the gold rush provided the incentives necessary to revolutionize our transportation infrastructure, Bitcoin can provide the same dramatic changes to our energy infrastructure.

First, let's begin with a brief explanation of what Bitcoin is. Bitcoin can be thought of as a form of digital gold that can be sent over the internet. It is the first verifiably scarce digital asset. Instead of a being controlled by a single entity, Bitcoin uses a decentralized global network of peer-to-peer computers. With this architecture, two individuals can send and receive bitcoin without trusted intermediaries.

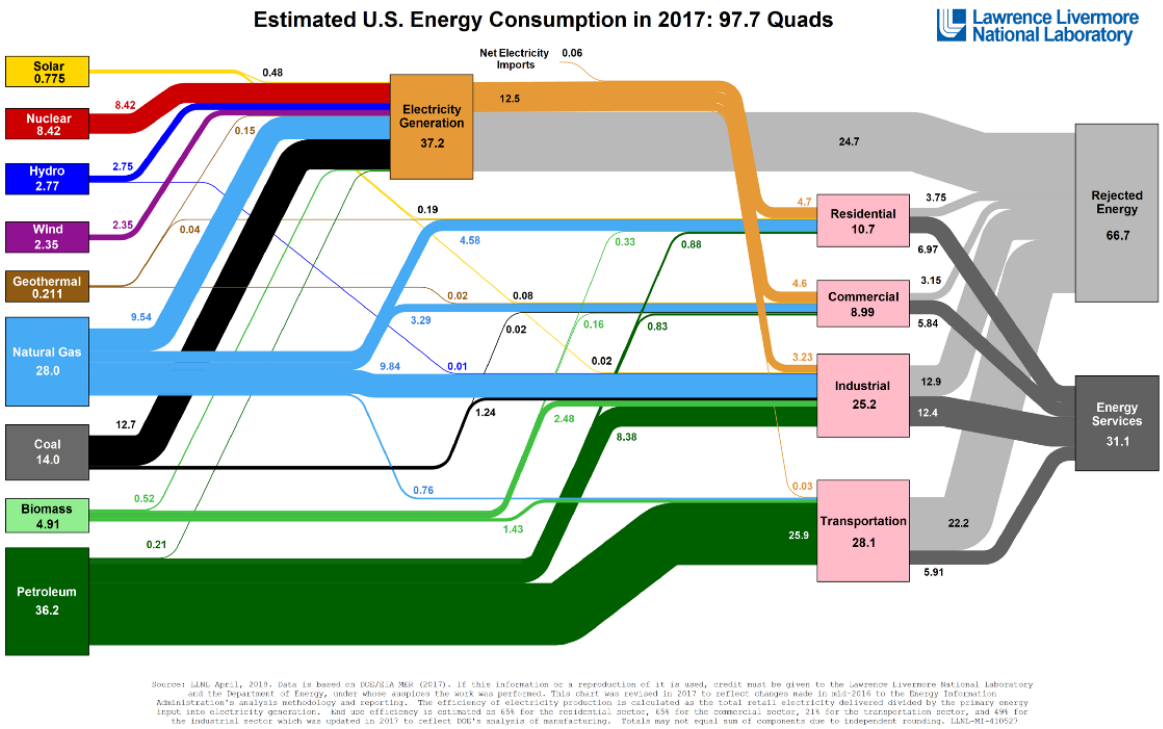
Bitcoin's novel structure gives it unprecedented characteristics. It is more scarce than any physical resource, infinitely divisible, teleporting, instantly verifiable, and cryptographically secured. With over a decade of continuous operation, Bitcoin has established itself as a peerless form of storing and communicating value.

Like other resources, new bitcoins are created through a process of mining. This involves expending electricity to secure the network and receiving a payout of freshly minted coins in return. However, unlike traditional mining, Bitcoin mining can be done anywhere electricity is available. The implications of this radically new design are staggering. For the first time, energy producers can tap into a global market for energy anywhere in the world.

With this in mind, let's turn to our current energy landscape.

Turning Waste Into Wealth

America has an energy problem—waste. Below is a chart from the Lawrence Livermore National Laboratory.[21] Each year they produce a chart showing just how much is wasted in our energy production. Notice that rejected energy accounts for around two-thirds of all electricity generation. This is energy that is produced but ultimately does not go to useful work. The amount wasted annually is around 66.7 quadrillion BTU's ("quads") of energy. For perspective, that is the energy equivalent of **wasting 2.3 billion metric tons of coal every year**.



Source: LLNL April, 2019. Data is based on DOE/EIA MER (2017). If this information or a reproduction of it is used, credit must be given to the Lawrence Livermore National Laboratory and the Department of Energy, under whose auspices the work was performed. This chart was revised in 2017 to reflect changes made in mid-2016 to the Energy Information Administration's analysis methodology and reporting. The efficiency of electricity production is calculated as the total retail electricity delivered divided by the primary energy input into electricity generation. End use efficiency is estimated as 65% for the residential sector, 65% for the commercial sector, 21% for the transportation sector, and 49% for the industrial sector which was updated in 2017 to reflect DOE's analysis of manufacturing. Totals may not equal sum of components due to independent rounding. LLNL-MI-410527

To make matters worse, this number has been increasing on a relative basis over time. In 1970 LLNL found our proportion of rejected energy was around 48%.

While much of this waste comes from inefficient appliances, transportation systems, and industrial processes, the largest share of rejected energy comes directly from electricity production itself, around 24.7 quads. This is precisely where Bitcoin can make a difference. By converting that wasted energy into Bitcoin, our energy producers will be more cost-efficient and energy-efficient without increasing emissions.

This is possible because no power plant is perfectly efficient. Excess capacity must be generated to meet demands that are constantly fluctuating from season to season, day by day, and hour by hour. To deal with this otherwise wasted energy, a grid equipped with Bitcoin miners could fluctuate with behind-the-meter demand and mine Bitcoin with excess reserves. If there was an energy intensive event (i.e. an especially hot afternoon), that excess capacity could be automatically allocated from the miners to the rest of the grid. The U.S. could lead this effort with 1) grant programs for plants to upgrade their systems, 2) tax incentives for plants mining with wasted energy, or 3) direct development and provision of mining technology.

The secondary benefits for economic growth are staggering. Increasing the efficiency of energy companies could drive the costs of energy to much lower rates. This would bring new power plants and energy suppliers online and could accelerate advances in energy technology, such as micro-reactors. As Ayers and Warr carefully argue in their book, ***The Economic Growth Engine***,

economic growth for the past two centuries has been driven largely by the declining effective cost of energy.[22] Their empirical analysis suggests the effect of energy efficiency, known as Jevon's Paradox, is the key driver for increased economic output. After examining many developed economies, they found that each economy's growth was directly stimulated by recent gains in energy efficiency. They conclude that new dramatic developments are needed in energy production, otherwise prolonged global depression is "a serious risk."[23]

Some early adopters are making this a reality with Bitcoin. Greenidge Power Plant in New York State have started testing Bitcoin mining to increase their station's efficiency in off-peak times. Their efforts are already generating around $50,000 of extra revenue per day at minimal costs to the plant. This drives home a powerful concept:

Bitcoin does not waste energy—it consumes energy waste.

This is precisely the paradigm shift for energy efficiency and production that Ayers and Warr call for. It's hard to comprehend how powerful an impact Bitcoin could have on the energy sector, and the economy more broadly. Transforming our power grid, establishing new forms of energy production, and reshaping electricity markets across the country would be a true energy renaissance. This dramatic shift would bring a myriad of economic benefits such as reducing household and business costs, creating many new well-paying jobs, and strengthening our global competitiveness. Federal officials have underscored this approach. Secretary of Energy Mark Menezes recently championed the importance of advanced projects that "enhance energy productivity…supporting the competitiveness of the entire U.S. manufacturing industry."

Meeting these economic objectives could easily lead to further secondary benefits through a stronger consumer, more foreign investment, sustained economic growth, and a robust, long-term profit motive for advanced energy technology.[25]

Lastly, there is the Bitcoin itself. If the United States strategically built a significant position in Bitcoin (i.e. 250,000+ BTC) before announcing plans for Bitcoin mining, the returns could be astronomical. A serious initiative by the U.S. would send a global message about Bitcoin's value and potential. Exchange rates would multiply overnight. By leading rather than following, America can create a windfall for our nation with the stroke of a pen.

Orange is the New Green

The recent collapse of the OPEC+ negotiations sent markets tumbling and America's energy sector into a financial spiral. This dramatic event and others

like it (such as last year's attacks on Abqaiq) highlight the continued importance of establishing American energy independence.

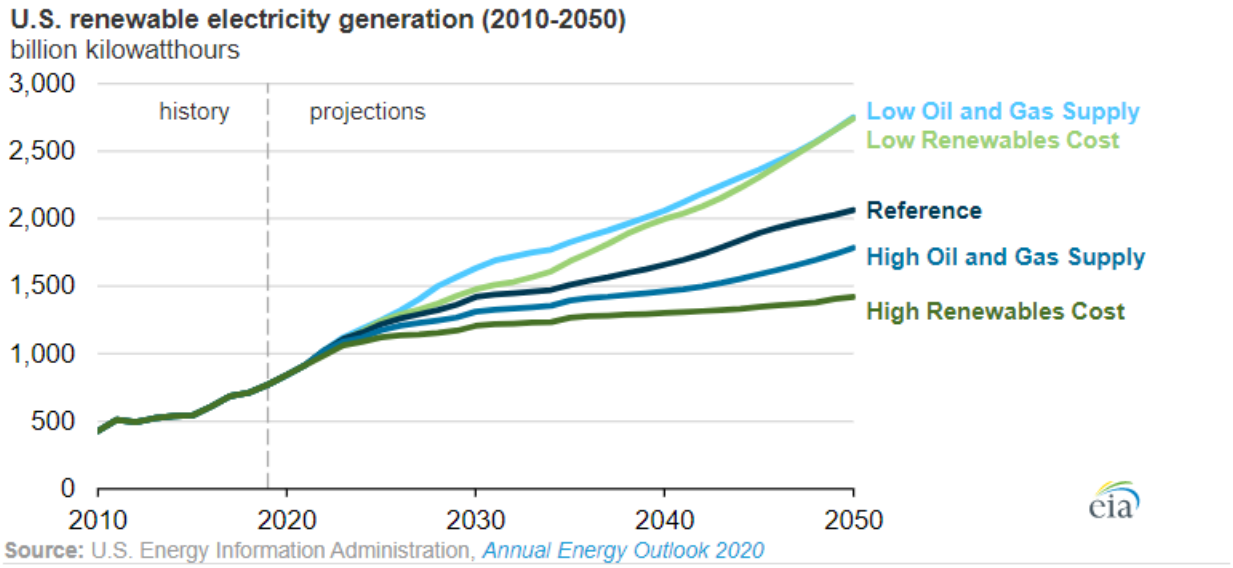
Despite decades of effort, America's economy is still heavily reliant on foreign fossil fuels. As the backbone of our economic system, depending on potential adversaries to supply our energy needs is a dangerous situation. Our current position leaves us vulnerable to foreign instability, market manipulation, attacks on supply infrastructure, as well as accidents and natural disasters. While a complete reduction in foreign energy imports is a tall order, Bitcoin can make significant gains by paving the way for renewable energy.

Sustainable energy like wind, solar, and nuclear are abundant. Nuclear energy alone could power the earth for hundreds of thousands of years with available supplies. The challenge for these resources is how expensive they are, especially when competing with existing infrastructure. However, Bitcoin mining presents the opportunity to quickly bootstrap renewables by turning excess capacity into profit.

The reasoning is as follows: when creating a new power plant, large amounts of excess capacity must be built into the system, especially with intermittent renewables such as wind, water, and solar. This excess enables a plant to reliably meet a location's future energy needs, peak demands, and population growth. While this excess is typically factored into the cost of producing new renewable capacity, Bitcoin erases these costs. Rather than having excess capacity go to waste, new renewables could start using their energy for Bitcoin production from day one. Furthermore, Bitcoin miners are perfect for providing _demand-side flexibility, _an essential aspect of renewable viability.[26]

The potential for Bitcoin-powered renewables is already evident in China. A 2019 report by Coinshares found that approximately 75% of Bitcoin mining comes from renewable energy sources, much of which stems from newly created hydroelectricity.[27] These new revenue streams have brought power plants online which otherwise would not have been economically viable given existing population density.

These field results match studies conducted by U.S. Energy Information Administration. Their latest Energy Outlook Report finds that lower cost is directly associated with a faster renewable transition.[28] As costs for renewable generation fall due to Bitcoin profits, renewable production will rapidly gain market share over imported fossil fuels.



The benefits of this bootstrapping effect are two-fold. First, cheaper renewables provide a clear path to energy independence. With a profitable and viable strategy for renewable energy, America could quickly begin its transition away from foreign fossil fuels and towards greater energy security.

Second, Bitcoin is a major victory for environmental sustainability. While many eco-advocates simply focus on reducing consumption, the best path to sustainability is vigorously pursuing profitability for clean energy. Once they are cost competitive, markets will create the proper incentives to bring new renewables into existence. Thus Bitcoin is a major step towards solving environmental sustainability domestically as well as signaling to other international actors on how to build competitive renewable grids.

Going green with Bitcoin not only helps the environment, but keeps us secure from foreign actors. Other countries are already beginning to take advantage of these benefits for their own energy markets. America should lead the way and set the stage for a renewable energy revolution that will shock the world.

Final Thoughts

Just a few months ago, Treasury Secretary Steve Mnuchin publicly declared Bitcoin to be “an issue of national security.” On this point, he could not be more correct. Bitcoin is a serious issue for our financial, energy, and environmental security. Each of these alone merit serious attention, but together they are one of the most important decisions facing us for years to come.

America is a nation of people who work hard, dream big, and never give up. The United States has the unprecedented opportunity to usher in a new era of prosperity, reigniting U.S. economic growth, building a strong base for

funding our armed services, and firmly establishing American energy independence. It is time to embrace who we are and forge our own future with Bitcoin. ***A special thanks to Karina for helping polish this up.***

Footnotes:

1. Department of Defense, ***National Security Strategy of the United States of America***,2017, p. 18–24, www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905-2.pdf
2. @CSPAN. " Fed Chair Powell: "The federal budget is on an unsustainable path with high and rising debt." ***Twitter***, 3 Nov. 2019, www.twitter.com/cspan/status/1194676593366577153?s=20
3. Congressional Budget Office, _The Budget and Economic Outlook: 2020 to 2030, _2019, www.cbo.gov/system/files/2020-01/56020-CBO-Outlook.pdf
4. Cox, Jeff. "Real US debt levels could be 2,000% of economy, a Wall Street report suggests" ***CNBC***, 9 Sep. 2019, www.cnbc.com/2019/09/09/real-us-debt-levels-could-be-a-shocking-2000percent-of-gdp-report-suggests.html
5. Hoisington Investment Management, ***Quarterly Review and Outlook Fourth Quarter 2019, _14 Jan. 2020***, _www.hoisingtonmgt.com/pdf/HIM2019Q4NP.pdf
6. ***Id.***
7. Department of Defense, _National Security Strategy Summary, _2018,dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf
8. The Heritage Foundation, _Heritage 2016 Index of US Military Strength, _2016, p. 12, www.ims-2016.s3.amazonaws.com/PDF/2016_Index_of_US_Military_Strength_ABOUT_EXECUTIVE_SUMMARY.pdf
9. The Heritage Foundation, "Executive Summary", 30 Oct. 2019, www.heritage.org/military-strength/executive-summary
10. Gregg, Sharon."Trump overstates military spending and readiness in face of Iran conflict.", ***The Washington Post***, 6. Jan. 2020, www.washingtonpost.com/us-policy/2020/01/06/trump-overstates-military-spending-readiness-potential-iran-conflict-looms/
11. Hawkings, William. "The Navel Industrial Base is in Worse Shape Than You Think." ***U.S. Naval Institute***, Aug. 2019, www.usni.org/magazines/proceedings/2019/august/naval-industrial-base-worse-shape-you-think
12. Mark Gunzinger, Carl Rehberg, and Gillian Evans. "America's Endangered Nuclear Deterrent: The Case for Funding Two Critical Capabilities." ***War on the Rocks***, 23 Apr 2018,

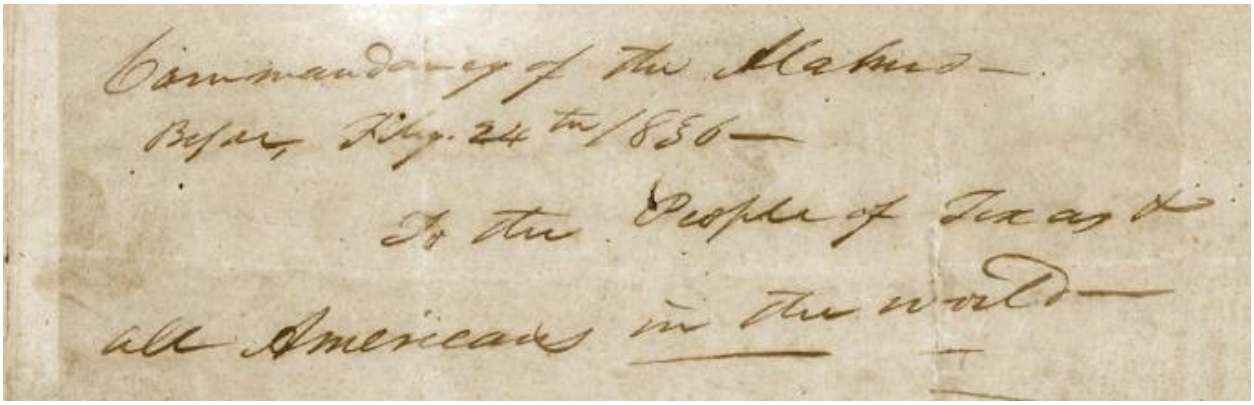
www.warontherocks.com/2018/04/americas-endangered-nuclear-deterrent-the-case-for-funding-two-critical-capabilities/
13. Townsend, Erik. _Dr. Lacy Hunt: The Bond Bull Market is NOT over! _Lacy Hunt, Macro Voices, 24 May 2018.
14. ***Id.***
15. Joseph Davis and Marc D. Weidenmier. "AMERICA'S FIRST GREAT MODERATION" National Bureu of Economic Research_, _Working Paper 21856, 2016, www.nber.org/papers/w21856.pdf
16. _Id. _at 15.
17. _Id. _at 14.
18. ***Id.*** at 16.
19. Rawls, James J., and Richard J. Orsi, editors. ***A Golden State: Mining and Economic Development in Gold Rush California***. University of California Press, 1999, p. 287, http://ark.cdlib.org/ark:/13030/ft758007r3/
20. For a great introduction to how bitcoin operates, I recommend this video https://www.youtube.com/watch?v=bBC-nXj3Ng4 Additional resources can be found at https://www.lopp.net/bitcoin-information/getting-started.html
21. https://flowcharts.llnl.gov
22. Ayres, Robert and Warr, Benjamin. ***The Economic Growth Engine: How Energy and Work Drive Material Prosperity.*** 2010.
23. ***Id.***
24. "Department of Energy Awards $187 Million to Strengthen U.S. Manufacturing Competitiveness" Department of Energy, 10 Feb. 2020. https://www.energy.gov/articles/department-energy-awards-187-million-strengthen-us-manufacturing-competitiveness
25. For further research on the benefits of energy production see, Kümmel. ***The Second Law of Economics: Energy, Entropy, and the Origins of Wealth***. Laitner, 2013. "Linking Energy Efficiency to Economic Productivity: Recommendations for Improving the Robustness of the U.S. Economy." Khan, 2012. ***The Long-Term Energy Efficiency Potential: What the Evidence Suggests***.
26. International Renewable Energy Agency, _DEMAND-SIDE FLEXIBILITY FOR POWER SECTOR TRANSFORMATION, _Dec 2019. https://www.irena.org/publications/2019/Dec/Demand-side-flexibility-for-power-sector-transformation
27. Christopher Bendiksen and Samuel Gibbons. "The Bitcoin Mining Network" Coinshares Research. May 2019, https://coinsharesgroup.com/assets/resources/Research/bitcoin-mining-network-june-2019-fidelity-foreword.pdf
28. Energy Information Administration, Annual Energy Outlook 2020, 2020, https://www.eia.gov/outlooks/aeo/

Bitcoin is a Rally Cry

By Parker Lewis

Posted March 26, 2020

“To the People of Texas and all Americans in the world.” In his open call to arms from the Alamo, Lt. Colonel William B. Travis began with an expression of America as an idea extending beyond borders, to all Americans in the world. It was a plea to all those that valued the fight for liberty and freedom. Outnumbered ten-to-one, Travis responded to a demand for surrender with a cannon shot. He was no more than 27 years old at the time. Texas declared its independence a week later, but within days, the Alamo fell. The Travis letter became the rallying cry of a revolution. Remember the Alamo. Ultimately, Texas won its independence. Always outnumbered, it is a reminder that the endless pursuit of freedom is a most powerful equalizer. And it is something inherent to the character of Americans in all the world.

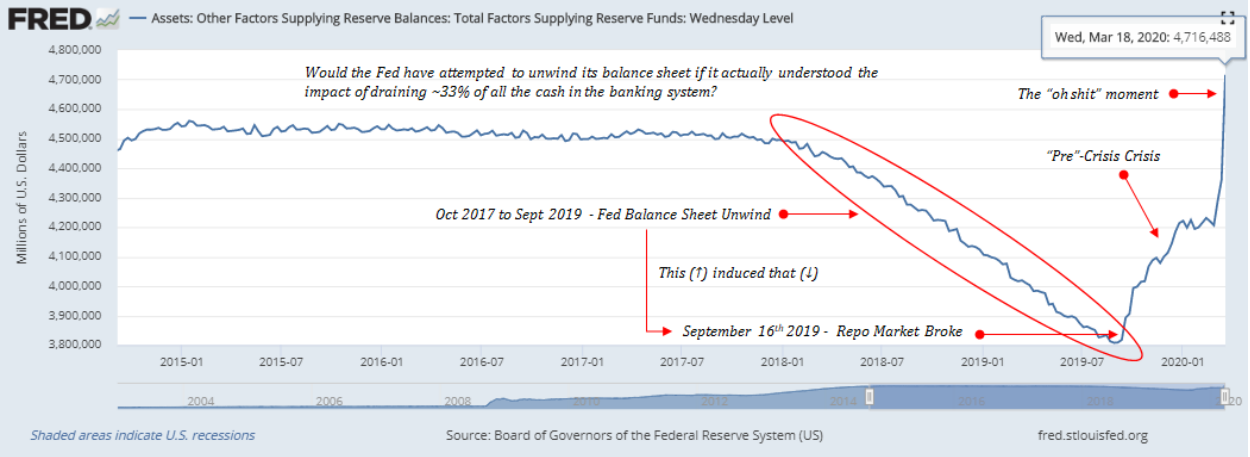

Commandancy of the Alamo—
Bejar Feby. 24th 1836—
To the People of Texas &
all Americans in the world—

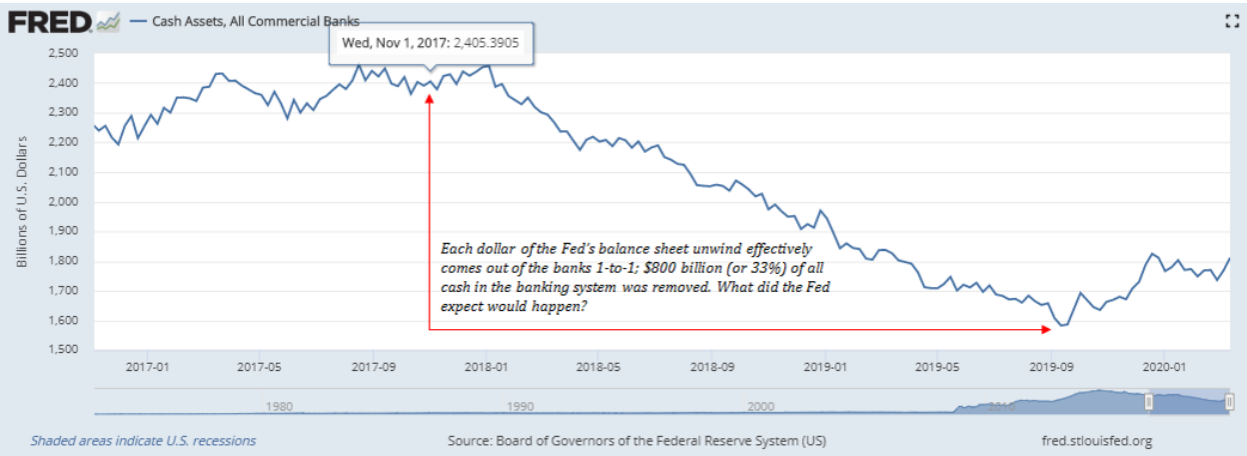
(Opening of the Travis Letter from the Alamo, February 24, 1836)

Minus the lionized heroes and a literal declaration of independence, bitcoin is still very much a fight for freedom, and it is similarly becoming a rally cry to all those that refuse to sit back and accept the fate of our tenuous financial system. The very idea of freedom may be the single most important tenet underpinning the monetary revolution to which bitcoin is giving rise. When the war is won, it will likely find its way directly into a constitutional amendment (even though it’s already covered by the first amendment). The right of the people to keep and bear bitcoin. Prior to bitcoin, everyone had no practical choice but to opt into a flawed currency system. That changed when bitcoin was released into the wild in 2009. Bitcoin is completely voluntary, it is controlled by no one, and it affords everyone the ability to store and transfer value in a form of currency that cannot be manipulated. Bitcoin may not be synonymous with the right to life, liberty and the pursuit of happiness but for

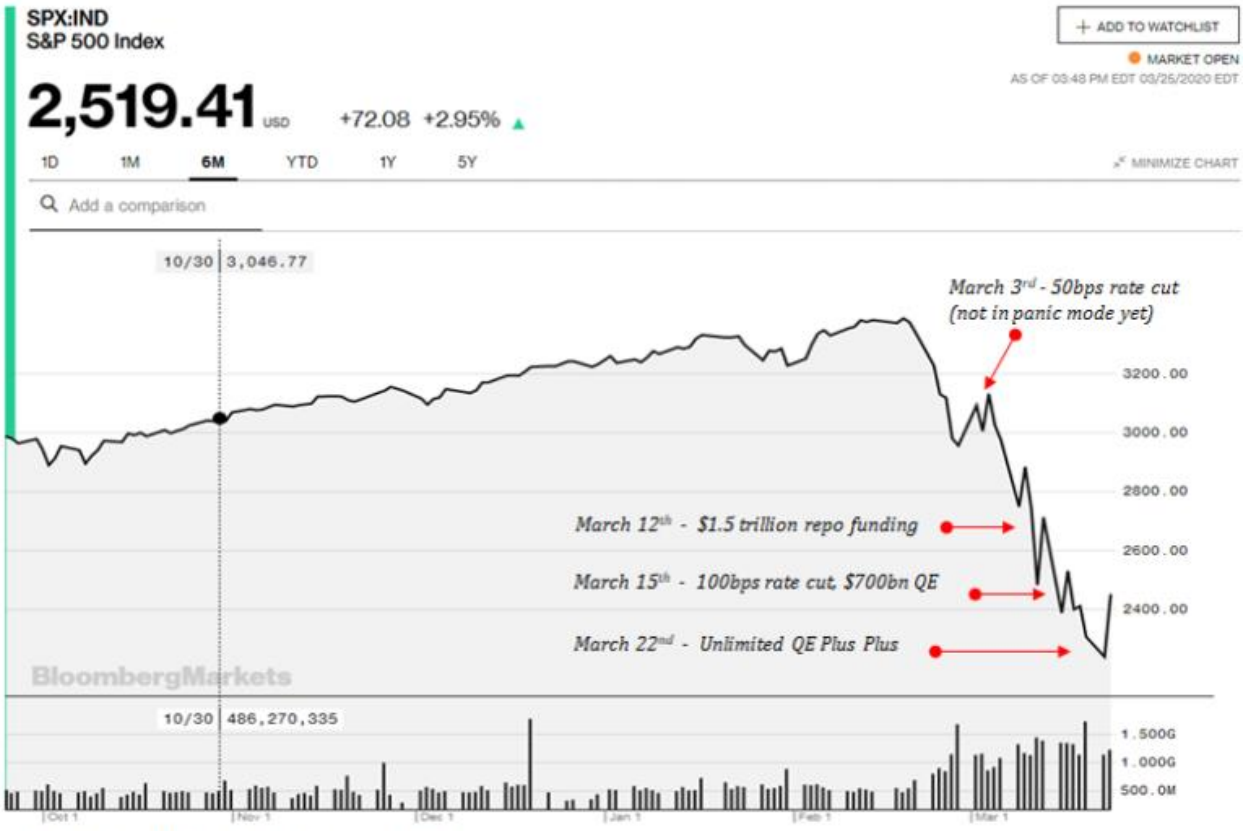
those that choose to rely upon it as a better path forward, it is a fundamental and inalienable right.

While bitcoin is valued for different reasons by different people, it consistently appeals to those that have identified the inherent level of freedom afforded by such a powerful tool, particularly in a world full of never-ending economic calamities. As the fragility and instability of the global financial system becomes more apparent by the day, central bankers and politicians scramble in a race to see who can provide more stimulus to an economy that is red-lining. Lest we not forget, the instability in the financial system is not just appearing; it is reappearing. The structural issues resurfacing are the same that existed during the 2008 financial crisis. Before the oil war and the global pandemic, the repo funding markets broke in September 2019. The writing was not just on the wall, it was in the repo markets. If it were not these recent events acting as the accelerant, it would have been some other random "act of god" which would have made evident what remained under the surface all along: a highly-levered financial system primed to break at the first signs of any material stress.





Even before the global shutdown (i.e. government-accelerated panic), the Fed had already supplied ~$500 billion in emergency funding to the repo markets. Now the fuel is really being dumped on the fire. But it is not just the scale that is alarming; it is the clear demonstration of control being lost through a meandering path of incrementalism. After the stock market crashed initially, the Fed issued an emergency 50bps interest rate cut; the market crashed some more and the Fed then announced an incremental $1.5 trillion in short-term funding (1-3 months) to be supplied in the repo markets. The market crashed again and three days later, a formal $700 billion "quantitative easing" program was announced to outright purchase $500 billion in U.S. government treasuries and $200 billion in mortgage-backed securities. Coinciding with this move, short-term rates were cut 100bps (all the way to zero).



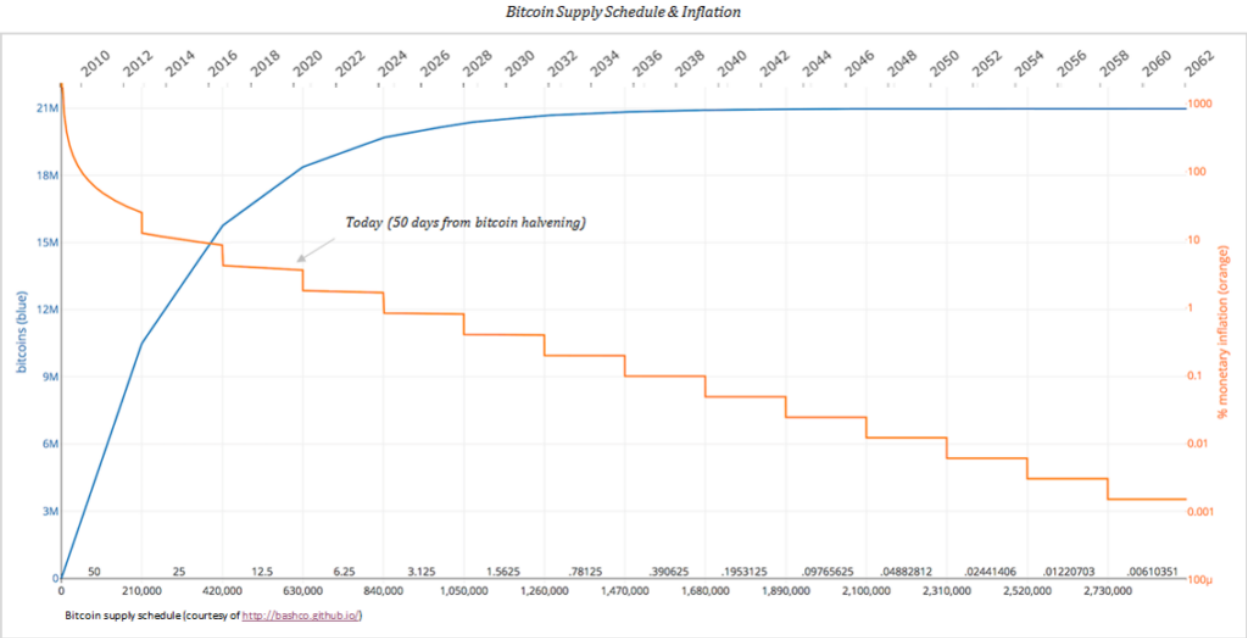
Source: BloombergMarkets (chart annotated by author)

Yep, the market crashed again, credit markets dislocated and the Fed followed with its "whatever it takes" response, announcing an unlimited QE program. Its three most aggressive moves to date all transpired within a 10-day window. And in its latest unprecedented act, the Fed will begin buying corporate bonds on the secondary market as well as participate in primary issuances of corporate credit. It also expanded its purchases of mortgage backed securities to include commercial mortgage backed securities

(commercial real estate). In addition, the Fed established a facility to issue asset backed securities to purchase student loans, auto loans, credit card loans, etc. All of this without a price tag, and just a promise to do whatever it takes. It would be funny if it weren't so serious, but the real question is, if the Fed were in control, why was it so reactionary? Why did its plans change so drastically in a ten-day period if it ever understood the extent of the issue? Never mind the unintended consequences, it is merely a demonstration that the Fed is not in control. Why would it have announced a $700 billion program if it didn't expect it to work? It's a classic game of guess and check, except the consequences can never be checked (only the immediate market reactions). The problem is our economy is at stake.

"There's an infinite amount of cash at the Federal Reserve" – Neel Kashkari, Minneapolis Fed President – March 22, 2020 (60 Minutes)

"To lend to a bank, we simply use the computer to mark up the size of the account they have with the Fed [...] it's much more akin to printing money than it is borrowing." – Ben Bernanke, Former Fed Chair – March 15, 2009 (60 Minutes)



Make no mistake, the $1.5 trillion supplied to the repo markets will be converted to increment the Fed's formal quantitative easing program, and the entire unquantified program should conservatively be expected to exceed $4 trillion when all is said and done. The Fed cannot put out the fire that is a liquidity crisis through short-term funding, and it will have no other choice but to monetize a larger share of the credit system than it did in 2008 because the problem is now larger. In addition, while not yet passed, Congress is working on an initial $2.0 trillion stimulus package in response to

the global pandemic. With a market already suffering a liquidity crisis, the banking system does not magically have this cash on hand to finance a massive expansion of the Federal government's deficit. There is a liquidity crisis unfolding after all. As a result, the Fed will be forced to finance any fiscal response through an ever-expanding quantitative easing program. It is the only way for the banks to get the cash needed to finance such a fiscal stimulus. All roads lead back to the Fed and endless QE.

This is the new normal and there is nothing sustainable about it. It is also not a reality we have to accept. There is a better way. As the world looks on, amidst the fear and panic, it often seems that there is no alternative. It is unclear when so many began to view the government's role as one of fighting global pandemics (rather than the free market) but that is the world for which so many seem to aggressively demand. It is a symptom of failing to understand the root problem. It is misdiagnosing the fallout of a global pandemic and falsely believing the only hope is to allocate money created out of thin air by central banks and governments. It is predictably irrational. There is no reason even a few-month, complete economic shutdown should put the world on the brink of a global depression. Instead, it is the output of an inherently fragile financial system, one dependent on perpetual credit expansion necessary to sustain itself and without which it would begin to collapse. It is the fragility of the global financial system itself that is the problem, not a global pandemic. Do not be fooled. This isn't a pandemic induced failure of the financial system. This was a 100% eventuality, pandemic or not. If not for its heavy dependence on credit and an unsustainable degree of leverage, the world would not be waking up to the S&P 500 futures locked limit down with seeming regularity.

And the economic dependence on credit as well as the high degree of system leverage are not a natural function of either capitalism or a free market. This market setup is a function of central banks everywhere. The instability is not by design but the market structure is. In response to every economic slow down (or crisis) which has appeared over the last four decades, central banks (including the Fed) have responded by increasing the money supply and reducing interest rates, such that existing debt levels could be sustained and such that more credit could be created. Every time the system as a whole attempted to deleverage, central banks worked to prevent it through monetary stimulus, ultimately kicking the can down the road and allowing decades of economic imbalance to accumulate in the credit system. This is the root cause of the inherent fragility in the financial system (see here). And it is why each time an economic disruption surfaces, the monetary response from central banks need be larger and more extreme. With greater imbalance comes the need for a bigger boat.

In doing so, the entire system is pushed further and further out onto the same ledge. The terminal risk to the system (the stability of the underlying currency) becomes greater and greater. Everyone is unwittingly forced to be along for this most unnerving of rides, but for those paying attention to the real game that is being played, bitcoin is increasingly becoming the clearest path to opt out of the insanity. Simplified down to the least common denominator, quantitative easing is a forced debasement (or devaluation) of monetary savings. It distorts every pricing mechanism within an economy and its intended goal is the expansion of credit. When history books are written of this pre-bitcoin era, the failure to understand the consequence of distorting global pricing mechanisms will be identified as the source of all other critically flawed assumptions in modern central banking doctrine. There is no escaping it. You can only hope to manage the fallout. But where don't-tread-on-me meets the come-and-take-it mentality, freedom loving Americans of all the world and of all walks of life are beginning to say enough is enough. There has to be a better way because there always is.

That is core to the very idea of hope and the very nature of human ingenuity. It is an unwillingness to accept the new normal as a fait accompli. If quantitative easing can be simplified down to a debasement of monetary savings; bitcoin can be simplified down to the freedom to convert value into a form of currency that cannot be manipulated. In ***the Road to Serfdom***, Hayek describes the function of money most aptly: "It would be much truer to say that money is one of the greatest instruments of freedom ever invented by man." As he goes on to further explain, it is money that ultimately affords people a range of choice far greater than could otherwise be imaginable. It does so by distributing knowledge through its pricing mechanism, the single most important market signal (in aggregate) which facilitates economic coordination and the allocation of resources. However, as the freedoms afforded by one monetary medium become impaired, it should be no surprise that human ingenuity would find a way to route around and spawn a new creation that performs that same function more effectively. That is bitcoin and there is no going back. The proverbial cat is out of the bag and the distribution of knowledge is naturally exponential.

The promise of bitcoin is a more stable monetary system. There are no promises of what its value will be on any given day; the only assurance it provides is that its supply is not subject to manipulation or systematic debasement by a central bank (or anyone else). There is the seemingly constant question as to whether bitcoin is a “safe-haven” and more recently, why bitcoin has become correlated to the broader (collapsing) financial markets. The simple reality is that bitcoin is not a safe-haven, at least not as commonly defined in the mainstream. It is not held widely enough for it to possibly be a safe-haven. It remains nascent and it is perfectly predictable that at the onset of a global deleveraging event, a liquid asset would be sold along with everything else.

However, what remains true is that bitcoin is the antifragile competitor to the inherently fragile financial system.

In his book under the same name, Nassim Taleb describes antifragility as not just robust or resilient, but as the opposite of fragile. Antifragile systems actually gain strength and feed on volatility. The recent volatility in bitcoin is likely just the beginning but what it really represents is uninterrupted and unceasing price discovery. There are no circuit breakers in bitcoin and there are no bailouts. Each individual participant is maximally accountable and it is a market devoid of moral hazard. When the dust settles, what does not kill bitcoin only makes it stronger. In a literal sense. It is surviving and thriving in the wild, without any central coordination. It is not for the faint of heart, but it is the land of the free and the home of the brave. When it survives, there will still only be 21 million bitcoin, and its very survival will reinforce its place in the world. Increasingly, with each monetary stimulus injected into the legacy financial system, bitcoin’s core value function will become more apparent and more intuitive to more people. It will not just be by chance; it will be so because of the stark contrast bitcoin provides. Even with all its volatility, it is laying the foundation of a more stable monetary system.

Bitcoin Price Chart (Source: Coinbase Pro Exchange, 6 hour intervals)

Because the supply of bitcoin cannot be manipulated, its price and its supply of credit will similarly and forever be unmanipulable. Both will be determined on the market. As a result, the size of the bitcoin credit system will never sustain otherwise unsustainable imbalances. Beyond the nature of its fixed supply, this is where the contrast lies in practical application. The accumulation of sustained credit system imbalances (induced by central banks) is the inherent source of fragility in the global economy today. In a market built on the foundation of a currency that cannot be manipulated, as soon as imbalances arise, economic forces will naturally course correct, preventing the system-wide and systemic credit risk that plagues the legacy financial system. Rather than impair the future by allowing imbalances to accumulate beneath the surface, the unmanipulable supply of bitcoin will act as a governor to stamp out fires as soon as they appear. The fragile individual components of the system will be sacrificed and the system as a whole will become more antifragile by that very function.

For Joe Squawk (your modern-day average joe), it was Facebook's Libra that made bitcoin more intuitive. For others, it is hyperinflation in Venezuela. And now for many, it will increasingly become the incessant reality that financial crises and QE are a recurring fact of life. No matter how many cycles of quantitative easing the Fed and its global counterparts have in their bag of tricks, bitcoin is inevitably becoming a rallying cry for all those that see the train wreck coming and are unwilling to stand idly by. It is not just a collective act of civil disobedience; it is an individual recognition of the need to act in self-preservation. There is a point in time for most everyone when common sense and survival instinct naturally take the reins. The avenue may be different for each individual, but at the end of the day, bitcoin is a means to preserve some form of freedom that is otherwise being impaired or infringed. Whether governments attempt to ban bitcoin or it is mistakenly blamed for the failures of the legacy system, always remember the simplicity of what bitcoin represents. It is nothing more than the individual freedom to convert real world value into a form of money that cannot be manipulated. It is a most basic and fundamental freedom but one that must be earned. So to all Americans in the world, stay humble, stack sats, and hold the damn line. Whatever it takes.

"The enemy has demanded a surrender [...] I have answered the demand with a cannon shot"
– Lt. Colonel William B. Travis (February 24, 1836) Link to Full Travis Letter

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

Calling Bitcoin a NSA/CIA Project Is Disrespectful to Cypherpunks

By Vlad Costea

Posted March 27, 2020

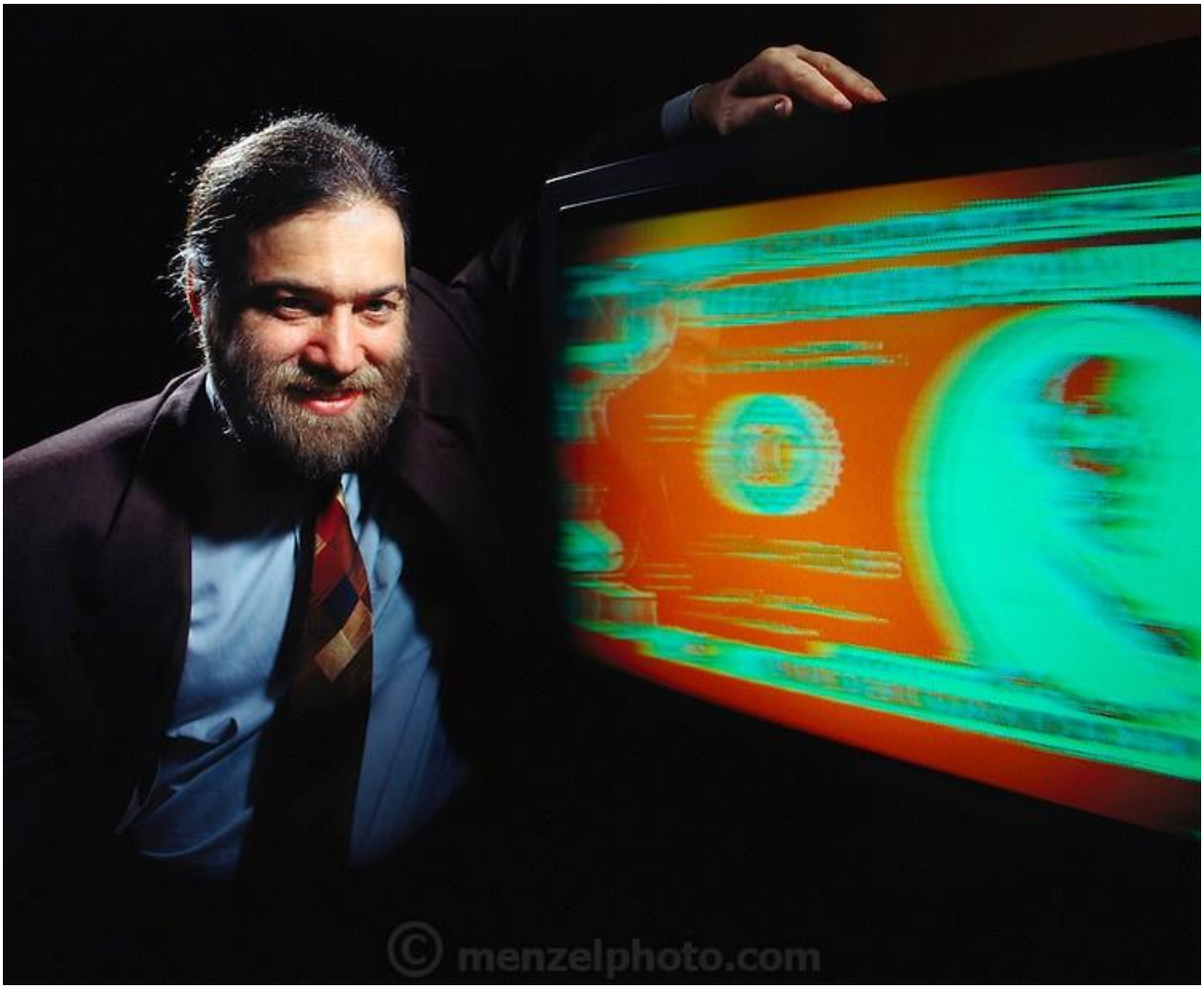
I've recently asked my Twitter followers to mention their favorite Bitcoin conspiracy theory. Surprisingly, most respondents have mentioned the CIA, the NSA, or another "three-letter agency" as the potential creators of the cryptocurrency. Deater Bob suggested that Satoshi Nakamoto might have leaked the Bitcoin project from sources within the US government. Gilroy pointed out to a master plan that would eventually use Satoshi's coins as the foundation for a new US treasury. The likes of Juan Galt and Jack have also suggested that the NSA might have been involved. And in spite of some creative replies (such as Wladimir Van Der Laan's theory about Bitcoin being a fungus and Bmo Masari's suggestion that the internet itself might have attained consciousness in order to create Bitcoin), I couldn't stop thinking about the popular associations between the creation of Bitcoin and governmental agencies.

Therefore, I will explain why the association is wrongful – and even if Satoshi Nakamoto was the CIA or the NSA, Bitcoin no longer belongs to him, and it isn't even as innovative as most people think. Bitcoin didn't come out of nowhere and borrows multiple breakthroughs that cypherpunks have previously made. To Satoshi Nakamoto's credit, he/she/they/it have created the best solutions for the Byzantine Generals Problem, and is/are responsible for releasing a form of decentralized electronic money that actually succeeded. The difficulty adjustment every 2016 blocks is also a fine touch, and one which has been crucial for the survival of the network. However, there is a cypherpunk tradition that precedes Satoshi's emergence by 20+ years. And this article will present only a few of the inventions that have taught Satoshi how to design Bitcoin and which proven flaws to avoid.

Satoshi Nakamoto might be the CIA/NSA, but Bitcoin is rooted in the cypherpunk tradition.

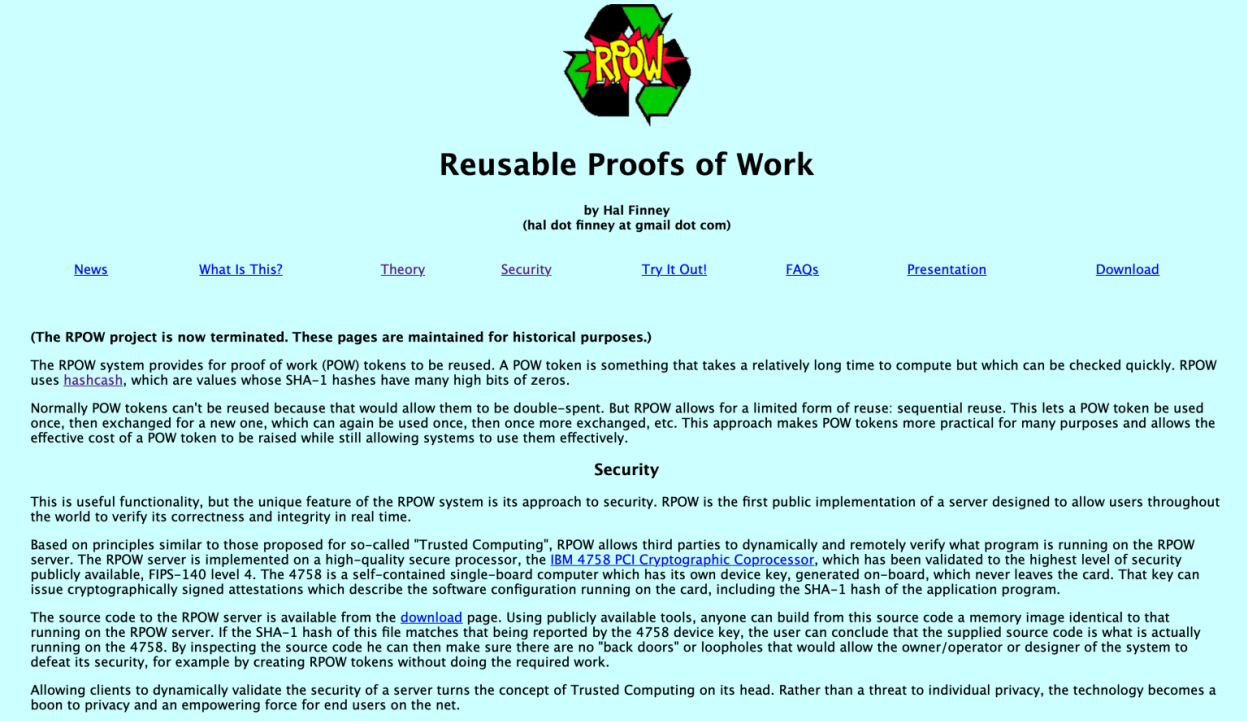
Lots of nocoiners, precoiners, and poorly informed bitcoiners think that Satoshi

Nakamoto invented the blockchain and deserves all the credits for the accounting system which spawned an entire industry. Like many other cryptographic inventions, the blockchain was first conceptualized by David Chaum during his PhD at Berkeley University. His 1979 Vault system even includes checks and balances that very much resemble Bitcoin's: watchers (block explorers), doers (nodes), executives (miners), czars (developers). Chaum also created the first form of digital money (ecash) with the DigiCash corporation. It was designed to fix the trust issues of online credit card payments with a form of money that is private enough to conceal personal data that is irrelevant to the transaction. However, its centralization ultimately led to a disappointing demise in the late 1990s. Interestingly, Satoshi doesn't mention Chaum in the Bitcoin whitepaper.



Let's get back to the blockchain: the idea of an hash chain that is used for linked timestamping is also presented in a 1991 research paper by Stuart Haber & W. Scott Stornetta. Unlike David Chaum's work, Satoshi does reference this breakthrough in the Bitcoin whitepaper. Also, cypherpunk

Jameson Lopp has cited the research as a precursor to Bitcoin's blockchain. Then there's the choice of Elliptic Curve Digital Signature Algorithm (ECDSA), published in 1998 by Canadian computer science researchers Don Johnson, Alfred Menezes, and Scott Vanstone. With ECDSA, public keys, private keys, and signatures get generated in order to guarantee that the bitcoins can only be spent by the rightful owners. A popular theory says that Satoshi Nakamoto picked ECDSA over Schnorr signatures out of convenience, as more libraries were available to suit his/their specific needs when designing Bitcoin. Yet there are lots of privacy concerns (that do involve the NSA's tendency to implant backdoors) that will eventually replace ECDSA with Schnorr signatures (thanks, Pieter Wuille!). The idea of cryptography that uses public keys is also not proprietary to Satoshi Nakamoto: Ralph Merkle was researching the topic in 1980 (as acknowledged by the Bitcoin creator in the whitepaper), and Phil Zimmermann's private e-mailing tool PGP (on which Hal Finney has worked for many years) has been available on the internet for free since 1991.



Reusable Proofs of Work

by Hal Finney
(hal dot finney at gmail dot com)

News | What Is This? | Theory | Security | Try It Out! | FAQs | Presentation | Download

(The RPOW project is now terminated. These pages are maintained for historical purposes.)

The RPOW system provides for proof of work (POW) tokens to be reused. A POW token is something that takes a relatively long time to compute but which can be checked quickly. RPOW uses hashcash, which are values whose SHA-1 hashes have many high bits of zeros.

Normally POW tokens can't be reused because that would allow them to be double-spent. But RPOW allows for a limited form of reuse: sequential reuse. This lets a POW token be used once, then exchanged for a new one, which can again be used once, then once more exchanged, etc. This approach makes POW tokens more practical for many purposes and allows the effective cost of a POW token to be raised while still allowing systems to use them effectively.

Security

This is useful functionality, but the unique feature of the RPOW system is its approach to security. RPOW is the first public implementation of a server designed to allow users throughout the world to verify its correctness and integrity in real time.

Based on principles similar to those proposed for so-called "Trusted Computing", RPOW allows third parties to dynamically and remotely verify what program is running on the RPOW server. The RPOW server is implemented on a high-quality secure processor, the IBM 4758 PCI Cryptographic Coprocessor, which has been validated to the highest level of security publicly available, FIPS-140 level 4. The 4758 is a self-contained single-board computer which has its own device key, generated on-board, which never leaves the card. That key can issue cryptographically signed attestations which describe the software configuration running on the card, including the SHA-1 hash of the application program.

The source code to the RPOW server is available from the download page. Using publicly available tools, anyone can build from this source code a memory image identical to that running on the RPOW server. If the SHA-1 hash of this file matches that being reported by the 4758 device key, the user can conclude that the supplied source code is what is actually running on the 4758. By inspecting the source code he can then make sure there are no "back doors" or loopholes that would allow the owner/operator or designer of the system to defeat its security, for example by creating RPOW tokens without doing the required work.

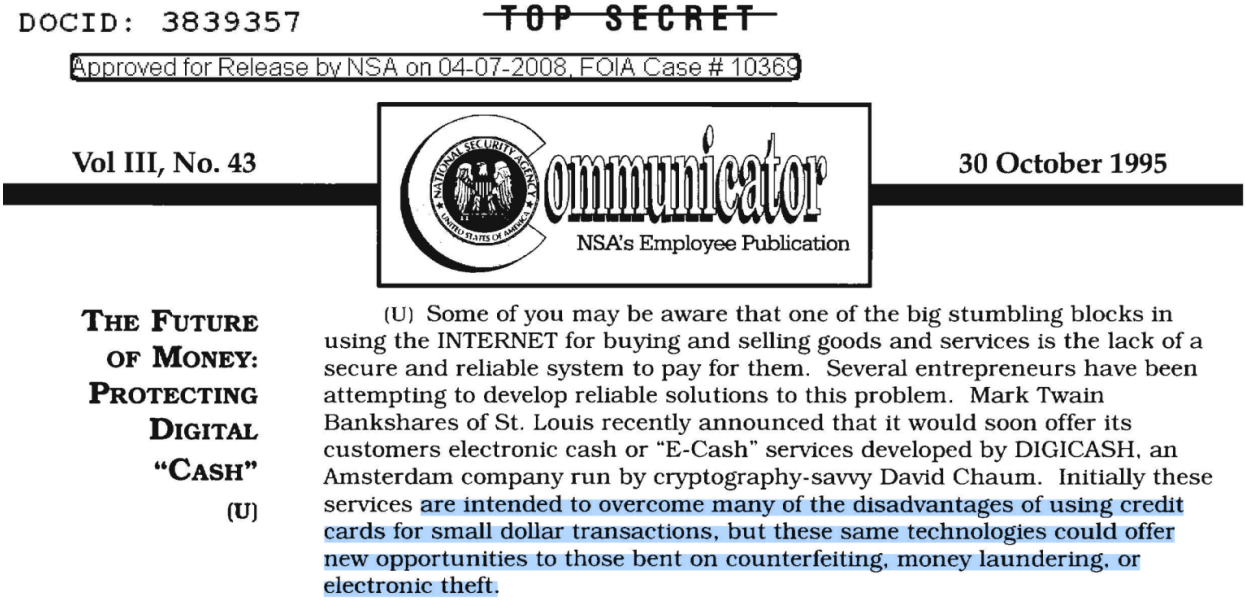
Allowing clients to dynamically validate the security of a server turns the concept of Trusted Computing on its head. Rather than a threat to individual privacy, the technology becomes a boon to privacy and an empowering force for end users on the net.

Speaking of Hal Finney, Bitcoin makes use of his Reusable Proof of Work (RPOW) breakthrough. However, it's Adam Back who gets cited in the whitepaper for inventing the hashcash system in 1997 and perfecting it to prevent e-mail spam. Without these cryptographic breakthroughs, Bitcoin could have never reached the same degree of security and the brilliant mining incentives most likely wouldn't have existed. Yet another great cypherpunk who doesn't get cited in the whitepaper but has basically solved

90% of Satoshi's problems is Nick Szabo. His Bit gold system successfully connects many puzzle pieces from amongst the most brilliant cryptographic discoveries, and also creates the "digital gold" principles that are rooted in Austrian economics (scarcity, fixed issuance rate which avoids the pitfalls of hyperinflation, easy verification). Unfortunately, the Bit gold design relied on a majority of network participants and could be easily become subjected to 51% attacks. What Satoshi Nakamoto did was to replace the rule of CPUs with the rule of hash power.

These cypherpunks were all about privacy and resisting the NSA

The "punk" in "cypherpunk" should successfully delineate the movement from government servitude. According to Tim May's 1994 opus "The Cyphernomicon", the cypherpunks were very much against surveillance and sought to keep their privacy on the internet while inventing tools to also help others. Compliance in itself was synonymous with an ideological capitulation. David Chaum wrote "Blind Signatures for Untraceable Payments" in 1983, and "Security Without Identification: Card Computers to Make Big Brother Obsolete" in 1985.



DOCID: 3839357 ~~TOP SECRET~~

Approved for Release by NSA on 04-07-2008, FOIA Case # 10369

Vol III, No. 43 — Communicator — NSA's Employee Publication — 30 October 1995

THE FUTURE OF MONEY: PROTECTING DIGITAL "CASH" (U)

(U) Some of you may be aware that one of the big stumbling blocks in using the INTERNET for buying and selling goods and services is the lack of a secure and reliable system to pay for them. Several entrepreneurs have been attempting to develop reliable solutions to this problem. Mark Twain Bankshares of St. Louis recently announced that it would soon offer its customers electronic cash or "E-Cash" services developed by DIGICASH, an Amsterdam company run by cryptography-savvy David Chaum. Initially these services are intended to overcome many of the disadvantages of using credit cards for small dollar transactions, but these same technologies could offer new opportunities to those bent on counterfeiting, money laundering, or electronic theft.

In an October 1995 report by the NSA (which was declassified in 2008), some concerns were expressed in regards to the ways in which DigiCash can be used for criminal activities. The existence of this particular document proves that Chaum's intentions were real and he truly was concerned with privacy. It's very unlikely that cypherpunks like Finney, Szabo, Back, Haber, and Stornetta worked for the NSA, CIA, or any other governmental agency. Otherwise their work would have been classified and restricted to only be used by authorized personnel. And even if we assume that the open source

work was released as such to get further improved by other voluntary cryptographers on the internet, the fact that these tools work against the monopolistic interests of the NSA/CIA also makes the cypherpunks look pure at heart. If the NSA decides to use RPOW or the ideas behind Bit gold to build a system of their own (which most likely happened already to some extent), it doesn't mean that the inventors of these systems were their employees.

Bitcoin was invented by Satoshi, but it never belonged to him

At most, a returning Satoshi Nakamoto can move his coins and spend them. There is no backdoor key, there is no reserved lead developer position, and there is no active developer who awaits the return of the creator. Like it or not, Bitcoin is not the same network it was in 2009. It has undergone numerous improvements and will continue to leave Satoshi Nakamoto's legacy behind as more parts get replaced. After all, the point of Bitcoin is not to remain unchanged over time, but to keep its monetary policy, guarantee that Satoshi can return at any time and move the coins, and preserve decentralization. There is a lot that Satoshi Nakamoto got right, but also plenty of code that was removed or replaced by developers. Hal Finney has spent a lot of time fixing design flaws in Bitcoin (and even added extra zeroes to define the system's smallest monetary unit as 1/100.000.000 BTC) and he set a precedent for future devs to seek more elegant and efficient fixes for an otherwise rigid project.

Bitcoin as a monetary system is set in stone with a fixed supply, a predictable inflation until 2140, clear mining rewards, and convenient difficulty adjustments every 2016 blocks. But Bitcoin as a network is bound to receive lots of upgrades that make it faster, more private, and more efficient. Improvement proposals like Schnorr signatures, Taproot, MAST, and Grafroot are designed to bring greater privacy and block efficiency (transactions will get smaller and more affordable). Then there are lots of privacy improvements that are being explored on altcoin networks and sidechains (it's only a matter of time until Confidential Transactions or

MimbleWimble get added to the base layer to some degree). In the future, it's likely for transaction privacy to become more popular, and smart tricks that still guarantee supply auditability and inflation resistance will be implemented. If Satoshi returned, he probably wouldn't recognize his own invention. But that's for the better, as the network is growing and becoming much more efficient for its purpose. Bitcoin is like a muscle car which receives upgrades without ever changing the body frame – it will always retain the main design qualities, but with a better engine and bulletproof windows.

If Satoshi Nakamoto is the NSA/CIA, then Bitcoin does not belong to them anyway

Is Bitcoin designed by a three-letter agency? It's definitely possible. Could the CIA and NSA use Bitcoin for transactions? That's even more likely. But neither of these two probabilities lead to a conclusion that puts a governmental agency in control. Right now, Bitcoin may possibly be the most decentralized computer network on the planet. It has functioned for almost 11 years with only two instances of downtime (due to an inflation bug in 2010 and due to poor network synchronization in 2013) and has ~10000 nodes operating worldwide (not counting the ones running on Tor and the ones that didn't open the 8333 port). Some argue that backdoors may exist: and the most damage they can do is break the signatures (which can lead to funds being stolen) or break the cryptography behind SHA256. In either case, it's possible for the community to hard fork to a new chain, replace both ECDSA and SHA256 with existing alternatives that have already been already been developed, and restore previous coin ownership on the basis of cryptographic proof. The solution seems unpopular now, but may prove to be the last resort in the event of a serious attack of the kind which Bitcoin never really faced. The battle against Big Brother is relentless, and it's clear that government officials understand the trade-offs involved in launching attacks or momentarily lack the means to engage. It's also probable that the CIA and the NSA find the existence of Bitcoin convenient, as they use it themselves and have their own ways to track transactions on the blockchain by looking at communications between participants and other network-level clues. But

even if we assume that Satoshi Nakamoto was the father of all CIA agents, the experiment has escaped his hands and he is no longer in control – and nor will he ever be again, unless the network becomes more centralized (as it happened with BCH and BSV).

And even if half of the Bitcoin community is under CIA's paycheck, then the other half can still resist attacks by moving to another chain which retains the rules but changes the security. It's all open-source software and the means to protect one's property should be enforced. Yet thanks to the brilliant network incentives, it's better for everyone (CIA agents or not) to stick together and protect the same network. For as long as greed works, Bitcoin will remain secure and adversarial in terms of who it onboards and for what reasons. The "don't trust, verify" motto mostly refers to other people's nodes and implies having your own node as a way of proving that the funds exist and are rightfully yours. Therefore, it's an assumption that everyone else is out there to rob you – because you know, everyone's a scammer.

Muh Satoshi

The Satoshi Nakamoto we know from forum posts and the cypherpunk mailing list was pretty humble and down-to-earth. He was willing to help anyone understand how Bitcoin works – with the exception of Daniel Larimer, who got dismissed in a pretty badass way. However, turning him into some sort of Messianic figure who gave us the power of the Holy Spirit and departed to return "someday" is definitely wrong. We can't deny Satoshi's contributions to the world of cryptography, but we can't exaggerate his work either. Sure, the story of the unknown computer programmer who released an innovative digital money system out of nowhere seems romantic. It

attracts newcomers and it keeps the media busy with phony investigations. Yet the genius of Satoshi Nakamoto is overstated and there is very little that he added to the otherwise impressive but lesser popular inventions of his peers. It's the classic example of Isaac Newton and Gottfriend Wilhelm Leibniz: everyone knows about the former and his story with the apple, but tends to forget about the latter. They both discovered integral mathematical calculus around the same time, but the glory appears to be on the side of the English polymath to an unfair extent. The bottom line is that it doesn't matter who Satoshi Nakamoto really was and it's extremely irrelevant at this point in Bitcoin's development. Also, the NSA/CIA stories are pretty unfortunate given the cypherpunk origins of Bitcoin. **While Satoshi might have been the NSA, then Bitcoin clearly isn't.**

37EmPGG6mw2BSq54WVEs8EJJToNZXopKV4

Enjoyed the article? Donate to the Bitcoin Takeover project: 37EmPGG6mw2BSq54WVEs8EJJToNZXopKV4

Stock-to-Flow Influences on Bitcoin Price

Challenging the popular understanding

By Nick

Posted March 27, 2020

Abstract

This article attempts to completely invalidate the statistics behind the idea that there is any stock-to-flow relationship to Bitcoin price. The proposed Ordinary Least Squares (OLS) model is shown to be seriously deficient due to the serial correlation in the residuals. The Engle-Granger method is shown to be not usable as a test for cointegration due to requirements for the test not being met. The Johansen method is similarly invalidated. Finally, an Auto Regressive Distributed Lag model (ARDL) is built to test for cointegration. The ARDL model does not falsify the stock to flow relationship. Thus whilst many tests have been able to be shown to be incorrect or have series errors, we have been able to reject the hypothesis that stock-to-flow does not have an important non-spurious influence on the US dollar price of Bitcoin.

Notes

- All analysis was performed using Stata 14.
- This is not financial advice.

Notation

Medium is relatively limited for mathematical notation. The usual notation for an estimate of a statistical parameter is to place a hat on top. Instead, we define the estimate of a term as [ ]. e.g. the estimate of β = [β]. If we are representing a 2x2 matrix, we will do so like this [r1c1, r1c2 \ r2c1, r2c2] etc. Subscripted items are superseded by @ — eg for the 10th position in a vector X we would normally subscript X with 10. We will instead write X@10.

Introduction

Scientific method is difficult for most to comprehend. It is counterintuitive. It can lead to conclusions that do not reflect personal beliefs. It takes a foundation in the method to understand this basic fundamental concept: ***it is ok to be wrong***. This should be something that is taught in school. If we are afraid of getting it wrong, we will never propose anything new. The history of scientific discovery is therefore by its' very nature surrounded in serendipity.

Things that people discover by accident can be just as important as (or more important than) whatever it is they originally set out to do. Their original ideas might have been incorrect or inconclusive, but the things they discovered on the journey built the framework for those who follow.

According to the great modern scientific philosopher Karl Popper, testing a hypothesis for an incorrect outcome is the only reliable way to add weight to the argument that it is correct. If rigorous and repeated tests cannot show that a hypothesis is incorrect, then with each test the hypothesis assumes a higher likelihood of being correct. This concept is called Falsifiability. This article aims to falsify the statistical analysis used thus far to verify the stock-to-flow model of Bitcoin value, as defined in Modelling Bitcoin's Value with Scarcity[14].

Defining The Problem

To falsify a hypothesis, first we must state what it is:

Null Hypotheses (H0): Stock to flow does not have a measurable influence on Bitcoin price

Alternative Hypotheses (H1): Stock to flow does have a measurable infuence on Bitcoin price

Readers of the first article in this series3 will note that we have swapped around the null and alternative hypothesis. Readers will also note we are looking specifically at price, not market cap.

In [14], PlanB chose to test H0 by fitting an Ordinary Least Squares (OLS) regression on the natural log of the market capitalisation of Bitcoin and the natural log of the stock-to-flow. There was no accompanying diagnostics nor any identified reasoning for the log transformation in both variables, other than the idea that a log-log model can be expressed as a power law. The model did not take into account the possibility of a spurious relationship due to non-stationarity.

In 3 we explored some alternative models, including ones that do account for the possibility of a spurious relationship. We tested carefully stock to flow and price with both DFGLS and KPSS tests to verify from both directions that both variables were in fact non-stationary. However, the stock to flow variable is not something uninfluenced by the halving events, where the "flow" is literally cut in half. This is more akin to a structural break, rather than a non-stationary increase. Thus we test each halving period's stock to flow for stationarity with the DFGLS and KPSS test, as well as the entirety of the variable with the Ziffer-Andrews test for stationarity (which was developed to deal with such structural breaks).

Ordinary Least Squares (OLS)

Ordinary least squares regression is a way to estimate a linear relationship between two or more variables.

First, let us define a linear model as some function of X that equals Y with some error.

$Y = \beta X + \varepsilon$

where Y is the dependent variable, X is the independent variable, ε *is the error term and* β *is the multiplier of X*. The goal of OLS is to estimate β such that ε is minimised.

In order for [β] to be a reliable estimate, some basic assumptions must be met:

1. There is a linear relationship between the dependent and independent variables
2. The errors are homoscedastic (that is — they have a constant variance)
3. The error is normally distributed with a mean of zero
4. There is no autocorrelation in the error (that is — the errors aren't correlated with the lag of the errors)

In the first article of this series 3 we tested the first three of these assumptions. We will now test the fourth — that is how bad is the serial correlation in the residuals (and can we fix it?)

Serial Correlation in the Residuals

We begin by looking at a scatter plot matrix of the lags of the residuals. Serial correlation will show up here as essentially a straight line from the lower left corner of each individual graph to the upper right corner.

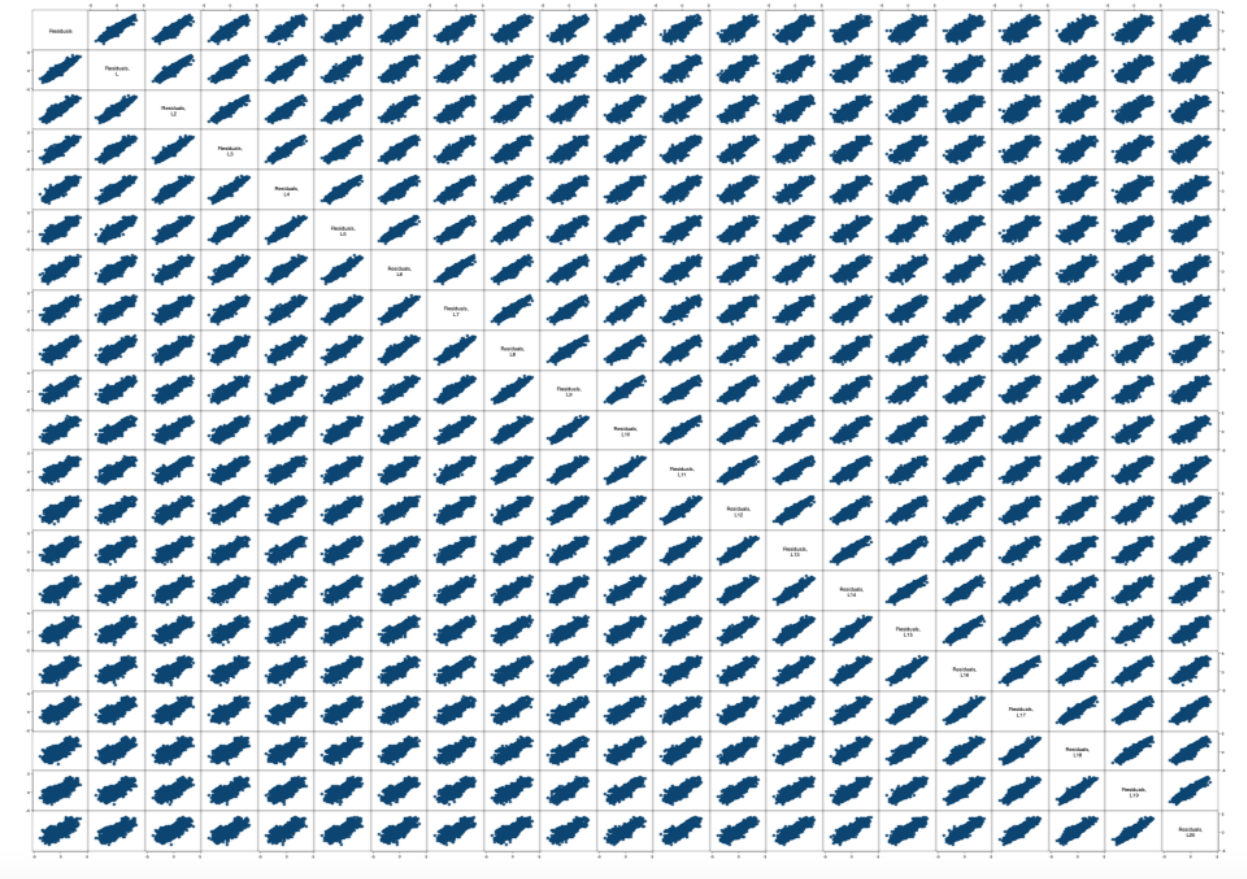


Figure 1 — Scatter plot matrix of Residuals v Lags of Residuals — High correlation shown all the way back to 20 lags

The visual evidence in figure 1 is quite damning. There is serial correlation heavily present. We can confirm this with the Breusch-Godfrey test. The null of the test is no autocorrelation present.

```
. estat bgodfrey, lags(1/10)

Breusch-Godfrey LM test for autocorrelation
```

lags(p)	chi2	df	Prob > chi2
1	3029.750	1	0.0000
2	3091.052	2	0.0000
3	3105.196	3	0.0000
4	3114.592	4	0.0000
5	3115.648	5	0.0000
6	3120.179	6	0.0000
7	3123.664	7	0.0000
8	3126.150	8	0.0000
9	3128.412	9	0.0000
10	3128.697	10	0.0000

H0: no serial correlation

Figure 2 — Breush-Godfrey test for autocorrelation — can reject the null with a high degree of confidence.

We can reject the null in Figure 2 for all lags in the test. This confirms our visual inspection results of autocorrelation in the residuals.

Prais-Winsten regression

Prais-Winsten regression assumes the residuals follow an AR(1) process and accounts for it via the “rho”. Below, we can see the original OLS in figure 3 and the Prais regression in figure 4. In figure 4, we also see the values of the Durbin-Watson statistic — first for the unchanged OLS, and then after accounting for serial correlation.

Source	SS	df	MS	Number of obs	=	3,537
				F(1, 3535)	=	30592.38
Model	31029.9959	1	31029.9959	Prob > F	=	0.0000
Residual	3585.56707	3,535	1.01430469	R-squared	=	0.8964
				Adj R-squared	=	0.8964
Total	34615.5629	3,536	9.78946916	Root MSE	=	1.0071

lnprice	Coef.	Std. Err.	t	P>|t|	[95% Conf.	Interval]
lnsf	3.115083	.01781	174.91	0.000	3.080164	3.150002
_cons	-1.614766	.0437264	-36.93	0.000	-1.700497	-1.529034

Figure 3 — Original OLS regression results

```
Prais-Winsten AR(1) regression -- iterated estimates

      Source |       SS           df       MS      Number of obs   =     3,537
-------------+----------------------------------   F(1, 3535)      =      0.00
       Model |           0          1           0   Prob > F        =    1.0000
    Residual |  10.8222786      3,535  .003061465   R-squared       =         .
-------------+----------------------------------   Adj R-squared   =         .
       Total |  10.6838894      3,536  .003021462   Root MSE        =    .05533

------------------------------------------------------------------------------
     lnprice |      Coef.   Std. Err.      t    P>|t|     [95% Conf. Interval]
-------------+----------------------------------------------------------------
        lnsf |   .0141339   .0074991     1.88   0.060    -.000569    .0288369
       _cons |   4.617012   .7074442     6.53   0.000     3.229972    6.004052
-------------+----------------------------------------------------------------
         rho |    .998937
------------------------------------------------------------------------------
Durbin-Watson statistic (original)    0.149173
Durbin-Watson statistic (transformed) 1.920013
```

Figure 4 — Prais-Winsten regression results.

Durbin-Watson is for this case interpreted as the closer to 2, the less likely there is to be serial correlation in the residuals.

As we can see, the Prais-Wnisten regression accounts for the serial correlation, however the influence of stock to flow appears greatly diminished, and in fact in this instance, **we cannot reject the null hypothesis (that stock to flow does not have an influence on price).**

Stationarity

In 1, we used the Johansen test for cointegration. One of the key assumptions in that test (and the simpler Engle-Granger test) is that both variables are non-stationary.

We tested for stationarity in 3 using the DFGLS test and the KPSS test and concluded that both variables were non-stationary. However, conceptually it can be seen that the halving events are more like structural breaks in the stock to flow variable. Thus here we test for stationarity using those tests within the halving epochs.

DF-GLS for **lnsf** Number of obs = **1395**
Maxlag = **23** chosen by Schwert criterion

[lags]	DF-GLS tau Test Statistic	1% Critical Value	5% Critical Value	10% Critical Value
23	**-0.649**	**-3.480**	**-2.829**	**-2.543**
22	**-0.636**	**-3.480**	**-2.830**	**-2.544**
21	**-0.648**	**-3.480**	**-2.831**	**-2.545**
20	**-0.618**	**-3.480**	**-2.832**	**-2.546**
19	**-0.598**	**-3.480**	**-2.833**	**-2.547**
18	**-0.613**	**-3.480**	**-2.834**	**-2.548**
17	**-0.660**	**-3.480**	**-2.836**	**-2.549**
16	**-0.694**	**-3.480**	**-2.837**	**-2.550**
15	**-0.674**	**-3.480**	**-2.838**	**-2.551**
14	**-0.709**	**-3.480**	**-2.839**	**-2.552**
13	**-0.762**	**-3.480**	**-2.840**	**-2.553**
12	**-0.758**	**-3.480**	**-2.841**	**-2.554**
11	**-0.796**	**-3.480**	**-2.842**	**-2.555**
10	**-0.824**	**-3.480**	**-2.843**	**-2.556**
9	**-0.868**	**-3.480**	**-2.844**	**-2.557**
8	**-0.909**	**-3.480**	**-2.845**	**-2.558**
7	**-0.900**	**-3.480**	**-2.846**	**-2.558**
6	**-0.977**	**-3.480**	**-2.847**	**-2.559**
5	**-1.051**	**-3.480**	**-2.848**	**-2.560**
4	**-1.100**	**-3.480**	**-2.849**	**-2.561**
3	**-1.132**	**-3.480**	**-2.850**	**-2.562**
2	**-1.208**	**-3.480**	**-2.851**	**-2.563**
1	**-1.456**	**-3.480**	**-2.852**	**-2.564**

Opt Lag (Ng-Perron seq t) = **18** with RMSE **.2011813**
Min SC = **-3.115792** at lag **7** with RMSE **.2062518**
Min MAIC = **-3.18074** at lag **18** with RMSE **.2011813**

Figure 5 — first halving epoch

We can conclude for the first epoch, that there is insufficient evidence to reject that stock to flow is non-stationary.

DF-GLS for **lnsf** Number of obs = **1296**
Maxlag = **22** chosen by Schwert criterion

[lags]	DF-GLS tau Test Statistic	1% Critical Value	5% Critical Value	10% Critical Value
22	**-4.643**	**-3.480**	**-2.829**	**-2.544**
21	**-4.798**	**-3.480**	**-2.830**	**-2.545**
20	**-5.073**	**-3.480**	**-2.832**	**-2.546**
19	**-5.156**	**-3.480**	**-2.833**	**-2.547**
18	**-5.501**	**-3.480**	**-2.834**	**-2.548**
17	**-5.832**	**-3.480**	**-2.835**	**-2.549**
16	**-6.097**	**-3.480**	**-2.836**	**-2.550**
15	**-6.083**	**-3.480**	**-2.838**	**-2.551**
14	**-6.115**	**-3.480**	**-2.839**	**-2.552**
13	**-5.847**	**-3.480**	**-2.840**	**-2.553**
12	**-5.641**	**-3.480**	**-2.841**	**-2.554**
11	**-5.546**	**-3.480**	**-2.842**	**-2.555**
10	**-5.911**	**-3.480**	**-2.843**	**-2.556**
9	**-6.390**	**-3.480**	**-2.844**	**-2.557**
8	**-6.928**	**-3.480**	**-2.845**	**-2.558**
7	**-7.511**	**-3.480**	**-2.846**	**-2.559**
6	**-8.142**	**-3.480**	**-2.848**	**-2.560**
5	**-9.119**	**-3.480**	**-2.849**	**-2.561**
4	**-9.757**	**-3.480**	**-2.850**	**-2.562**
3	**-10.479**	**-3.480**	**-2.851**	**-2.563**
2	**-12.124**	**-3.480**	**-2.852**	**-2.564**
1	**-14.158**	**-3.480**	**-2.853**	**-2.565**

Opt Lag (Ng-Perron seq t) = **21** with RMSE **.0917698**
Min SC = **-4.680195** at lag **11** with RMSE **.0931748**
Min MAIC = **-4.658865** at lag **22** with RMSE **.0916823**

Figure 6 — second halving epoch

For the second epoch, the evidence is more clear — the stock to flow variable is definitely stationary for the second epoch.

DF-GLS for **lnsf** Number of obs = **1332**
Maxlag = **23** chosen by Schwert criterion

[lags]	DF-GLS tau Test Statistic	1% Critical Value	5% Critical Value	10% Critical Value
23	**-6.363**	**-3.480**	**-2.828**	**-2.543**
22	**-6.777**	**-3.480**	**-2.830**	**-2.544**
21	**-7.104**	**-3.480**	**-2.831**	**-2.545**
20	**-7.320**	**-3.480**	**-2.832**	**-2.546**
19	**-7.425**	**-3.480**	**-2.833**	**-2.547**
18	**-7.026**	**-3.480**	**-2.834**	**-2.548**
17	**-6.971**	**-3.480**	**-2.835**	**-2.549**
16	**-6.658**	**-3.480**	**-2.836**	**-2.550**
15	**-6.447**	**-3.480**	**-2.838**	**-2.551**
14	**-6.802**	**-3.480**	**-2.839**	**-2.552**
13	**-6.966**	**-3.480**	**-2.840**	**-2.553**
12	**-7.191**	**-3.480**	**-2.841**	**-2.554**
11	**-7.439**	**-3.480**	**-2.842**	**-2.555**
10	**-7.806**	**-3.480**	**-2.843**	**-2.556**
9	**-7.846**	**-3.480**	**-2.844**	**-2.557**
8	**-8.014**	**-3.480**	**-2.845**	**-2.558**
7	**-8.448**	**-3.480**	**-2.846**	**-2.559**
6	**-9.099**	**-3.480**	**-2.847**	**-2.560**
5	**-9.566**	**-3.480**	**-2.848**	**-2.561**
4	**-10.896**	**-3.480**	**-2.849**	**-2.562**
3	**-11.653**	**-3.480**	**-2.850**	**-2.562**
2	**-14.415**	**-3.480**	**-2.851**	**-2.563**
1	**-17.459**	**-3.480**	**-2.852**	**-2.564**

Opt Lag (Ng-Perron seq t) = **19** with RMSE **.0991603**
Min SC = **-4.576626** at lag **3** with RMSE **.1003476**
Min MAIC = **-4.318251** at lag **15** with RMSE **.0997666**

Figure 7 — third halving epoch

In the third epoch, the evidence is overwhelming that stock to flow is stationary. There appears to be a trend toward stationarity through the epochs.

The Zivot-Andrews test for unit root allows for structural breaks in the series, which conceptually aligns with how the halvings impact the flow (and consequently the stock to flow ratio).

Zivot-Andrews unit root test for lnsf

Allowing for break in intercept

Lag selection via TTest: lags of D.lnsf included = 7

Minimum t-statistic -10.081 at 27may2011 (obs 875)

Critical values: 1%: -5.34 5%: -4.80 10%: -4.58

Clearly the Zivot-Andrews test works well here and agrees with the broken down DFGLS tests.

Log(Stock to Flow) is stationary. I(0). This would be fantastic news if Log(price) was also stationary (it would mean the original OLS PlanB did was valid), however it is non-stationary — the Zivot-Andrews test cannot the null.

Zivot-Andrews unit root test for lnprice

Allowing for break in intercept

Lag selection via TTest: lags of D.lnprice included = 7

Minimum t-statistic -3.644 at 16jan2013 (obs 1475)

Critical values: 1%: -5.34 5%: -4.80 10%: -4.58

In 3, we naively assumed stock to flow was integrated order (1) and price was integrated order (1). However, these test show that stock to flow is integrated order (0) and price is integrated order (1).

The Johansen test was used to test for cointegration in 3 — the problem is, we cannot mix orders of integration in this test. We cannot mix them in the simpler Engle-Granger test, either. There is only one possible test that the author is aware of that can deal with mixed order integration — the ARDL bounds test.

Auto Regressive Distributed Lag (ARDL) Model

Autoregressive distributed lag (ARDL) models regress the dependent variable on its lags and on the lags of one or more additional regressors.

ARDL models can, among other things, be used for the estimation and testing of level relationships. Key contributions in this area are [12] and [13]. For a succinct exposition of ARDL models in the context of cointegration, see [5 & 6].

An important feature of the ARDL model is it allows us to investigate relationships between mixed orders of integration.

```
. ardl lnprice lnsf, ec

ARDL(1,0) regression

Sample: 22jul2010 - 26mar2020                   Number of obs     =      3,536
                                                R-squared         =     0.0036
                                                Adj R-squared     =     0.0030
Log likelihood =  5246.9526                     Root MSE          =     0.0549
```

D.lnprice	Coef.	Std. Err.	t	P>|t|	[95% Conf.	Interval]
ADJ						
lnprice L1.	-.0024536	.0009161	-2.68	0.007	-.0042498	-.0006574
LR						
lnsf	2.179856	.5281401	4.13	0.000	1.144365	3.215346
SR						
_cons	.0044454	.0028119	1.58	0.114	-.0010677	.0099585

Figure 8 — ARDL model on daily data. We can see stock to flow has a significant long run influence on price.

```
. estat ectest

Pesaran, Shin, and Smith (2001) bounds test

H0: no level relationship                                   F =     6.360
Case 3                                                      t =    -2.678

Finite sample (1 variables, 3536 observations, 0 short-run coefficients)

Kripfganz and Schneider (2018) critical values and approximate p-values

   |  10%              |  5%               |  1%               |  p-value
   |     I(0)     I(1) |     I(0)     I(1) |     I(0)     I(1) |     I(0)     I(1)
---+-------------------+-------------------+-------------------+-------------------
 F |    4.053    4.804 |    4.935    5.761 |    6.883    7.859 |    0.016    0.032
 t |   -2.569   -2.914 |   -2.865   -3.225 |   -3.435   -3.823 |    0.078    0.158

do not reject H0 if
    both F and t are closer to zero than critical values for I(0) variables
      (if p-values > desired level for I(0) variables)
reject H0 if
    both F and t are more extreme than critical values for I(1) variables
      (if p-values < desired level for I(1) variables)
```

Figure 9 — Bounds test for a level relationship. We can reject the null hypothesis of no level relationship easily at the 10% critical level, further providing evidence to the s2f claim (NB we are looking at the I(0) variable s2f).

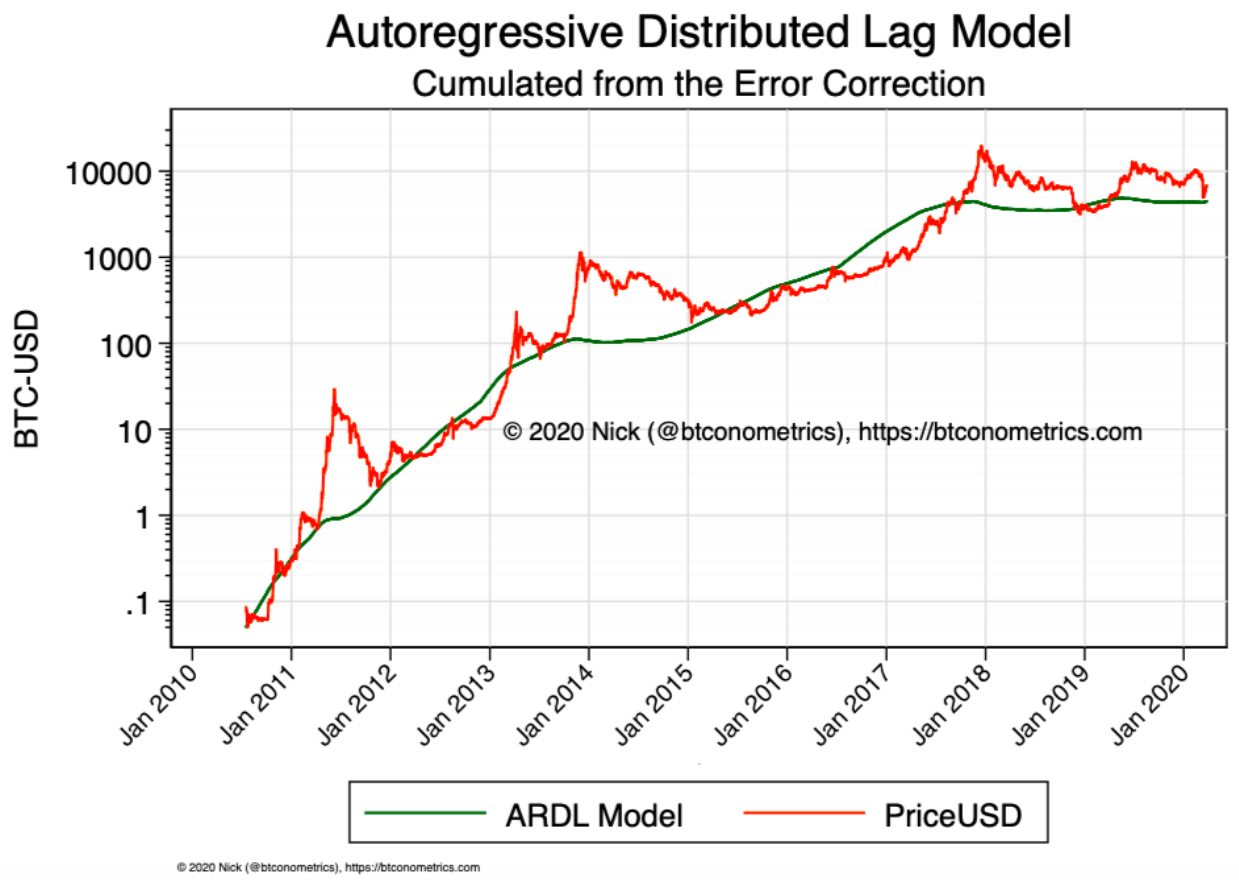


Figure 10 — Showing the long-run (LR) influence of stock to flow on price

Discussion

The bounds test for a level relationship in the ARDL model provides very robust evidence to **reject** the null hypothesis and conclude that **stock to flow does have a significant influence on the US Dollar price of Bitcoin.**

Further research is required as the coefficient for the long run parameter is significantly lower than the OLS parameter. Future research should focus on improving the ARDL specification, including adjusting for confounding or potentially effect mediating variables (such as the difficulty adjustment).

Follow me on twitter: @btconometrics or visit my website: https://btconometrics.com for further information.

Citations and Further Reading

1. Popper, Karl (1959). The Logic of Scientific Discovery (2002 pbk; 2005 ebook ed.). Routledge. ISBN 978–0–415–27844–7
2. Murray, M. (1994). A Drunk and Her Dog: An Illustration of Cointegration and Error Correction. The American Statistician,48(1), 37–39. doi:10.2307/2685084

3. Nick. (2019), Falsifying Stock-to-Flow As a Model of Bitcoin Value — The Drunken Value of Bitcoin, btconometrics.com — https://medium.com/swlh/falsifying-stock-to-flow-as-a-model-of-bitcoin-value-b2d9e61f68af
4. Dickey, D. A. and W. A. Fuller (1979). Distribution of the estimators for autoregressive time series with a unit root. Journal of the American Statistical Association, 74 (366), 427–431.
5. Hassler, U. and J. Wolters (2006): Autoregressive Distributed Lag Models and Cointegration. Allgemeines Statistisches Archiv, 90, 59–74.
6. Hassler, U. and J. Wolters (2005): Autoregressive Distributed Lag Models and Cointegration. Freie Universitaet Berlin, Working Paper №2005/22.
7. Kripfganz, S. and D. Schneider (2018): Response Surface Regressions for Critical Value Bounds and Approximate p-values in Equilibrium Correction Models. Manuscript, University of Exeter and Max Planck Institute for Demographic Research. Available at www.kripfganz.de/research/Kripfganz_Schneider_ec.html.
8. Luetkepohl, H. (2005): New Introduction to Multiple Time Series Analysis. Berlin, Heidelberg: Springer Verlag.
9. MacKinnon, J. G. (1991). Critical values for cointegration tests. In: R. F. Engle and C. W. J. Granger (Eds.): Long-Run Economic Relationships: Readings in Cointegration, Chapter 13, pp. 267–276. Oxford, UK: Oxford University Press.
10. MacKinnon, J. G. (1996). Numerical distribution functions for unit root and cointegration tests. Journal of Applied Econometrics, 11 (6), 601–618.
11. Narayan, P.K. (2005): The Saving and Investment Nexus for China: Evidence from Cointegration Tests. Applied Economics, 37 (17), 1979–1990.
12. Pesaran, M.H. and Y. Shin (1999): An Autoregressive Distributed Lag Modelling Approach to Cointegration Analysis. In: Strom, S. (Ed.): Econometrics and Economic Theory in the 20th Century: The Ragnar Frisch Centennial Symposium. Cambridge, UK: Cambridge University Press.
13. Pesaran, M.H., Shin, Y. and R.J. Smith (2001): Bounds Testing Approaches to the Analysis of Level Relationships. Journal of Applied Econometrics, 16 (3), 289–326.
14. PlanB. (2019) Modelling Bitcoins Value with Scarcity. https://medium.com/@100trillionUSD/modeling-bitcoins-value-with-scarcity-91fa0fc03e25

The Number Zero and Bitcoin

By Robert Breedlove

Posted March 28, 2020

Satoshi gave the world Bitcoin, a true “something for nothing.” His discovery of absolute scarcity for money is an unstoppable idea that is changing the world tremendously, just like its digital ancestor: the number zero.

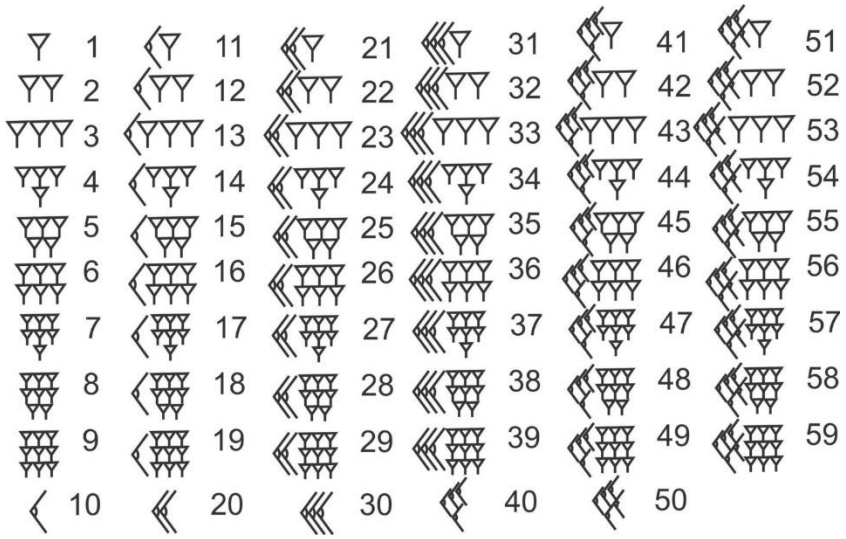
Zero is Special

"In the history of culture the discovery of zero will always stand out as one of the greatest single achievements of the human race." — Tobias Danzig, Number: The Language of Science

Many believe that Bitcoin is "just one of thousands of cryptoassets"—this is true in the same way that the number zero is just one of an infinite series of numbers. In reality, Bitcoin is special, and so is zero: each is an invention which led to a discovery that fundamentally reshaped its overarching system—for Bitcoin, that system is money, and for zero, it is mathematics. Since money and math are mankind's two universal languages, both Bitcoin and zero are critical constructs for civilization.

For most of history, mankind had no concept of zero: an understanding of it is not innate to us—a symbol for it had to be invented and continuously taught to successive generations. Zero is an abstract conception and is not discernible in the physical world—no one goes shopping for zero apples. To better understand this, we will walk down a winding path covering more than 4,000 years of human history that led to zero becoming part of the empirical bedrock of modernity.

Numerals, which are symbols for numbers, are the greatest abstractions ever invented by mankind: virtually everything we interact with is best grasped in numerical, quantifiable, or digital form. Math, the language of numerals, originally developed from a practical desire to count things—whether it was the amount of fish in the daily catch or the days since the last full moon. Many ancient civilizations developed rudimentary numeral systems: in 2000 BCE, the Babylonians, who failed to conceptualize zero, used two symbols in different arrangements to create unique numerals between 1 and 60:

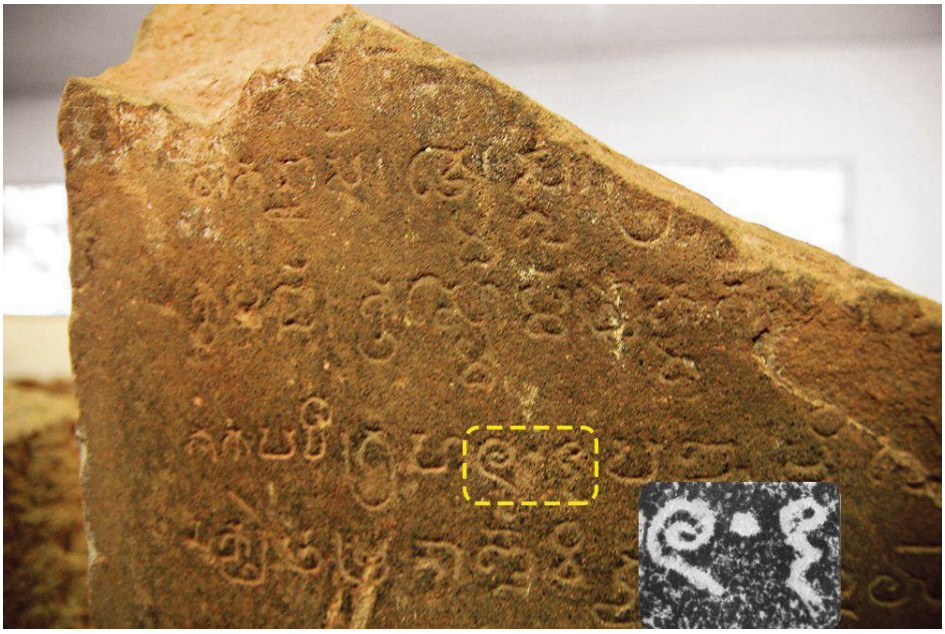


Babylonian cuneiform was a relatively inefficient numeral system — notice how many more written strokes are necessary for each number symbol — and calculation using it was even more cumbersome.

Vestiges of the base-60 Babylonian cuneiform system still exist today: there are 60 seconds in a minute, 60 minutes in an hour, and 6 sets of 60 degrees in a circle. But

this ancient system lacked a zero, which severely limited its usefulness. Ancient Greeks and Mayans developed their own numeral systems, each of which contained rough conceptions of zero. However, the first explicit and arithmetic use of zero came from ancient Indian and Cambodian cultures. They created a system with nine number symbols and a small dot used to mark the absence of a number—the original zero. This numeral system would eventually evolve into the one we use today:

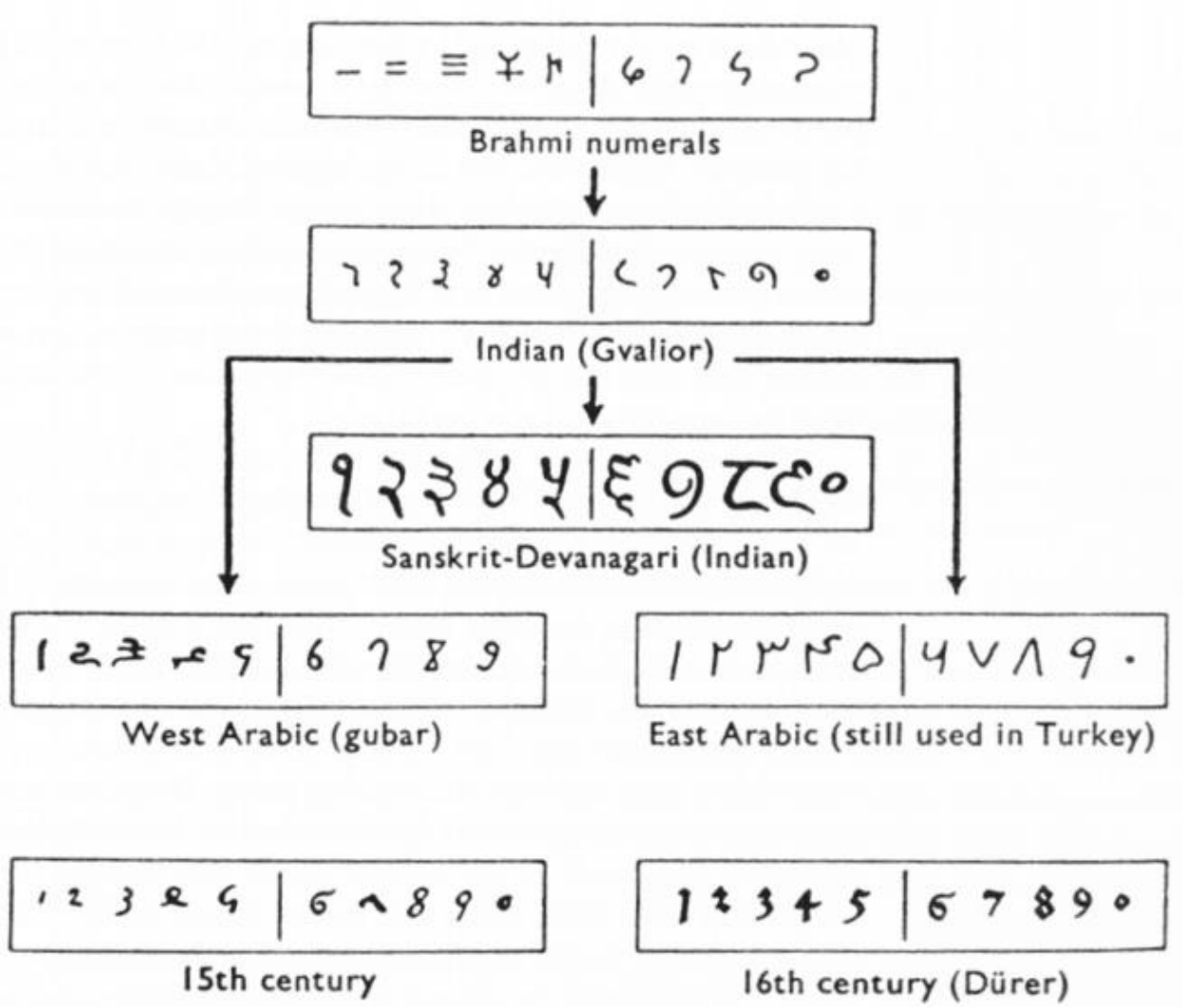
The first known written zero: from the Bakhshali manuscript which contains pages dating back to the 3rd and 4th centuries AD.



Inscription K-127 bears the earliest zero ever discovered—dated from the 7th century, it was discovered in the 19th century in Cambodia.

In the 7th century, the Indian mathematician Brahmagupta developed terms for zero in addition, subtraction, multiplication, and division (although he struggled a bit with the latter, as would thinkers for centuries to come). As the discipline of mathematics matured in India, it was passed through trade networks eastward into China and westward into Islamic and Arabic cultures. It was this western advance of zero which ultimately led to the inception of

the Hindu-Arabic numeral system—the most common means of symbolic number representation in the world today:



The Economization of Math

When zero reached Europe roughly 300 years later in the High Middle Ages, it was met with strong ideological resistance. Facing opposition from users of the well-established Roman numeral system, zero struggled to gain ground in Europe. People at the time were able to get by without zero, but (little did they know) performing computation without zero was horribly inefficient. An apt analogy to keep in mind arises here: both math and money are possible without zero and Bitcoin, respectively—however both are tremendously more wasteful systems without these core elements. Consider the difficulty of doing arithmetic in Roman numerals:

Using Roman numerals, the sum 1,223 + 1,104 becomes:

	MCCXXIII	+	MCIV	
=	MCCXXIII	+	MCIIII	
	M	CC	XX	III
+	M	C		IIII
=	MM	CCC	XX	IIIIII
=	MMCCCXXVII			= 2,327

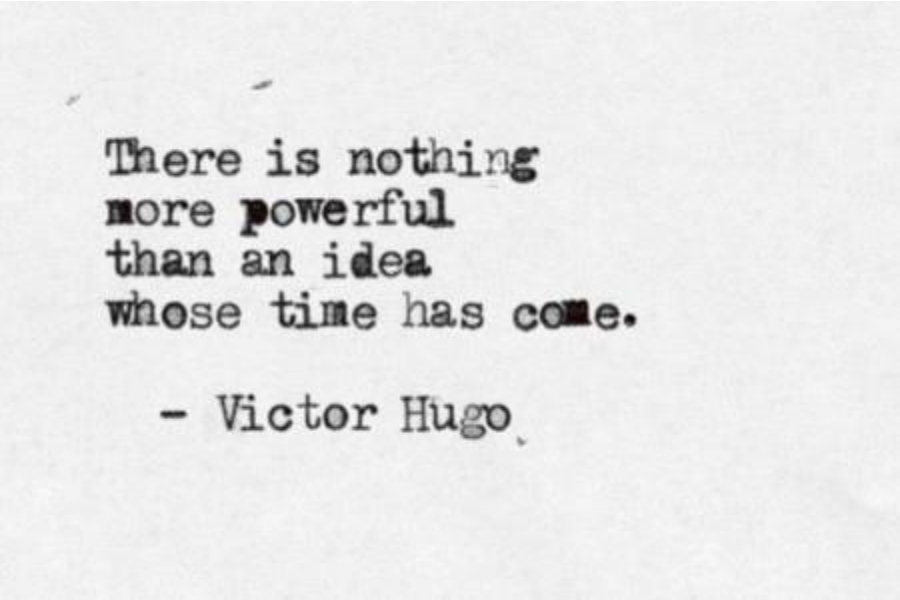
If you thought you were bad at arithmetic using numbers, just try doing it with letters.

Calculation performed using the Hindu-Arabic system is significantly more straightforward than with Roman numerals—and energy-efficient systems have a tendency to win out in the long run, as we saw when the steam engine outcompeted animal-sourced power or when capitalism prevailed over socialism (another important point to remember for Bitcoin later). This example just shows the pains of addition—multiplication and division were even more painstaking. As Amir D. Aczel described it in his book ***Finding Zero:***

"[The Hindu-Arabic numeral system] allowed an immense economy of notation so that the same digit, for example 4, can be used to convey itself or forty (40) when followed by a zero, or four hundred and four when written as 404, or four thousand when written as a 4 followed by three zeros (4,000). The power of the Hindu-Arabic numeral system is incomparable as it allows us to represent numbers efficiently and compactly, enabling us to perform complicated arithmetic calculations that could not have been easily done before."

Roman numeral inefficiency would not be tolerated for long in a world enriching itself through commerce. With trade networks proliferating and productivity escalating in tandem, growing prospects of wealth creation incentivized merchants to become increasingly competitive, pushing them to always search for an edge over others. Computation and record-keeping with a zero-based numeral system was qualitatively easier, quantitatively faster, and less prone to error. Despite Europe's resistance, this new numeral

system simply could not be ignored: like its distant progeny Bitcoin would later be, zero was an unstoppable idea whose time had come:



Functions of Zero

Zero's first function is as a placeholder in our numeric system: for instance, notice the "0" in the number "1,104" in the equation above, which indicates the absence of value in the tens place. Without zero acting as a symbol of absence at this order of magnitude in "1,104," the number could not be represented unambiguously (without zero, is it "1,104" or "114"?). Lacking zero detracted from a numeral system's capacity to maintain constancy of meaning as it scales. Inclusion of zero enables other digits to take on new meaning according to their position relative to it. In this way, zero lets us perform calculation with less effort—whether its pen strokes in a ledger, finger presses on a calculator, or mental gymnastics. Zero is a symbol for emptiness, which can be a highly useful quality—as Lao Tzu said:

"We shape clay into a pot, but it is the emptiness inside that holds whatever we want."

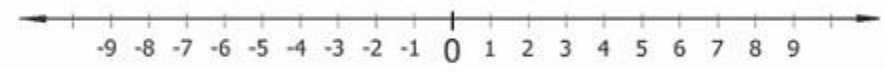
More philosophically, zero is emblematic of ***the void,*** as Aczel describes it:

"...the void is everywhere and it moves around; it can stand for one truth when you write a number a certain way — no tens, for example — and another kind of truth in another case, say when you have no thousands in a number!"

Drawing analogies to the functions of money: zero is the "store of value" on which higher order of magnitude numerals can scale; this is the reason we always prefer to see another zero at the end of our bank account or Bitcoin balance. In the same way a sound economic store of value leads to increased

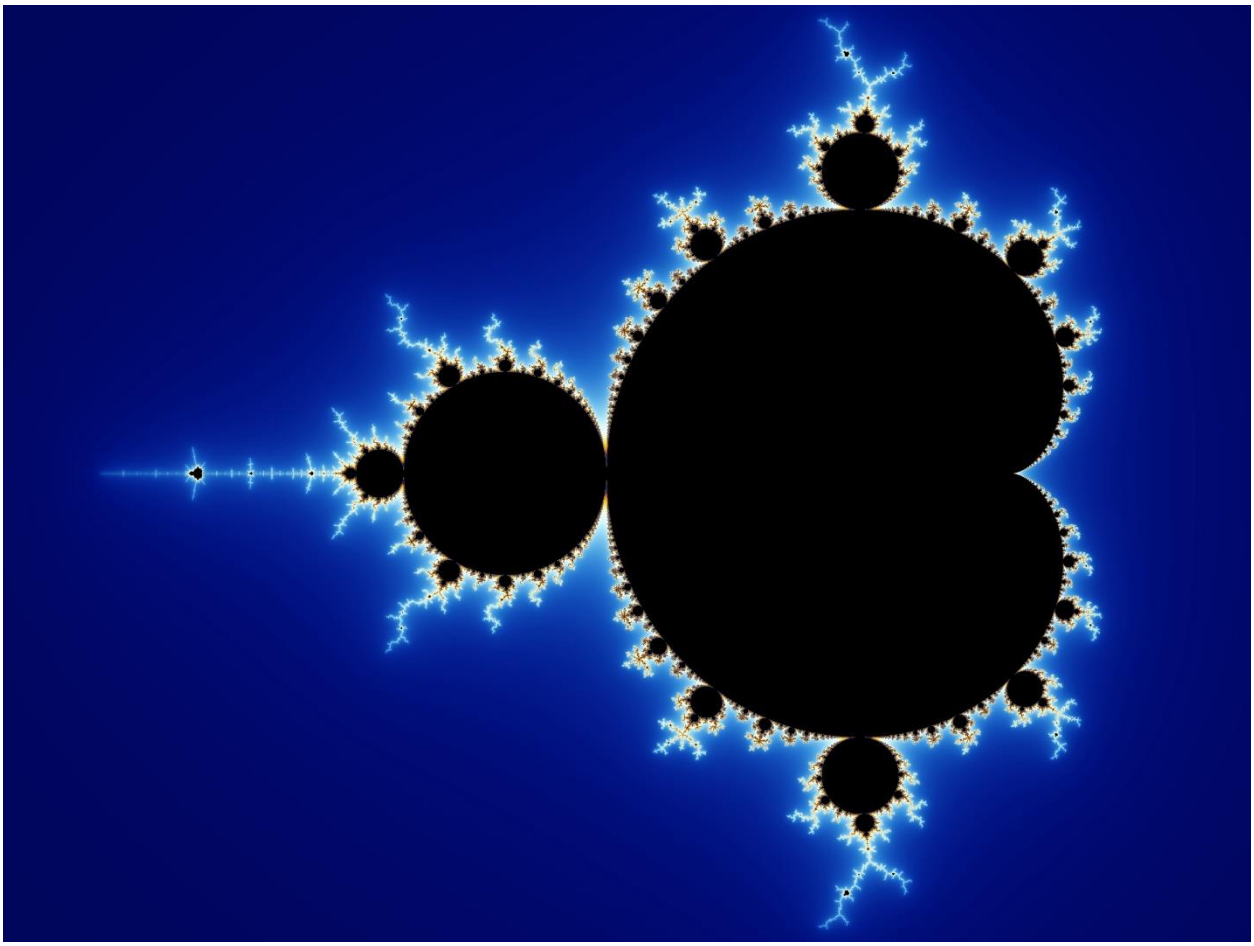
savings, which undergirds investment and productivity growth, so too does a sound mathematical placeholder of value give us a numeral system capable of containing more meaning in less space, and supporting calculations in less time: both of which also foster productivity growth. Just as money is the medium through which capital is continuously cycled into places of optimal economic employment, zero gives other digits the ability to cycle—to be used again and again with different meanings for different purposes.

Zero's second function is as a number in its own right: it is the midpoint between any positive number and its negative counterpart (like +2 and -2). Before the concept of zero, negative numbers were not used, as there was no conception of "nothing" as a number, much less "less than nothing." Brahmagupta inverted the positive number line to create negative numbers and placed zero at the center, thus rounding out the numeral system we use today. Although negative numbers were written about in earlier times, like the Han Dynasty in China (206 BCE to 220 BCE), their use wasn't formalized before Brahmagupta, since they required the concept of zero to be properly defined and aligned. In a visual sense, negative numbers are a reflection of positive numbers cast across zero:



Zero is the center of gravity for our entire numeral system, just as money is central to any economic system.

Interestingly, negative numbers were originally used to signify debts—well before the invention of double-entry accounting, which opted for debits and credits (partly to avoid the use of negative numbers). In this way, zero is the "medium of exchange" between the positive and negative domains of numbers—it is only possible to pass into, or out of, either territory by way of zero. By going below zero and conceptualizing negative numbers, many new and unusual (yet extremely useful) mathematical constructs come into being including imaginary numbers, complex numbers, fractals, and advanced astrophysical equations. In the same way the economic medium of exchange, ***money***, leads to the acceleration of trade and innovation, so too does the mathematical medium of exchange, ***zero***, lead to enhanced informational exchange, and its associated development of civilizational advances:



The Mandlebrot Set: one of the most famous examples of a fractal, a mind-bending mathematical structure formed with complex numbers that models the geometry of nature and its intrinsic complexity. One of the best known examples of mathematical beauty, this fractal exhibits infinite depth, breadth, and non-repeating self-similarity. Zero is a necessary prerequisite to such fractal modeling.

Zero's third function is as a facilitator for fractions or ratios. For instance, the ancient Egyptians, whose numeral system lacked a zero, had an extremely cumbersome way of handling fractions: instead of thinking of 3/4 as a ratio of three to four (as we do today), they saw it as the sum of 1/2 and 1/4. The vast majority of Egyptian fractions were written as a sum of numbers as 1/***n***, where ***n*** is the counting number—these were called unit fractions. Without zero, long chains of unit fractions were necessary to handle larger and more complicated ratios (many of us remember the pain of converting fractions from our school days). With zero, we can easily convert fractions to decimal form (like 1/2 to 0.5), which obsoletes the need for complicated conversions when dealing with fractions. This is the "unit of account" function of zero. Prices expressed in money are just exchange ratios converted into a money-denominated price decimal: instead of saying "this house costs eleven cars"

we say, “this house costs $440,000,” which is equal to the price of eleven $40,000 cars. Money gives us the ability to better handle exchange ratios in the same way zero gives us the ability to better handle numeric ratios.

Numbers are the ultimate level of objective abstraction: for example, the number 3 stands for the _idea _of “threeness” — a quality that can be ascribed to anything in the universe that comes in treble form. Equally, 9 stands for the quality of “nineness” shared by anything that is composed of nine parts. Numerals and math greatly enhanced interpersonal exchange of knowledge (which can be embodied in goods or services), as people can communicate about almost anything in the common language of numeracy. Money, then, is just the mathematized measure of capital available in the marketplace: it is the least common denominator among all economic goods and is necessarily the most liquid asset with the least mutable supply. It is used as a measuring system for the constantly shifting valuations of capital (this is why gold became money—it is the monetary metal with a supply that is most difficult to change). Ratios of money to capital (aka prices) are among the most important in the world, and ratios are a foundational element of being:

“In the beginning, there was the ratio, and the ratio was with God, and the ratio was God.” — John 1:1*

*(A more “rational” translation of Jesus’s beloved disciple John: the Greek word for ***ratio*** was λόγος (logos), which is also the term for ***word***.)

An ability to more efficiently handle ratios directly contributed to mankind’s later development of rationality, a logic-based way of thinking at the root of major social movements such as the Renaissance, the Reformation, and the Enlightenment. To truly grasp the strange logic of zero, we must start with its point of origin—the philosophy from which it was born.

Philosophy of Zero

“In the earliest age of the gods, existence was born from non-existence.” — The Rig Veda

Zero arose from the bizarre logic of the ancient East. Interestingly, the Buddha himself was a known mathematician — in early books about him, like the ***Lalita Vistara***, he is said to be excellent in numeracy (a skill he uses to woo a certain princess). In Buddhism, the logical character of the phenomenological world is more complex than true or false:

“Anything is either true,

Or not true,

Or both true and not true,

Or neither true nor not true.

This is the Lord Buddha's teaching."

This is the Tetralemma (or the four corners of the catuskoti): the key to understanding the seeming strangeness of this ancient Eastern logic is the concept of ***Shunya***, a Hindi word meaning zero: it is derived from the Buddhist philosophical concept of Śūnyatā (or Shunyata). The ultimate goal of meditation is the attainment of enlightenment, or an ideal state of nirvana, which is equivalent to emptying oneself entirely of thought, desire, and worldly attachment. Achievement of this absolute emptiness is the state of being in Shunyata: a philosophical concept closely related to ***the void***—as the Buddhist writer Thich Nhat Hanh describes it:

"The first door of liberation is emptiness, Shunyata

Emptiness always means empty of something

Emptiness is the Middle Way between existent and nonexistent

Reality goes beyond notions of being and nonbeing

True emptiness is called "wondrous being," because it goes beyond existence and nonexistence

The concentration on Emptiness is a way of staying in touch with life as it is, but it has to be practiced and not just talked about."

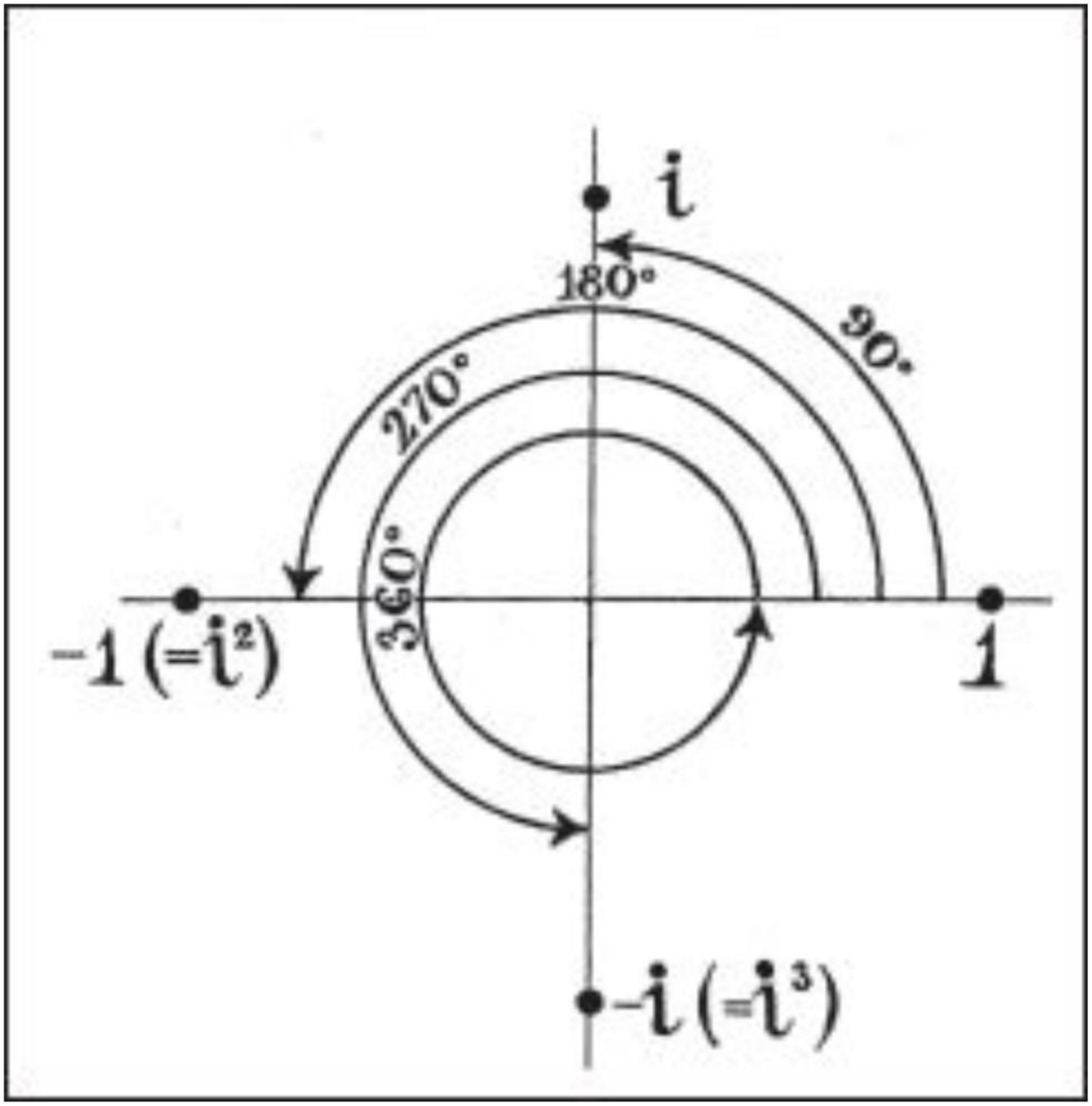
Or, as a Buddhist monk of ancient Wats temple in Southeast Asia described the meditative experience of the void:

"When we meditate, we count. We close our eyes and are aware only of where we are at in the moment, and nothing else. We count breathing in, 1; and we count breathing out, 2; and we go on this way. When we stop counting, that is the void, the number zero, the emptiness."

A direct experience of emptiness is achievable through meditation. In a true meditative state, the Shunyata and the number zero are one and the same. Emptiness is the conduit between existence and nonexistence, in the same way zero is the door from positive to negative numbers: each being a perfect reflection of the other. Zero arose in the ancient East as the epitome of this deeply philosophical and experiential concept of absolute emptiness. Empirically, today we now know that meditation benefits the brain in many ways. It seems too, that its contribution to the discovery of zero helped forge an idea that benefits mankind's collective intelligence — our global hive-mind.

Despite being discovered in a spiritual state, zero is a profoundly practical concept: perhaps it is best understood as a fusion of philosophy and

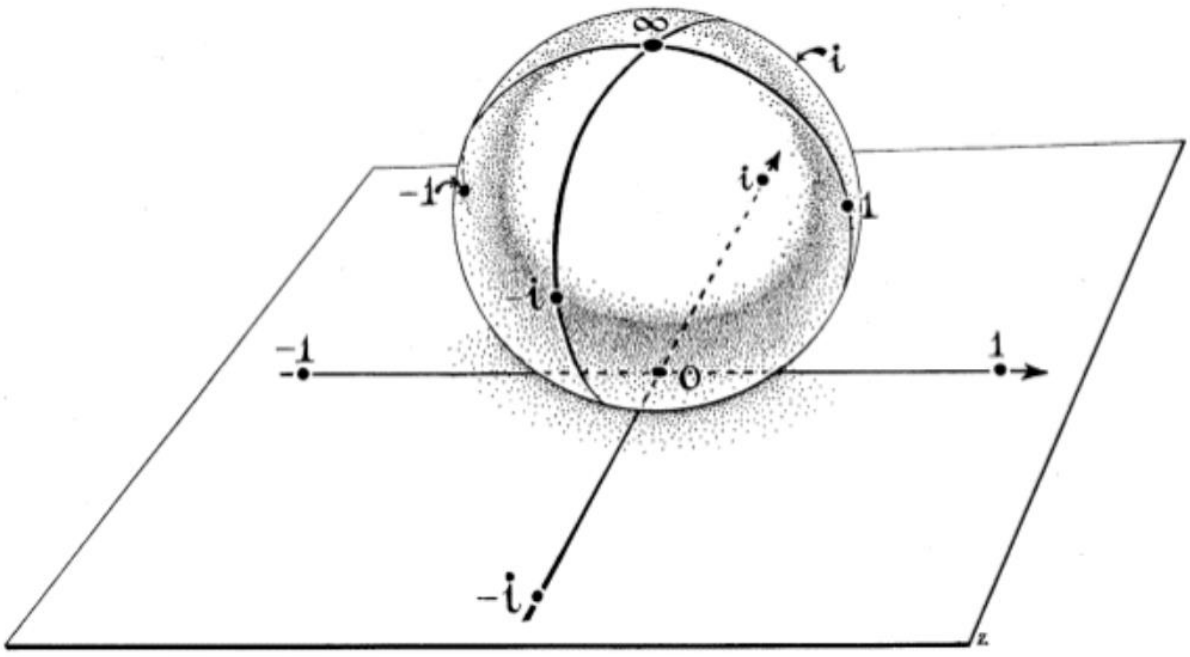
pragmatism. By traversing across zero into the territory of negative numbers, we encounter the imaginary numbers, which have a base unit of the square root of -1, denoted by the letter ***i. _The number _i _is paradoxical: consider the equations $x^2 + 1 = 0$ and $x^3 + 1 = 0$, the only possible answers are positive square root of -1 (_i***) and negative square root of -1 (-_i or i^3***), respectively. Visualizing these real and imaginary domains, we find a rotational axis centered on zero with orientations reminiscent of the tetralemma: one true (1), one not true (_i***), one both true and not true (-1 or i^2), and one neither true nor not true (-_i or i^3_):



Zero is the fulcrum between real and imaginary number planes.

Going through the gateway of zero into the realms of negative and imaginary numbers provides a more continuous form of logic when compared to the discrete either-or logic, commonly accredited to Aristotle and his followers. This framework is less "black and white" than the binary Aristotelean logic system, which was based on true or false, and provides many gradations of logicality; a more accurate map to the many "shades of grey" we find in nature. Continuous logic is insinuated throughout the world: for instance, someone may say "she wasn't unattractive," meaning that her appeal was ambivalent, somewhere between attractive and unattractive. This perspective is often more realistic than a binary assessment of attractive or not attractive.

Importantly, zero gave us the concept of infinity: which was notably absent from the minds of ancient Greek logicians. The rotations around zero through the real and imaginary number axes can be mathematically scaled up into a three-dimensional model called the ***Riemann Sphere***. In this structure, zero and infinity are geometric reflections of one another and can transpose themselves in a flash of mathematical permutation. Always at the opposite pole of this three-dimensional, mathematical interpretation of the tetralemma, we find zero's twin—infinity:

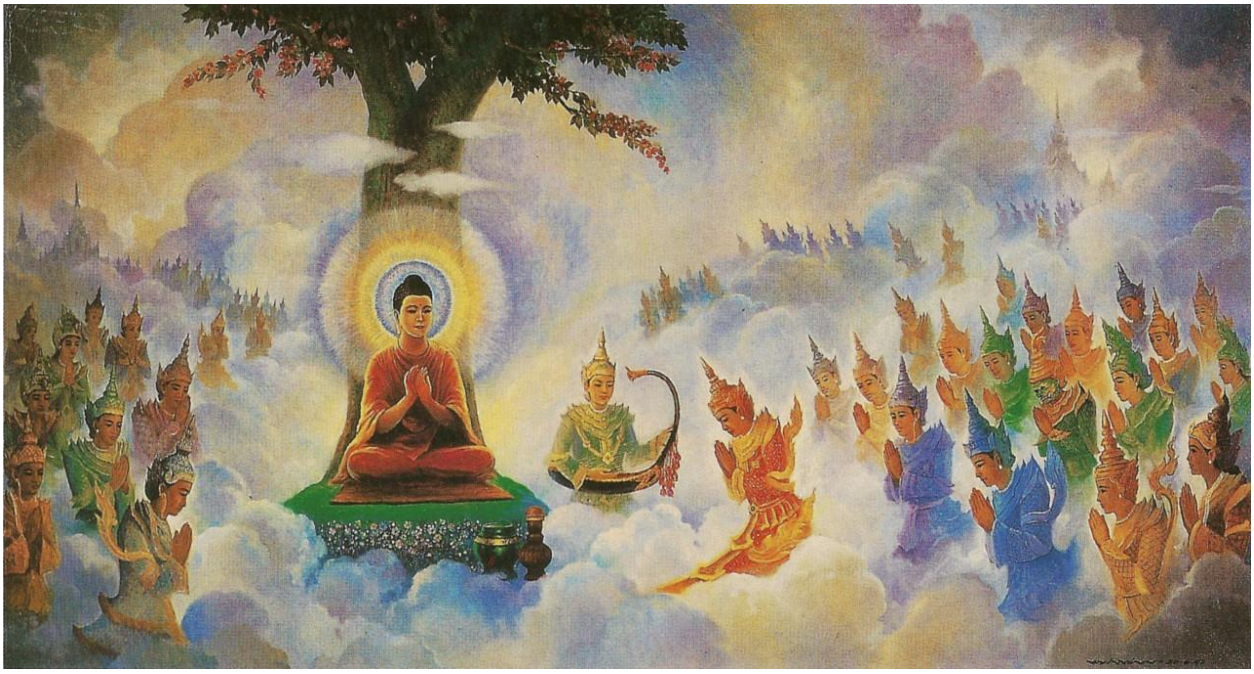


Scaling the real and imaginary number planes into the third dimension, we discover zero's twin: infinity.

The twin polarities of zero and infinity are akin to yin and yang — as Charles Seife, author of ***Zero: Biography of a Dangerous Idea,*** describes them:

"Zero and infinity always looked suspiciously alike. Multiply zero by anything and you get zero. Multiply infinity by anything and you get infinity. Dividing a number by zero yields infinity; dividing a number by infinity yields zero. Adding zero to a number leaves it unchanged. Adding a number to infinity leaves infinity unchanged."

In Eastern philosophy, the kinship of zero and infinity made sense: only in a state of absolute nothingness can possibility become infinite. Buddhist logic insists that everything is endlessly intertwined: a vast causal network in which all is inexorably interlinked, such that no single thing can truly be considered independent — as having its own isolated, non-interdependent essence. In this view, interrelation is the sole source of substantiation. Fundamental to their teachings, this truth is what Buddhists call ***dependent co-origination***, meaning that all things depend on one another. The only exception to this truth is ***nirvana***: liberation from the endless cycles of reincarnation. In Buddhism, the only pathway to nirvana is through pure emptiness:



Nirvana, the ultimate spiritual goal in Buddhism, is attained by entering the void in meditation—this is where zero was discovered.

Some ancient Buddhist texts state: "the truly absolute and the truly free must be nothingness." In this sense, the invention of zero was special; it can be considered the discovery of absolute nothingness, a latent quality of reality that was not previously presupposed in philosophy or systems of knowledge like mathematics. Its discovery would prove to be an emancipating force for mankind, in that zero is foundational to the mathematized, software-enabled reality of convenience we inhabit today.

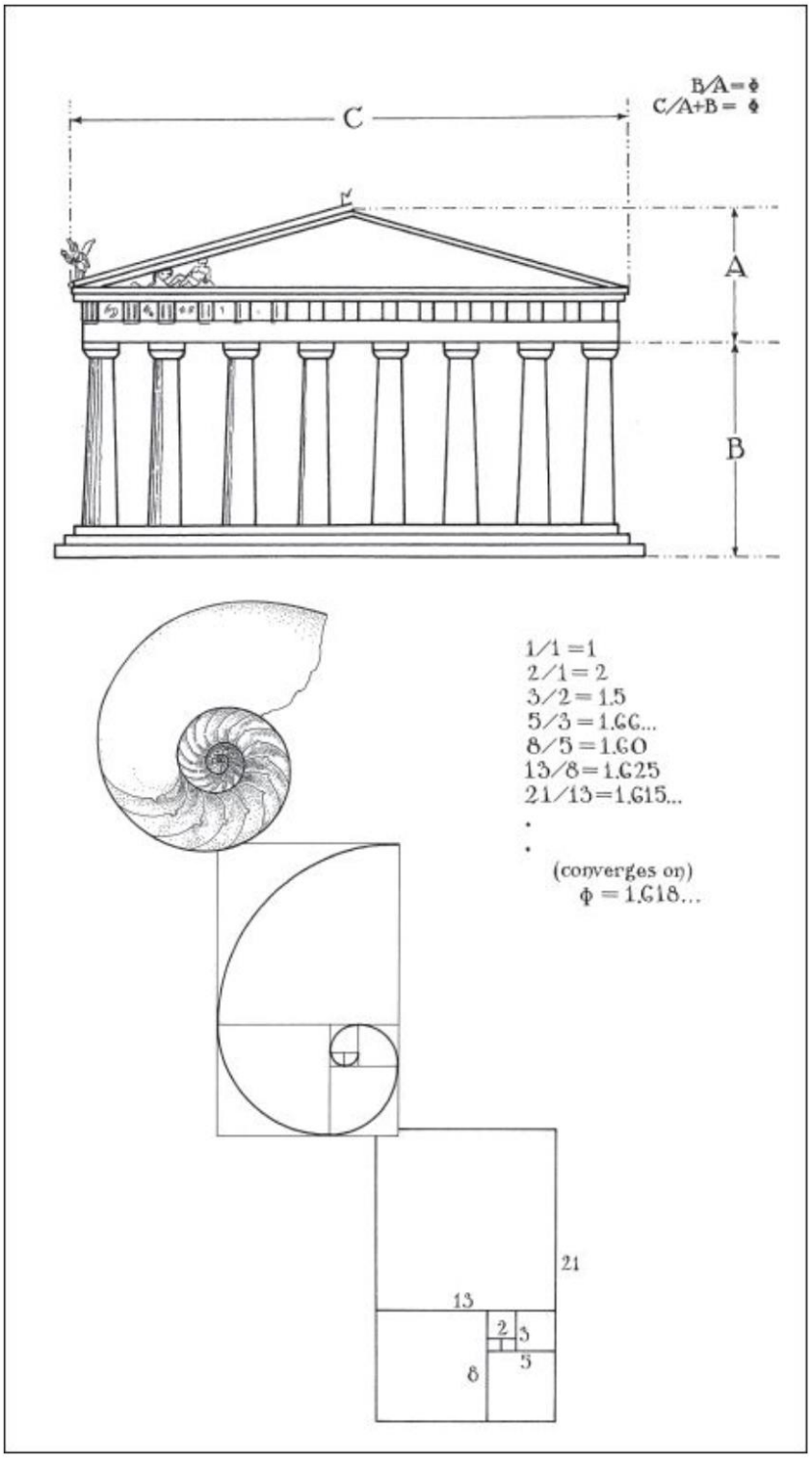
Zero was liberation discovered deep in meditation, a remnant of truth found in close proximity to nirvana — a place where one encounters universal, unbounded, and infinite awareness: God's kingdom within us. To buddhists, zero was a whisper from the ***universe***, from ***dharma,_from _God*** (words always fail us in the domain of divinity). Paradoxically, zero would ultimately shatter the institution which built its power structure by monopolizing access to God. In finding footing in the void, mankind uncovered the deepest, soundest substrate on which to build modern society: zero would prove to be a critical piece of infrastructure that led to the interconnection of the world via telecommunications, which ushered in the gold standard and the digital age (Bitcoin's two key inceptors) many years later.

Blazing a path forward: the twin conceptions of zero and infinity would ignite the Renaissance, the Reformation, and the Enlightenment — all movements that mitigated the power of The Catholic Church as the dominant institution in the world and paved the way for the industrialized nation-state.

Power of The Church Falls to Zero

The universe of the ancient Greeks was founded on the philosophical tenets of Pythagoras, Aristotle, and Ptolemy. Central to their conception of the cosmos was the precept that there is no void, no nothingness, no zero. Greeks, who had inherited their numbers from the geometry-loving Egyptians, made little distinction between shape and number. Even today, when we ***square*** a number (x^2), this is equivalent to converting a line into a square and calculating its area. Pythagoreans were mystified by this connection between shapes and numbers, which explains why they didn't conceive of zero as a number: after all, what shape could represent nothingness? Ancient Greeks believed numbers had to be visible to be real, whereas the ancient Indians perceived numbers as an intrinsic part of a latent, invisible reality separate from mankind's conception of them.

The symbol of the Pythagorean cult was the pentagram (a five-pointed star); this sacred shape contained within it the key to their view of the universe— the golden ratio. Considered to be the "most beautiful number," the golden ratio is achieved by dividing a line such that the ratio of the small part to the large part is the same as the ratio of the large part to the whole. Such proportionality was found to be not only aesthetically pleasing, but also naturally occurring in a variety of forms including nautilus shells, pineapples, and (centuries later) the double-helix of DNA. Beauty this objectively pure was considered to be a window into the transcendent; a soul-sustaining quality. The golden ratio became widely used in art, music, and architecture:



A simple sequence of calculations converges on the golden ratio, the "beautiful number" bountiful in nature. Beauty of this caliber heavily influenced many domains including architecture (as seen in the design of The Parthenon here).

The golden ratio was also found in musical harmonics: when plucking a string instrument from its specified segments, musicians could create the ***perfect fifth***, a dual resonance of notes said to be the most evocative musical relationship. Discordant tritones, on the other hand, were derided as the "devil in music." Such harmony of music was considered to be one and the same with that of mathematics and the universe—in the Pythagorean finite view of the cosmos (later called the Aristotelean ***celestial spheres*** model_), _movements of planets and other heavenly bodies generated a symphonic "harmony of the spheres"—a celestial music that suffused the cosmic depths. From the perspective of Pythagoreans, "all was number," meaning ratios ruled the universe. The golden ratio's seemingly supernatural connection to aesthetics, life, and the universe became a central tenet of Western Civilization and, later, The Catholic Church (aka The Church).

Zero posed a major threat to the conception of a finite universe. Dividing by zero is devastating to the framework of logic, and thus threatened the perfect order and integrity of a Pythagorean worldview. This was a serious problem for The Church which, after the fall of the Roman Empire, appeared as the dominant institution in Europe. To substantiate its dominion in the world, The Church proffered itself as the gatekeeper to heaven. Anyone who crossed The Church in any way could find themselves eternally barred from the holy gates. The Church's claim to absolute sovereignty was critically dependent on the Pythagorean model, as the dominant institution over Earth—which was in their view the center of the universe—necessarily held dominion in God's universe. Standing as a symbol for both the void and the infinite, zero was heretical to The Church. Centuries later, a similar dynamic would unfold in the discovery of absolute scarcity for money, which is dissident to the dominion of The Fed—the false church of modernity.

Ancient Greeks clung tightly to a worldview that did not tolerate zero or the infinite: rejection of these crucial concepts proved to be their biggest failure, as it prevented the discovery of calculus—the mathematical machinery on which much of the physical sciences and, thus, the modern world are constructed. Core to their (flawed) belief system was the concept of the "indivisible atom," the elementary particle which could not be subdivided ad infinitum. In their minds, there was no way beyond the micro barrier of the atomic surface. In the same vein, they considered the universe a "macrocosmic atom" that was strictly bound by an outermost sphere of stars winking down towards the cosmic core—Earth. As above, so below: with nothing conceived to be above this stellar sphere and nothing below the atomic surface, there was no infinity and no void:

A finite universe with Earth at the center was the central tenet of ancient Greek philosophy and, later, of The Catholic Church's institutional dominion over the world.

Aristotle (with later refinements by Ptolemy) would interpret this finite universe philosophically and, in doing so, form the ideological foundation for God's existence and The Church's power on Earth. In the Aristotelean conception of the universe, the force moving the stars, which drove the

motion of all elements below, was the prime mover: God. This cascade of cosmic force from on high downward into the movements of mankind was considered the officially accepted interpretation of divine will. As Christianity swept through the West, The Church relied upon the explanatory power of this Aristotelean philosophy as proof of God's existence in their proselytizing efforts. Objecting to the Aristotelean doctrine was soon considered an objection to the existence of God and the power of The Church.

Infinity was unavoidably actualized by the same Aristotelean logic which sought to deny it. By the 13th century, some bishops began calling assemblies to question the Aristotelean doctrines that went against the omnipotence of God: for example, the notion that "God can not move the heavens in a straight line, because that would leave behind a vacuum." If the heavens moved linearly, then what was left in their wake? Through what substance were they moving? This implied either the existence of the void (the vacuum), or that God was not truly omnipotent as he could not move the heavens. Suddenly, Aristotelean philosophy started to break under its own weight, thereby eroding the premise of The Church's power. Although The Church would cling to Aristotle's views for a few more centuries—it fought heresy by forbidding certain books and burning certain Protestants alive—zero marked the beginning of the end for this domineering and oppressive institution.

An infinite universe meant there were, at least, a vast multitude of planets, many of which likely had their own populations and churches. Earth was no longer the center of the universe, so why should The Church have universal dominion? In a grand ideological shift that foreshadowed the invention of Bitcoin centuries later, zero became the idea that broke The Church's grip on humanity, just as absolute scarcity of money is breaking The Fed's stranglehold on the world today. In an echo of history, us moderns can once again hear the discovery of nothing beginning to change everything.

Zero was the smooth stone slung into the face of Goliath, a death-stroke to the dominion of The Church; felled by an unstoppable idea, this oppressive institution's fall from grace would make way for the rise of the nation-state—the dominant institutional model in modernity.

Zero: An Ideological Juggernaut

Indoctrinated in The Church's dogma, Christianity initially refused to accept zero, as it was linked to a primal fear of the void. Zero's inexorable connection to nothingness and chaos made it a fearsome concept in the eyes of most Christians at the time. But zero's capacity to support honest weights and measures, a core Biblical concept, would prove more important than the countermeasures of The Church (and the invention of zero would later lead to the invention of the most infallible of weights and measures, the most honest

money in history—Bitcoin). In a world being built on trade, merchants needed zero for its superior arithmetic utility. As Pierre-Simon Laplace said:

"...[zero is] a profound and important idea which appears so simple to us now that we ignore its true merit. But its very simplicity and the great ease which it lent to all computations put our arithmetic in the first rank of useful inventions."

In the 13th century, academics like the renowned Italian mathematician Fibonacci began championing zero in their work, helping the Hindu-Arabic system gain credibility in Europe. As trade began to flourish and generate unprecedented levels of wealth in the world, math moved from purely practical applications to ever more abstracted functions. As Alfred North Whitehead said:

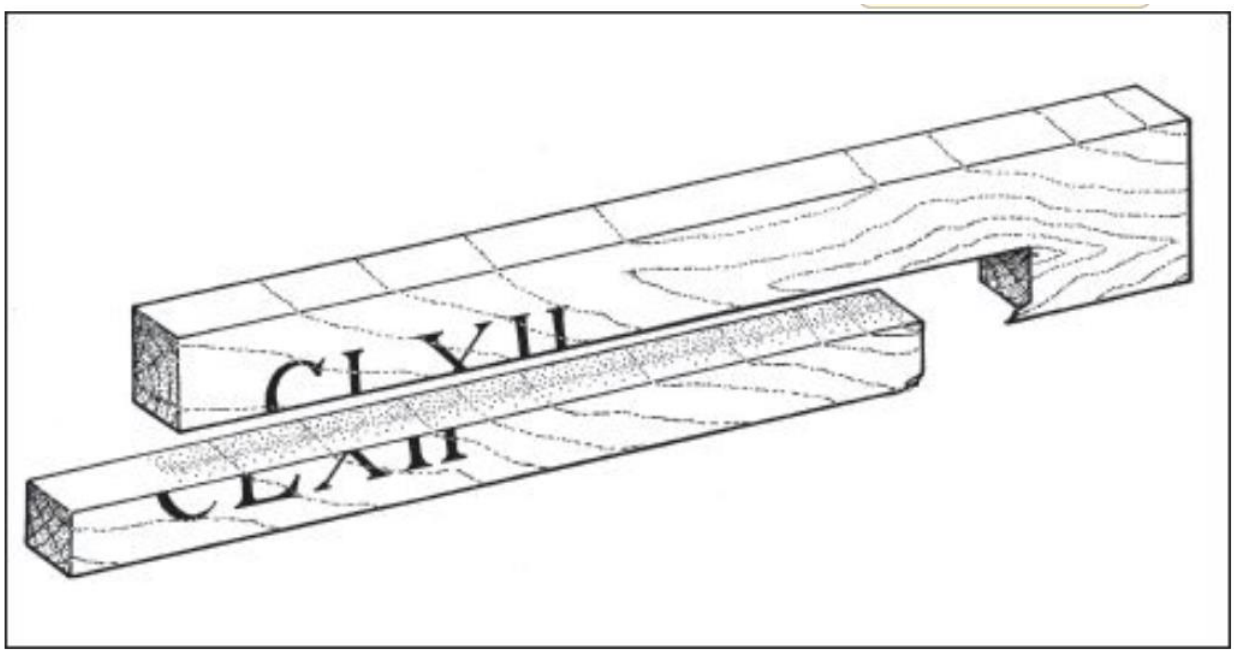
"The point about zero is that we do not need to use it in the operations of daily life. No one goes out to buy zero fish. It is in a way the most civilized of all the cardinals, and its use is only forced on us by the needs of cultivated modes of thought."

As our thinking became more sophisticated, so too did our demands on math. Tools like the abacus relied upon a set of sliding stones to help us keep track of amounts and perform calculation. An abacus was like an ancient calculator, and as the use of zero became popularized in Europe, competitions were held between users of the abacus (the abacists) and of the newly arrived Hindu-Arabic numeral system (the algorists) to see who could solve complex calculations faster. With training, algorists could readily outpace abacists in computation. Contests like these led to the demise of the abacus as a useful tool, however it still left a lasting mark on our language: the words ***calculate***, ***calculus***, and ***calcium*** are all derived from the Latin word for pebble—***calculus***.

The algorists competing against the abacists: contests like these

empirically proved the supremacy of a zero-based numeral system over others, even when aided by ancient mathematical tools like the abacus.

Before the Hindu-Arabic numerals, money counters had to use the abacus or a counting board to keep track of value flows. Germans called the counting board a ***Rechenbank***, which is why moneylenders came to be known as ***banks***. Not only did banks use counting boards, but they also used ***tally sticks*** to keep track of lending activities: the monetary value of a loan was written on the side of a stick, and it was split into two pieces, with the lender keeping the larger piece, known as the ***stock***—which is where we get the term ***stockholder:***

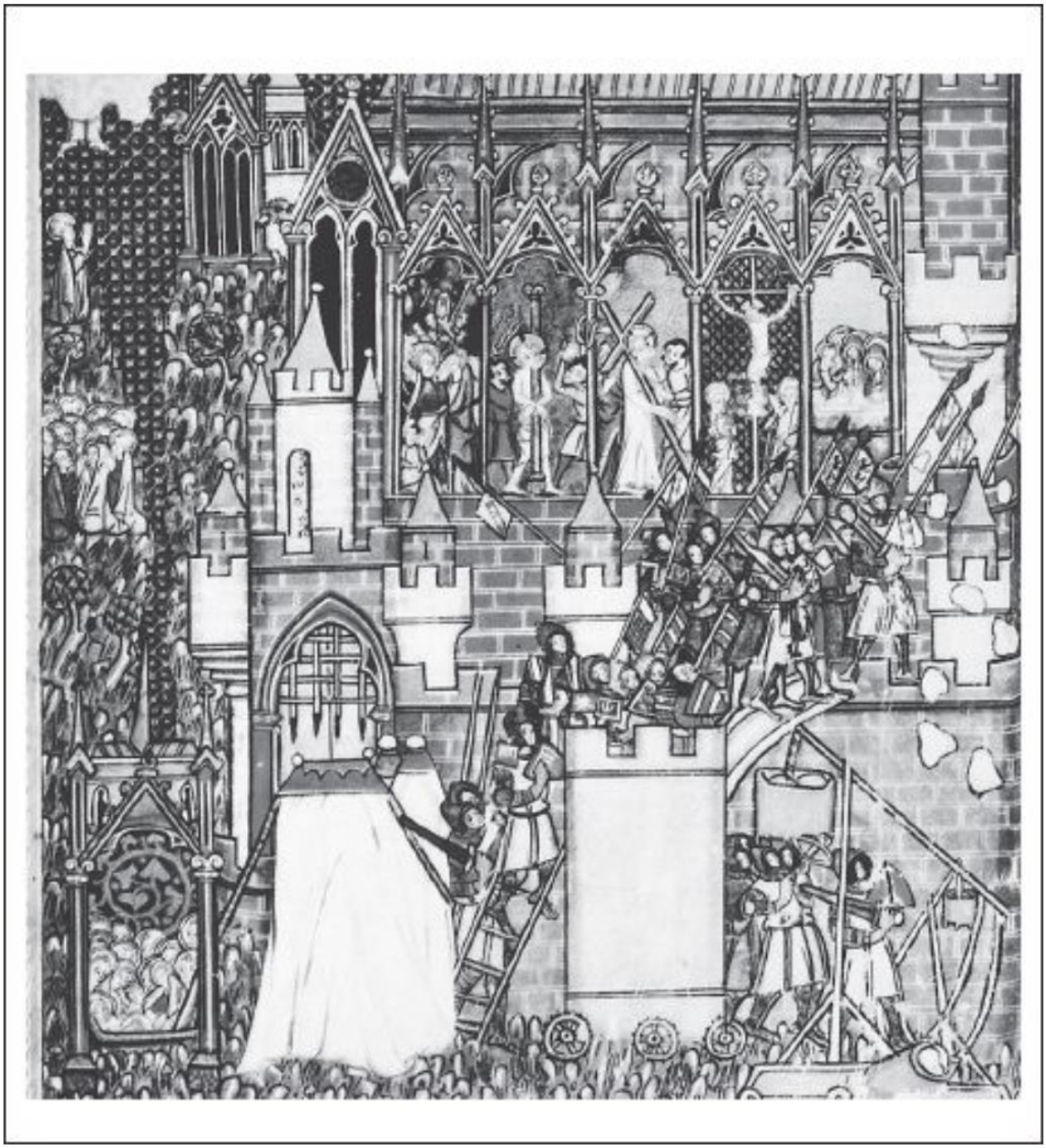


An ancient loan tracking device called a _tally stick: the lender kept the larger portion, the stock, and became a stockholder in the bank that made the loan._

Despite its superior utility for business, governments despised zero. In 1299, Florence banned the Hindu-Arabic numeral system. As with many profound innovations, zero faced vehement resistance from entrenched power structures that were threatened by its existence. Carrying on lawlessly, Italian merchants continued to use the zero-based numeral system, and even began using it to transmit encrypted messages. Zero was essential to these early encryption systems—which is why the word ***cipher***, which originally meant zero, came to mean "secret code." The criticality of zero to ancient encryption systems is yet another aspect of its contribution to Bitcoin's ancestral heritage.

At the beginning of the Renaissance, the threat zero would soon pose to the power of The Church was not obvious. By then, zero had been adapted as an

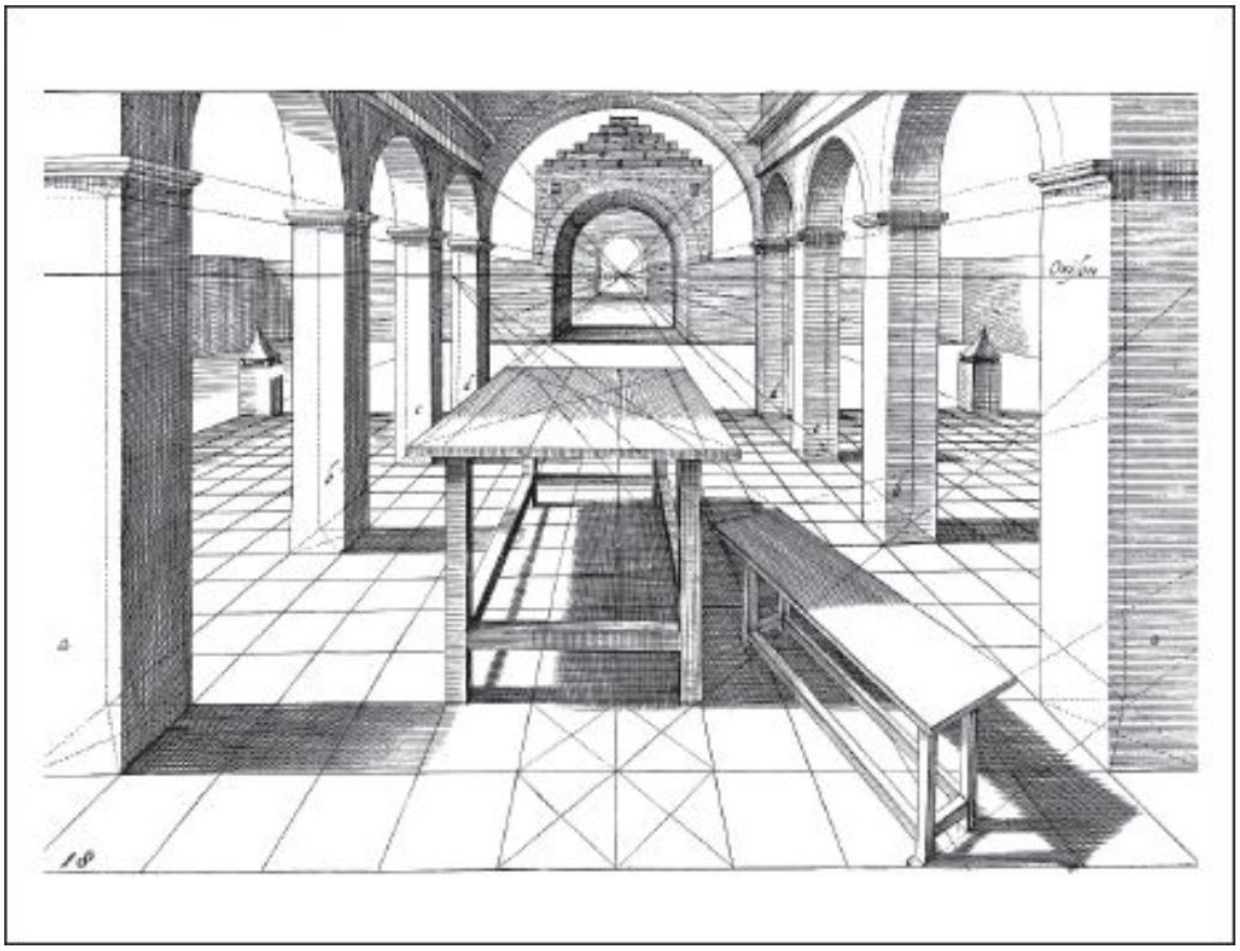
artistic tool to create the ***vanishing point***: an acute place of infinite nothingness used in many paintings that sparked the great Renaissance in the visual arts. Drawings and paintings prior to the vanishing point appear flat and lifeless: their imagery was mostly two-dimensional and unrealistic. Even the best artists couldn't capture realism without the use of zero:



Pre-Renaissance art: still better than a banana duct taped to a canvas.

With the concept of zero, artists could create a zero-dimension point in their work that was "infinitely far" from the viewer, and into which all objects in the

painting visually collapsed. As objects appear to recede from the viewer into the distance, they become ever-more compressed into the "dimensionlessness" of the vanishing point, before finally disappearing. Just as it does today, art had a strong influence on people's perceptions. Eventually, Nicholas of Cusa, a cardinal of The Church declared, "Terra non est centra mundi," which meant "the Earth is not the center of the universe." This declaration would later lead to Copernicus proving heliocentrism—the spark that ignited The Reformation and, later, the Age of Enlightenment:



By adding the vanishing point (a visual conception of zero) to drawings and paintings, art gained the realistic qualities of depth, breadth, and spatial proportion.

A dangerous, heretical, and revolutionary idea had been planted by zero and its visual incarnation, the vanishing point. At this point of infinite distance, the concept of zero was captured visually, and space was made infinite—as Seife describes it:

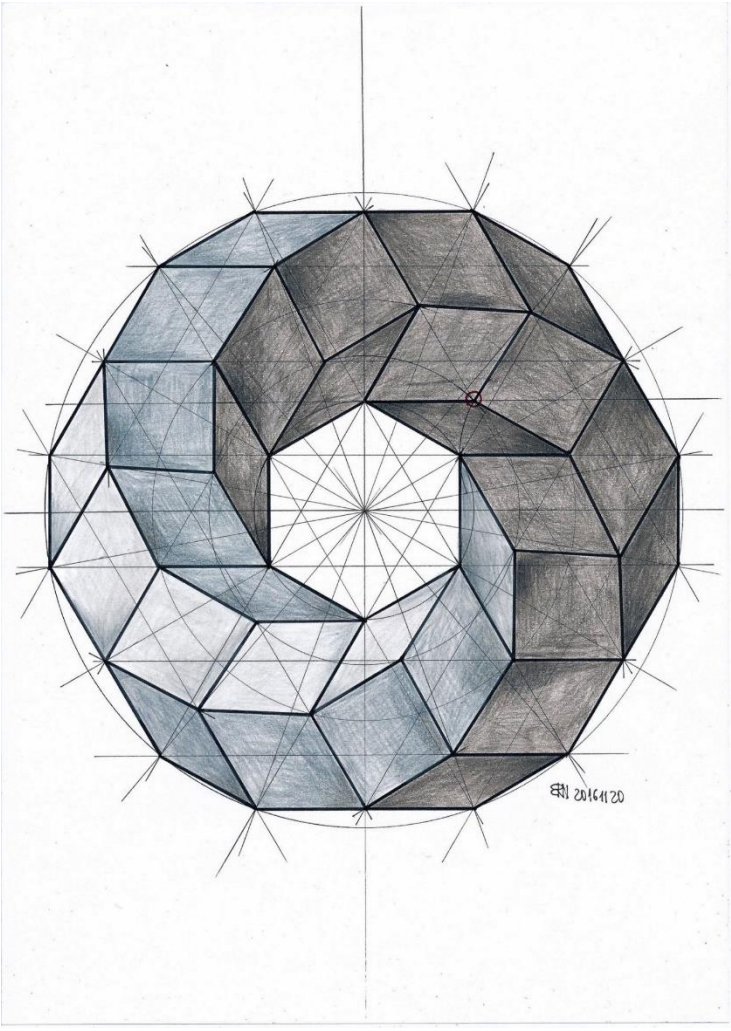
"It was no coincidence that zero and infinity are linked in the vanishing point. Just as multiplying by zero causes the number line to collapse into a point, the vanishing point has caused most of the universe to sit in a tiny dot. This is

a ***singularity***, a concept that became very important later in the history of science—but at this early stage, mathematicians knew little more than the artists about the properties of zero."

The purpose of the artist is to the mythologize the present: this is evident in much of the consumerist "trash art" produced in our current fiat-currency-fueled world. Renaissance artists (who were often also mathematicians, true Renaissance men) worked assiduously in line with this purpose as the vanishing point became an increasingly popular element of art in lockstep with zero's proliferation across the world. Indeed, art accelerated the propulsion of zero across the mindscape of mankind.

Modernity: The Age of Ones and Zeros

Eventually, zero became the cornerstone of calculus: an innovative system of mathematics that enabled people to contend with ever-smaller units approaching zero, but cunningly avoided the logic-trap of having to divide by zero. This new system gave mankind myriad new ways to comprehend and grasp his surroundings. Diverse disciplines such as chemistry, engineering, and physics all depend on calculus to fulfill their functions in the world today:



Calculus enables us to make symphonic arrangements of matter in precise accordance with our imaginations; this mathematical study of continuous change is fundamental to all physical sciences.

Zero serves as the source-waters of many technological breakthroughs—some of which would flow together into the most important invention in history: Bitcoin. Zero punched a hole and created a vacuum in the framework of mathematics and shattered Aristotelean philosophy, on which the power of The Church was premised. Today, Bitcoin is punching a hole and creating a vacuum in the market for money; it is killing Keynesian economics—

which is the propagandistic power-base of the nation-state (along with its apparatus of theft: the central bank).

In modernity, zero has become a celebrated tool in our mathematical arsenal. As the binary numerical system now forms the foundation of modern computer programming, zero was essential to the development of digital tools like the personal computer, the internet, and Bitcoin. Amazingly, all modern miracles made possible by digital technologies can be traced back to the invention of a figure for numeric nothingness by an ancient Indian mathematician: Brahmagupta gave the world a real "something for nothing," a generosity Satoshi would emulate several centuries later. As Aczel says:

"Numbers are our greatest invention, and zero is the capstone of the whole system."

A composition of countless zeroes and ones, binary code led to the proliferation and standardization of communications protocols including those embodied in the internet protocol suite. As people freely experimented with these new tools, they organized themselves around the most useful protocols like http, TCP/IP, etc. Ossification of digital communication standards provided the substrate upon which new societal utilities—like email, ride sharing, and mobile computing—were built. Latest (and arguably the greatest) among these digital innovations is the uninflatable, unconfiscatable, and unstoppable money called Bitcoin.

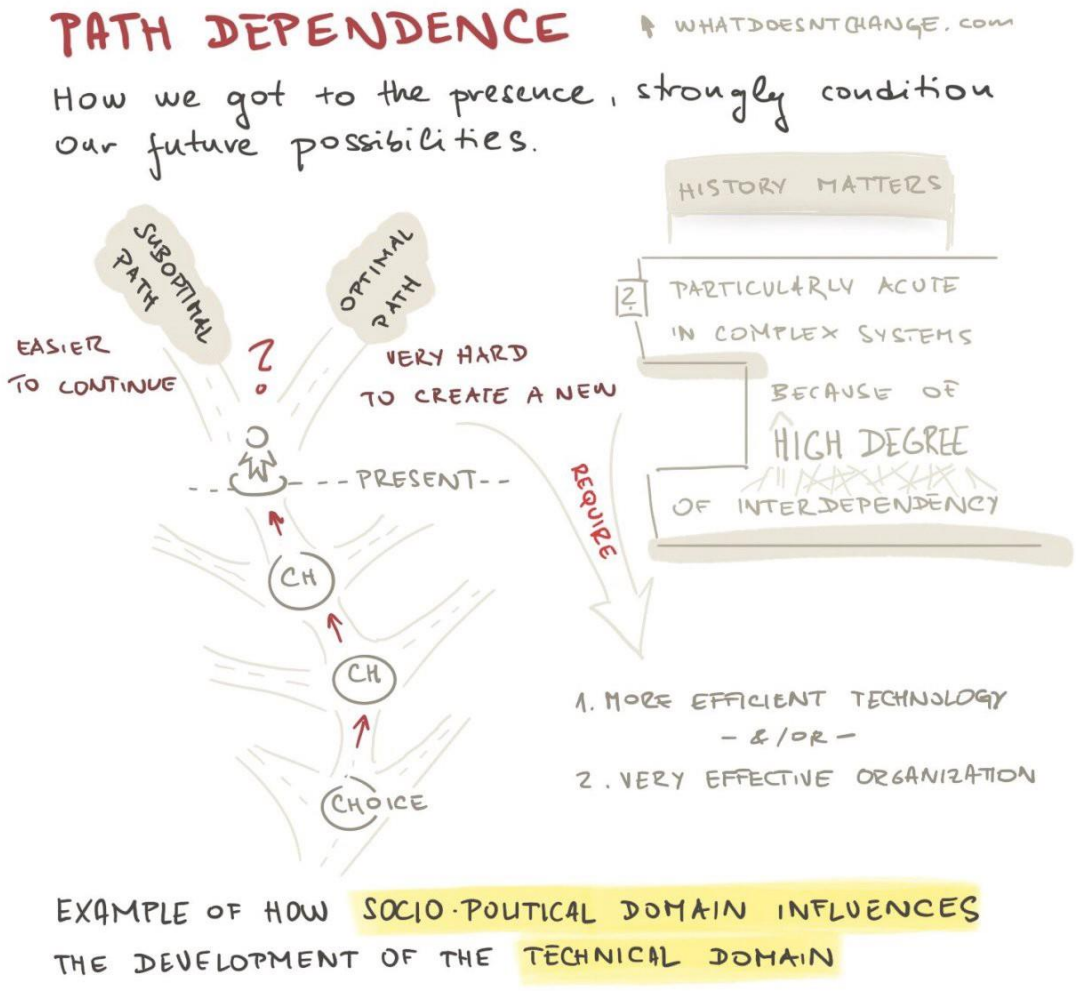
A common misconception of Bitcoin is that it is just one of thousands of cryptoassets in the world today. One may be forgiven for this misunderstanding, as our world today is home to many national currencies. But all these currencies began as warehouse receipts for the same type of thing—namely, monetary metal (usually gold). Today, national currencies are not redeemable for gold, and are instead liquid equity units in a pyramid scheme called fiat currency: a hierarchy of thievery built on top of the freely selected money of the world (gold) which their issuers (central banks) hoard to manipulate its price, insulate their inferior fiat currencies from competitive threats, and perpetually extract wealth from those lower down the pyramid.

Given this confusion, many mistakenly believe that Bitcoin could be disrupted by any one of the thousands of alternative cryptoassets in the marketplace today. This is understandable, as the reasons that make Bitcoin different are not part of common parlance and are relatively difficult to understand. Even Ray Dalio, the greatest hedge fund manager in history, said that he believes Bitcoin could be disrupted by a competitor in the same way that iPhone disrupted Blackberry. However, disruption of Bitcoin is extremely unlikely: Bitcoin is a path-dependent, one-time invention; its critical breakthrough is the discovery of absolute scarcity—a monetary property never before (and never again) achievable by mankind.

Like the invention of zero, which led to the discovery of "nothing as something" in mathematics and other domains, Bitcoin is the catalyst of a worldwide paradigmatic phase change (which some have started calling The Great Awakening). What numeral is to number, and zero is to the void for mathematics, Bitcoin is to absolute scarcity for money: each is a symbol that allows mankind to apprehend a latent reality (in the case of money, time). More than just a new monetary technology, Bitcoin is an entirely new economic paradigm: an uncompromisable base money protocol for a global, digital, non-state economy. To better understand the profundity of this, we first need to understand the nature of path-dependence.

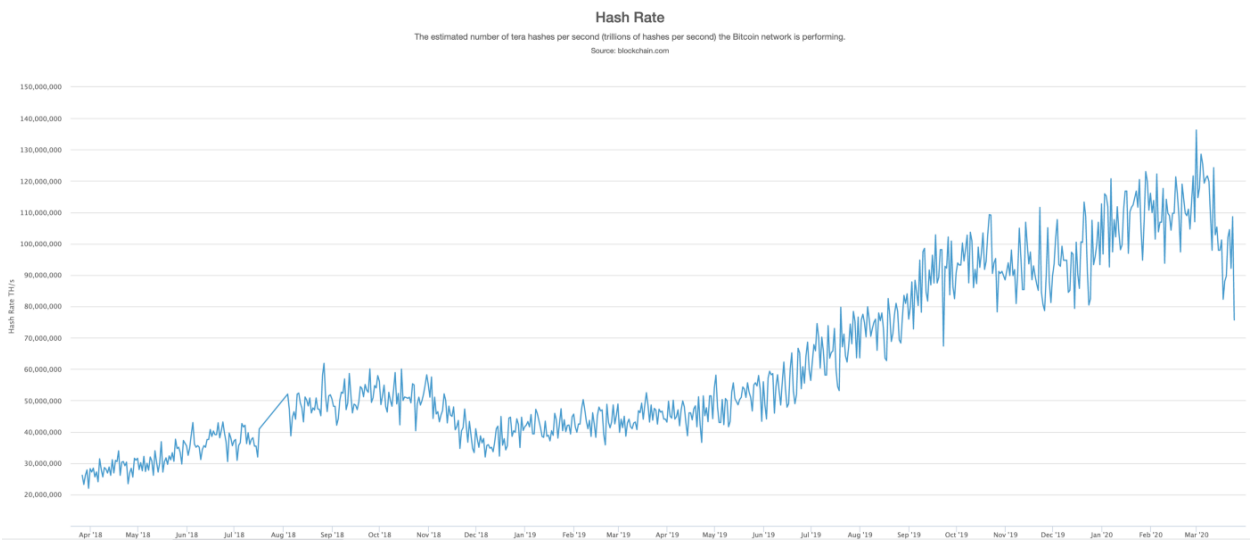
The Path-Dependence of Bitcoin

Path-dependence is the sensitivity of an outcome to the order of events that led to it. In the broadest sense, it means history has inertia:



Path-dependence entails that the sequence of events matters as much as the events themselves: as a simple example, you get a dramatically different result if you shower and then dry yourself off versus if you dry yourself off first and then shower. Path-dependence is especially prevalent in complex systems due to their high interconnectivity and numerous (often unforeseeable) interdependencies. Once started down a particular pathway, breaking away from its sociopolitical inertia can become impossible—for instance, imagine if the world tried to standardize to a different size electrical outlet: consumers, manufacturers, and suppliers would all resist this costly change unless there was a gigantic prospective gain. To coordinate this shift in standardization would require either a dramatically more efficient technology (a pull method—by which people stand to benefit) or an imposing organization to force the change (a push method—in which people would be forced to change in the face of some threat). Path-dependence is why occurrences in the sociopolitical domain often influence developments in the technical; US citizens saw path-dependent pushback firsthand when their government made a failed attempt to switch to the metric system back in the 1970s.

Bitcoin was launched into the world as a one of a kind technology: a non-state digital money that is issued on a perfectly fixed, diminishing, and predictable schedule. It was strategically released into the wild (into an online group of cryptographers) at a time when no comparative technology existed. Bitcoin's organic adoption path and mining network expansion are a non-repeatable sequence of events. As a thought experiment, consider that if a "New Bitcoin" was launched today, it would exhibit weak chain security early on, as its mining network and hash rate would have to start from scratch. Today, in a world that is aware of Bitcoin, this "New Bitcoin" with comparatively weak chain security would inevitably be attacked—whether these were incumbent projects seeking to defend their head start, international banking cartels, or even nation-states:



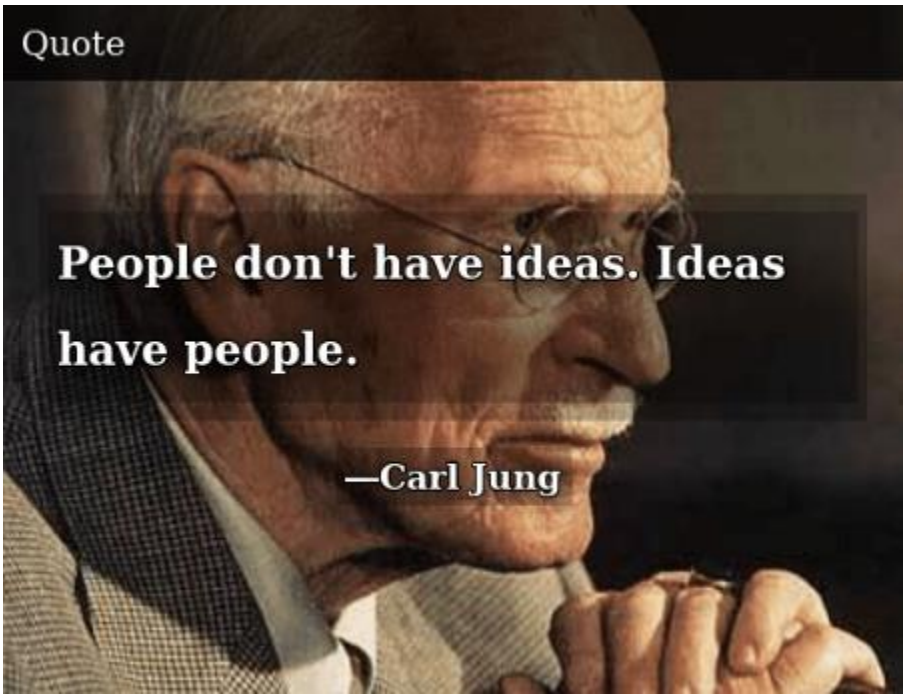
Bitcoin's head start in hash rate is seemingly insurmountable.

Path-dependence protects Bitcoin from disruption, as the organic sequence of events which led to its release and assimilation into the marketplace cannot be replicated. Further, Bitcoin's money supply is absolutely scarce; a totally unique and one-time discovery for money. Even if "New Bitcoin" was released with an absolutely scarce money supply, its holders would be incentivized to hold the money with the greatest liquidity, network effects, and chain security. This would cause them to dump "New Bitcoin" for the original Bitcoin. More realistically, instead of launching "New Bitcoin," those seeking to compete with Bitcoin would take a social contract attack-vector by initiating a hard fork. An attempt like this was already made with the "Bitcoin Cash" fork, which tried to increase block sizes to (ostensibly) improve its utility for payments. This chain fork was an abject failure and a real world reinforcement of the importance of Bitcoin's path-dependent emergence:

Bitcoin Cash is considering a rebrand to Bitcoin Crash.

Continuing our thought experiment: even if "New Bitcoin" featured a diminishing money supply (in other words, a deflationary monetary policy), how would its rate of money supply decay (deflation) be determined? By what mechanism would its beneficiaries be selected? As market participants (nodes and miners) jockeyed for position to maximize their accrual of economic benefit from the deflationary monetary policy, forks would ensue that would diminish the liquidity, network effects, and chain security for "New Bitcoin," causing everyone to eventually pile back into the original Bitcoin—just like they did in the wake of Bitcoin Cash's failure.

Path-dependence ensures that those who try to game Bitcoin get burned. Reinforced by four-sided network effects, it makes Bitcoin's first-mover advantage seemingly insurmountable. The idea of absolute monetary scarcity goes against the wishes of entrenched power structures like The Fed: like zero, once an idea whose time has come is released into the world, it is nearly impossible to put the proverbial genie back in the bottle. After all, unstoppable ideas are independent lifeforms:

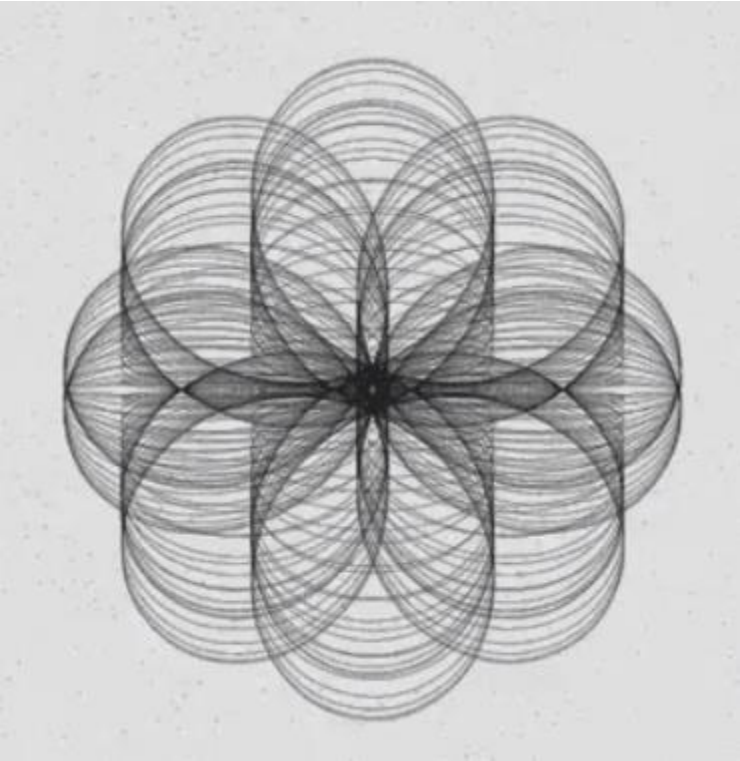


Finite and Infinite Games

Macroeconomics is essentially the set of games played globally to satisfy the demands of mankind (which are infinite) within the bounds of his time (which is strictly finite). In these games, scores are tracked in monetary terms. Using lingo from the groundbreaking book ***Finite and Infinite Games***, there are two types of economic games: unfree (or centrally planned) markets are ***theatrical***, meaning that they are performed in accordance with a predetermined script that often entails dutifulness and disregard for humanity. The atrocities committed in Soviet Russia are exemplary of the consequences of a theatrical economic system. On the other hand, free markets are ***dramatic***, meaning that they are enacted in the present according to consensual and adaptable boundaries. Software development is a good example of a dramatic market, as entrepreneurs are free to adopt the rules, tools, and protocols that best serve customers. Simply: theatrical games are governed by imposed rules (based on tyranny), whereas rulesets for dramatic games are voluntarily adopted (based on individual sovereignty).

From a moral perspective, sovereignty is always superior to tyranny. And from a practical perspective, tyrannies are less energy-efficient than free markets because they require tyrants to expend resources enforcing compliance with their imposed rulesets and protecting their turf. Voluntary games (free market capitalism) outcompete involuntary games (centrally planned socialism) as they do not accrue these enforcement and protection costs: hence the reason capitalism (freedom) outcompetes socialism (slavery) in the long run. Since interpersonal interdependency is at the heart of the comparative advantage and division of labor dynamics that drive the value proposition of cooperation and competition, we can say that money is an infinite game: meaning that its purpose is not to win, but rather to continue to play. After all, if one player had all the money, the game would end (like the game of Monopoly).

In this sense, Bitcoin's terminal money supply growth (inflation) rate of absolute zero is the ultimate monetary Schelling point — a game-theoretic focal point that people tend to choose in an adversarial game. In game theory, a game is any situation where there can be winners or losers, a strategy is a decision-making process, and a Schelling point is the default strategy for games in which the players cannot fully trust one another (like money):



Among many spheres of competing interpersonal interests, scarcity is the Schelling point of money.

Economic actors are incentivized to choose the money that best holds its value across time, is most widely accepted, and most clearly conveys market pricing information. All three of these qualities are rooted in scarcity: resistance to inflation ensures that money retains its value and ability to accurately price capital across time, which leads to its use as an exchange medium. For these reasons, holding the scarcest money is the most energy-efficient strategy a player can employ, which makes the absolute scarcity of Bitcoin an irrefutable Schelling point—a singular, unshakable motif in games played for money.

A distant digital descendent of zero, the invention of Bitcoin represents the *discovery* of absolute scarcity for money: an idea as equally unstoppable.

Similar to the discovery of absolute nothingness symbolized by zero, the discovery of absolutely scarce money symbolized by Bitcoin is special. Gold became money because out of the monetary metals it had the most inelastic (or relatively scarce) money supply: meaning that no matter how much time was allocated towards gold production, its supply increased the least. Since its supply increased the slowest and most predictable rate, gold was favored for storing value and pricing things—which encouraged people to voluntarily adopt it, thus making it the dominant money on the free market. Before Bitcoin, gold was the world's monetary Schelling point, because it made trade easier in a manner that minimized the need to trust other players. Like

its digital ancestor zero, Bitcoin is an invention that radically enhances exchange efficiency by purifying informational transmissions: for zero, this meant instilling more meaning per proximate digit, for Bitcoin, this means generating more salience per price signal. In the game of money, the objective has always been to hold the most relatively scarce monetary metal (gold); now, the goal is to occupy the most territory on the absolutely scarce monetary network called Bitcoin.

A New Epoch for Money

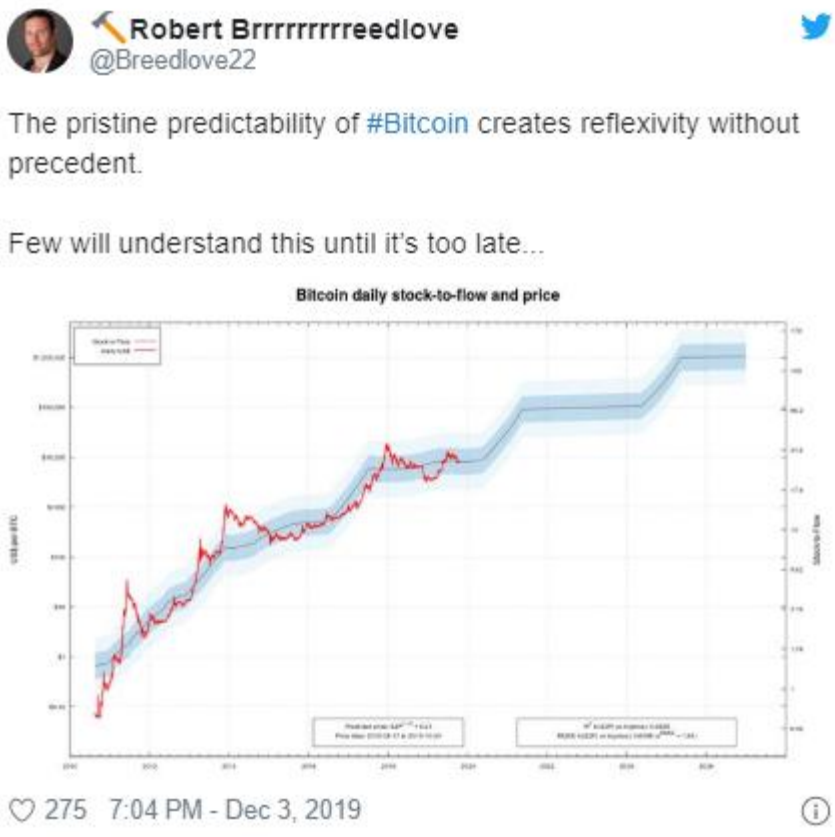
Historically, precious metals were the best monetary technologies in terms of money's five critical traits: divisibility, durability, portability, recognizability, and scarcity. Among the monetary metals, gold was relatively the most scarce, and therefore it outcompeted others in the marketplace as it was a more sound store of value. In the ascension of gold as money, it was as if free market dynamics were trying to zero-in on a sufficiently divisible, durable, portable, and recognizable monetary technology that was also absolutely scarce (strong arguments for this may be found by studying the Eurodollar system). Free markets are distributed computing systems that zero-in on the most useful prices and technologies based on the prevailing demands of people and the available supplies of capital: they constantly assimilate all of mankind's intersubjective perspectives on the world within the bounds of objective reality to produce our best approximations of ***truth***. In this context, verifiable scarcity is the best proxy for the truthfulness of money: assurance that it will not be debased over time.

As a (pre-Bitcoin) thought experiment, had a "new gold" been discovered in the Earth's crust, assuming it was mostly distributed evenly across the Earth's surface and was exactly comparable to gold in terms of these five monetary traits (with the exception that it was more scarce), free market dynamics would have led to its selection as money, as it would be that much closer to absolute scarcity, making it a better means of storing value and propagating price signals. Seen this way, gold as a monetary technology was the closest the free market could come to absolutely scarce money before it was discovered in its only possible form—digital. The supply of any physical thing can only be limited by the time necessary to procure it: if we could flip a switch and force everyone on Earth to make their sole occupation gold mining, the supply of gold would soon soar. Unlike Bitcoin, no physical form of money could possibly guarantee a permanently fixed supply—so far as we know, absolute scarcity can only be digital.

Digitization is advantageous across all five traits of money. Since Bitcoin is just information, relative to other monetary technologies, we can say: its divisibility is supreme, as information can be infinitely subdivided and recombined at near-zero cost (like numbers); its durability is supreme, as

information does not decompose (books can outlast empires); its portability is supreme, as information can move at the speed of light (thanks to telecommunications); and its recognizability is supreme, as information is the most objectively discernible substance in the universe (like the written word). Finally, and most critically, since Bitcoin algorithmically and thermodynamically enforces an absolutely scarce money supply, we can say that its scarcity is infinite (as scarce as time, the substance money is intended to tokenize in the first place). Taken in combination, these traits make absolutely scarce digital money seemingly indomitable in the marketplace.

In the same way that the number zero enables our numeric system to scale and more easily perform calculation, so too does money give an economy the ability to socially scale by simplifying trade and economic calculation. Said simply: scarcity is essential to the utility of money, and a zero-growth terminal money supply represents "perfect" scarcity — which makes Bitcoin as near a "perfect" monetary technology as mankind has ever had. Absolute scarcity is a monumental monetary breakthrough. Since money is valued according to reflexivity, meaning that investor perceptions of its future exchangeability influence its present valuation, Bitcoin's perfectly predictable and finite future supply underpins an unprecedented rate of expansion in market capitalization:



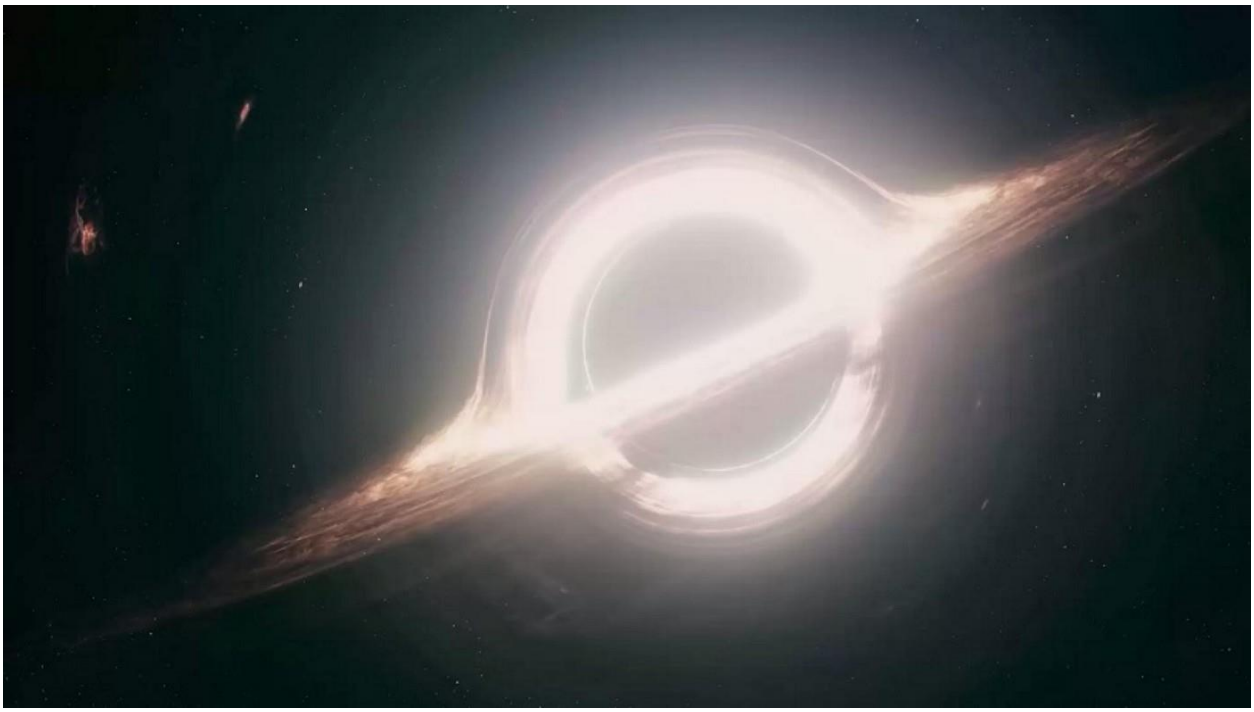
Bitcoin is truly unique: a perfectly scarce and predictably supplied money.

In summary: the invention of Bitcoin represents the discovery of absolute scarcity, or absolute irreproducibility, which occurred due to a particular sequence of idiosyncratic events that cannot be reproduced. Any attempt to introduce an absolutely scarce or diminishing supplied money into

the world would likely collapse into Bitcoin (as we saw with the Bitcoin Cash fork). Absolute scarcity is a one-time discovery, just like heliocentrism or any other major scientific paradigm shift. In a world where Bitcoin already exists, a successful launch via a proof-of-work system is no longer possible due to path-dependence; yet another reason why Bitcoin cannot be replicated or disrupted by another cryptoasset using this consensus mechanism. At this point, it seems absolute scarcity for money is truly a one-time discovery that cannot "disrupted" any more than the concept of zero can be disrupted.

A true "Bitcoin killer" would necessitate an entirely new consensus mechanism and distribution model; with an implementation overseen by an unprecedentedly organized group of human beings: nothing to date has been conceived that could even come close to satisfying these requirements. In the same way that there has only ever been one analog gold, there is likely to only ever be one digital gold. For the same quantifiable reasons a zero-based numeral system became a dominant mathematical protocol, and capitalism outcompetes socialism, the absolute scarcity of Bitcoin's supply will continue outcompeting all other monetary protocols in its path to global dominance.

Numbers are the fundamental abstractions which rule our world. Zero is the vanishing point of the mathematical landscape. In the realm of interpersonal competition and cooperation, money is the dominant abstraction which governs our behavior. Money arises naturally as the most tradable thing within a society—this includes exchanges with others and with our future selves. Scarcity is the trait of money that allows it to hold value across time, enabling us to trade it with our future selves for the foregone opportunity costs (the things we could have otherwise traded money for had we not decided to hold it). Scarce money accrues value as our productivity grows. For these reasons, the most scarce technology which otherwise exhibits sufficient monetary traits (divisibility, durability, recognizability, portability) tends to become money. Said simply: the most relatively scarce money wins. In this sense, what zero is to math, absolute scarcity is to money. It is an astonishing discovery, a window into the void, just like its predecessor zero:

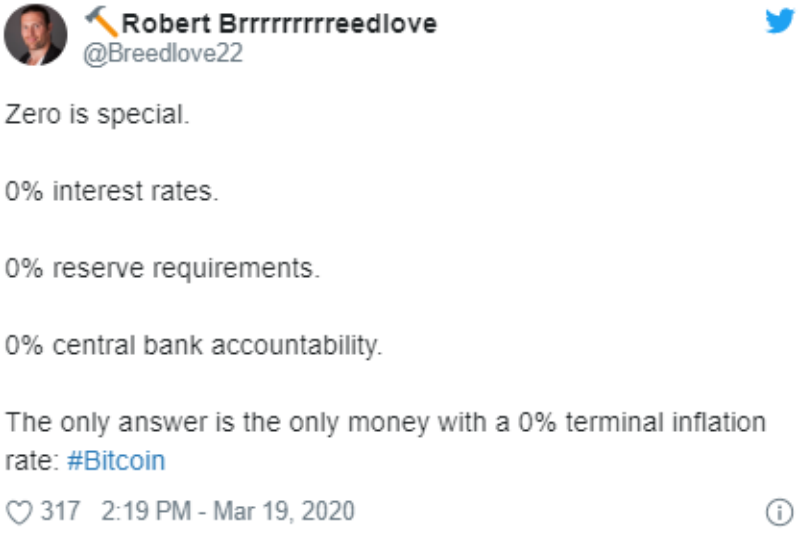


Actual footage of Bitcoin devouring fiat currencies.

Bitcoin is the global economic singularity: the ultimate monetary center of gravity — an exponential devourer of liquid value in the world economy, the epitome of time, and the zero-point of money.

Fiat Currency Always Falls to Zero

Zero has proven itself as the capstone of our numeral system by making it scalable, invertible, and easily convertible. In time, Bitcoin will prove itself as the most important network in the global economic system by increasing social scalability, causing an inversion of economic power, and converting culture into a realignment with Natural Law. Bitcoin will allow sovereignty to once again inhere at the individual level, instead of being usurped at the institutional level as it is today—all thanks to its special forebear, zero:

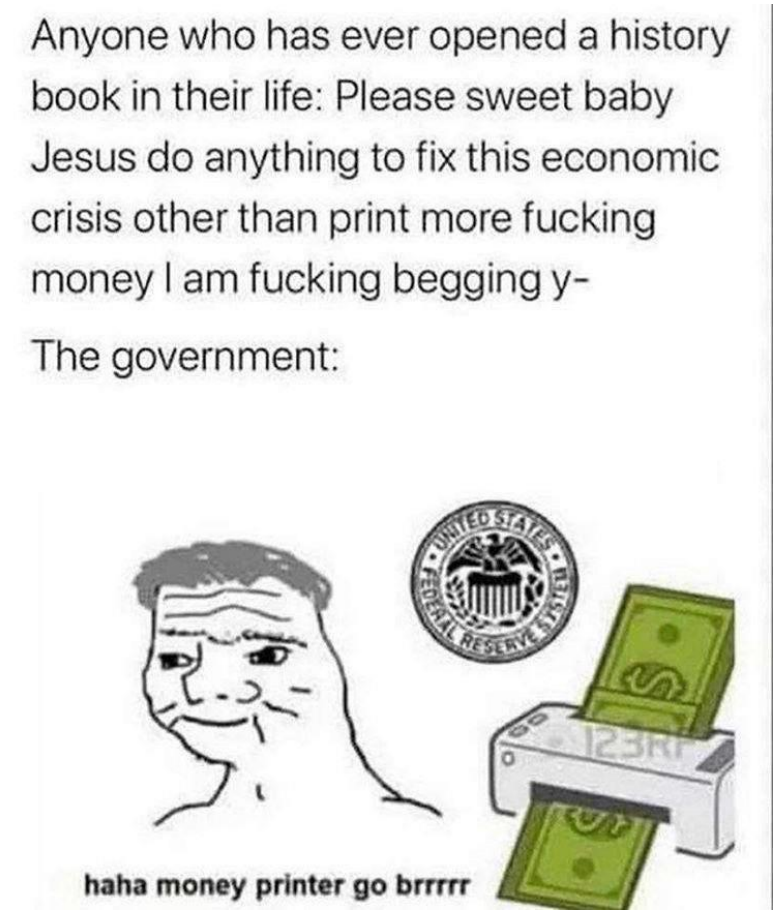


Central planning in the market for money (aka monetary socialism) is dying. This tyrannical financial hierarchy has increased worldwide wealth disparities, funded perpetual warfare, and plundered entire commonwealths to "bail out" failing institutions. A reversion to the free market for money is the only way to heal the devastation it has wrought over the past 100+ years. Unlike central bankers, who are fallible human beings that give into political pressure to pillage value from people by printing money, Bitcoin's monetary policy does not bend for anyone: it gives zero fucks. And in a world where central banks can "just add zeros" to steal your wealth, people's only hope is a "zero fucks" money that cannot be confiscated, inflated, or stopped:

Central banks literally "just add zeros" to steal vast swathes of societal wealth.

Bitcoin was specifically designed as a countermeasure to "expansionary monetary policies" (aka wealth confiscation via inflation) by central bankers. Bitcoin is a true zero-to-one invention, an innovation that profoundly changes society instead of just introducing an incremental advancement. Bitcoin is ushering in a new paradigm for money, nation-states, and energy-efficiency. Most importantly, it promises to break the cycle of criminality in which

governments continuously privatize gains (via seigniorage) and socialize losses (via inflation). Time and time again, excessive inflation has torn societies apart, yet the lessons of history remain unlearned—once again, here we are:



Thank you internet for all the hilarious yet meaningful memes.

The Zero Hour

How much longer will monetary socialism remain an extant economic model? The countdown has already begun: Ten. Nine. Eight. Seven. Six. Five. Four. Three. Two. One. Liftoff. Rocket technicians always wait for zero before ignition; countdowns always finalize at the zero hour. Oil price wars erupting in Eurasia, a global pandemic, an unprecedented expansionary monetary policy response, and another quadrennial Bitcoin inflation-rate halving: 2020 is quickly becoming the zero hour for Bitcoin.

Inflation rate and societal wellbeing are inversely related: the more reliably value can be stored across time, the more trust can be cultivated among market participants. When a money's roots to economic reality are severed—as happened when the peg to gold was broken and fiat currency was born—its supply inevitably trends towards infinity (hyperinflation) and the functioning of its underlying society deteriorates towards zero (economic collapse). An unstoppable free market alternative, Bitcoin is anchored to economic reality (through proof-of-work energy expenditure) and has an inflation rate predestined for zero, meaning that a society operating on a Bitcoin standard would stand to gain in virtually infinite ways. When Bitcoin's inflation rate finally reaches zero in the mid 22nd century, the measure of its soundness as a store of value (the stock-to-flow ratio) will become infinite;

people that realize this and adopt it early will benefit disproportionately from the resultant mass wealth transfer.

Zero and infinity are reciprocal: 1/∞ = 0 and 1/0 = ∞. In the same way, a society's wellbeing shrinks towards zero the more closely the inflation rate approaches infinity (through the hyperinflation of fiat currency). Conversely, societal wellbeing can, in theory, be expanded towards infinity the more closely the inflation rate approaches zero (through the absolute scarcity of Bitcoin).Remember: The Fed is now doing whatever it takes to make sure there is "infinite cash" in the banking system, meaning that its value will eventually fall to zero:

Market value of money always converges to its marginal cost of production: "Infinite cash" means dollars will inevitably become as valuable as the paper on which they are printed.

Zero arose in the world as an unstoppable idea because its time had come; it broke the dominion of The Church and put an end to its monopolization over access to knowledge and the gates to heaven. The resultant movement—The Separation of Church and State—reinvigorated self-sovereignty in the world, setting the individual firmly as the cornerstone of the state. Rising from The Church's ashes came a nation-state model founded on sound property rights, rule of law, and free market money (aka hard money). With this new age came an unprecedented boom in scientific advancement, wealth creation, and worldwide wellbeing. In the same way, Bitcoin and its underlying discovery of absolute scarcity for money is an idea whose time has come. Bitcoin is shattering the siege of central banks on our financial sovereignty; it

is invoking a new movement—The Separation of Money and State—as its revolutionary banner; and it is restoring Natural Law in a world ravaged by a mega-wealth-parasite—The Fed.

Only unstoppable ideas can break otherwise immovable institutions: zero brought The Church to its knees and Bitcoin is bringing the false church of The Fed into the sunlight of its long-awaited judgement day.

Both zero and Bitcoin are emblematic of the void, a realm of pure potentiality from which all things spring forth into being — the nothingness from which everything effervesces, and into which all possibility finally collapses. Zero and Bitcoin are unstoppable ideas gifted to mankind; gestures made in the spirit of "something for nothing." In a world run by central banks with zero accountability, a cabal that uses the specious prospects of "infinite cash" to promise us everything (thereby introducing the specter of hyperinflation), nothingness may prove to be the greatest gift we could ever receive...

Thank you Brahmagupta and Satoshi Nakamoto for your generosity.

Everything is Nothing.

0

With a Twist.

∞

Thank you for reading *The Number Zero and Bitcoin*.

Follow me on Twitter: https://twitter.com/Breedlove22

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 @relevantpeterschiff

And anyone else I forgot :)

Sources:

1. Thank you to Amir D. Aczel, author of ***Finding Zero***, whose work inspired much of this essay: https://www.amazon.com/Finding-Zero-Mathematicians-Odyssey-Uncover/dp/1250084911
2. Thank you Charles Seife, author of ***Zero: The Biography of a Dangerous Idea***, whose work inspired much of this essay. Many images used exploring the history of zero came from his book: https://www.amazon.com/gp/product/B000QUEHLM/ref=ppx_yo_dt_b_search_asin_title?ie=UTF8&psc=1
3. https://timesofindia.indiatimes.com/india/ancient-indian-text-pushes-back-history-of-zero-by-500-yrs/articleshow/60521958.cms
4. https://en.wikipedia.org/wiki/Negative_number
5. https://www.embibe.com/exams/real-life-applications-of-calculus/
6. https://whatdoesntchange.com/post/174845015609/path-dependence
7. https://www.livescience.com/42748-imaginary-numbers.html
8. https://www.smithsonianmag.com/history/origin-number-zero-180953392/
9. https://en.wikipedia.org/wiki/Nirvana
10. https://buddhism.stackexchange.com/questions/10003/are-there-pictures-paintings-of-nirvana
11. https://en.wikipedia.org/wiki/Absolute_(philosophy)

Thanks to Ben Prentice and Stephen Cole.

Stop Calling for a Free Market in Money

By Sven Schnieders

Posted March 29, 2020

Avoiding the Question

There are many people, coming mostly from the Austrian school of economics, who argue for a free market in money—a good example being Thorsten Polleit. (I admire his knowledge about economics, which is, unfortunately, only exceeded by his ignorance of Bitcoin.) Although I mostly agree with their reasoning and share the enthusiasm for such a free market, I cannot stop being astonished by the naivety of the idea.

The argument for a free market in money is often brought forward when discussing the future of money and, more importantly, when trying to answer the question what the best candidate for a new basis of our monetary system might be. Faced with such a difficult question, the easiest way out is to argue for a free market, which then decides this question. This reasoning is used in many other cases (where it is valid) and it might sound valid here, but as I will show, it is not. I want to emphasize again that I am in favor of a free market in money, and I do not want any form of money to be banned—everyone should be free to choose. However, arguing for fewer regulations so we can have a free market to finally decide which money is the best, is not only unproductive but also ignorant of the lesson history has taught us. But let us not get ahead of ourselves and first take a look at the argumentation.

Free Market in Money

The argumentation starts with the correct observation that nowadays, we do not have a free market in money. The State has put in place many regulations that make using alternative forms of money more difficult and costly (e.g. legal tender laws). For some payments—taxes—paying with a form of money other than fiat (i.e. USD, EUR, etc.) is not possible. So in good Austrian and libertarian tradition, those people call for fewer regulations to establish a free market. This free market will then decide which form of money (Fiat, Gold, Bitcoin, etc.) is the best. The stance is: "After the state has stopped to regulate this market, we can finally have a real competition to see which form of money prevails."

Gold is bad Money


POSTMASTER: PLEASE POST IN A CONSPICUOUS PLACE.—JAMES A. FARLEY, Postmaster General

UNDER EXECUTIVE ORDER OF THE PRESIDENT

Issued April 5, 1933

all persons are required to deliver

ON OR BEFORE MAY 1, 1933

all GOLD COIN, GOLD BULLION, AND GOLD CERTIFICATES now owned by them to a Federal Reserve Bank, branch or agency, or to any member bank of the Federal Reserve System.

Executive Order

FORBIDDING THE HOARDING OF GOLD COIN, GOLD BULLION AND GOLD CERTIFICATES.

For Further Information Consult Your Local Bank

GOLD CERTIFICATES may be identified by the words "GOLD CERTIFICATE" appearing thereon. The serial number and the Treasury seal on the face of a GOLD CERTIFICATE are printed in YELLOW. Be careful not to confuse GOLD CERTIFICATES with other issues which are redeemable in gold but which are not GOLD CERTIFICATES. Federal Reserve Notes and United States Notes are "redeemable in gold" but are not "GOLD CERTIFICATES" and are not required to be surrendered

Special attention is directed to the exceptions allowed under Section 2 of the Executive Order

This reasoning misses the crucial point that money which cannot succeed under the oppression of government is not a valid candidate for the basis of our monetary system. In other words: if a form of money cannot thrive under the current regulations it is bad money. This is the lesson people should have learned from the failure of gold—gold is good money, except that it is not. It is only good money as long as the government allows it to function, but as history has shown, it is awful once the state decides to outlaw it. This makes it a bad form of money. The physical nature of gold makes it extremely difficult to store and validate by yourself, which leads to centralization (I have explained this main flaw of gold in more detail in this essay). This centralization made it possible for governments to end the gold standard by easily taking control of most of the supply.

Perfect Environment

Calling for a free market in money is extremely naive and short-sighted because it is exactly the ability to succeed under oppression and regulations

that makes a particular form of money good in the first place. The importance of this insight cannot be overstated. You do not want money, which only works when the state allows it to work, but fails in the most crucial moments. The money market we have right now—with all these regulations and taxes—is a great environment to test all the different forms of money and see which one prevails; it is this market in which money has to thrive and not in some ideal free market. We need a form of money that works under the most hostile conditions, i.e., even after being banned—the only viable candidate for this is Bitcoin. Again, thriving in a free market without government interference and regulations is not sufficient to make a form of money good money. Good money needs to work in the real world against real adversity and not only succeed in an ideal free-market.

Bitcoin Against all Odds

The second reason I call arguing for a free market in money naive is that governments and central banks will not give up their power over the monetary system. It is not the free market that makes Bitcoin—good money—possible but rather Bitcoin that makes the free market possible. Arguing for a free market in money so we can finally decide on the best money, is putting the cart before the horse. Good money—money outside of the control of the state—needs to come first, then afterward, the state will get smaller, and regulations will be cut back because there won't be any money left to support such a huge state. It is not by trying to convince those in power that we will change the world and establish a free market but by the unstoppable force of Bitcoin. Bitcoin does not ask for permission, and Bitcoin does not depend on ruling back the state first. It succeeds against all odds, that is what makes it great money.

Conclusion

I hope that this essay is sufficient to convince those who argue in favor of a free market for money that 1.) it is not sufficient for money to only work under a benevolent—free market embracing—state, but that good money needs to work especially in those circumstances where it is facing adversity; we do not want another bad money like gold that fails us in times we need it the most, and 2.) it is naive to hope that by arguing in favor of a free market in money, the state and central banks will realize their mistakes and finally embrace it.

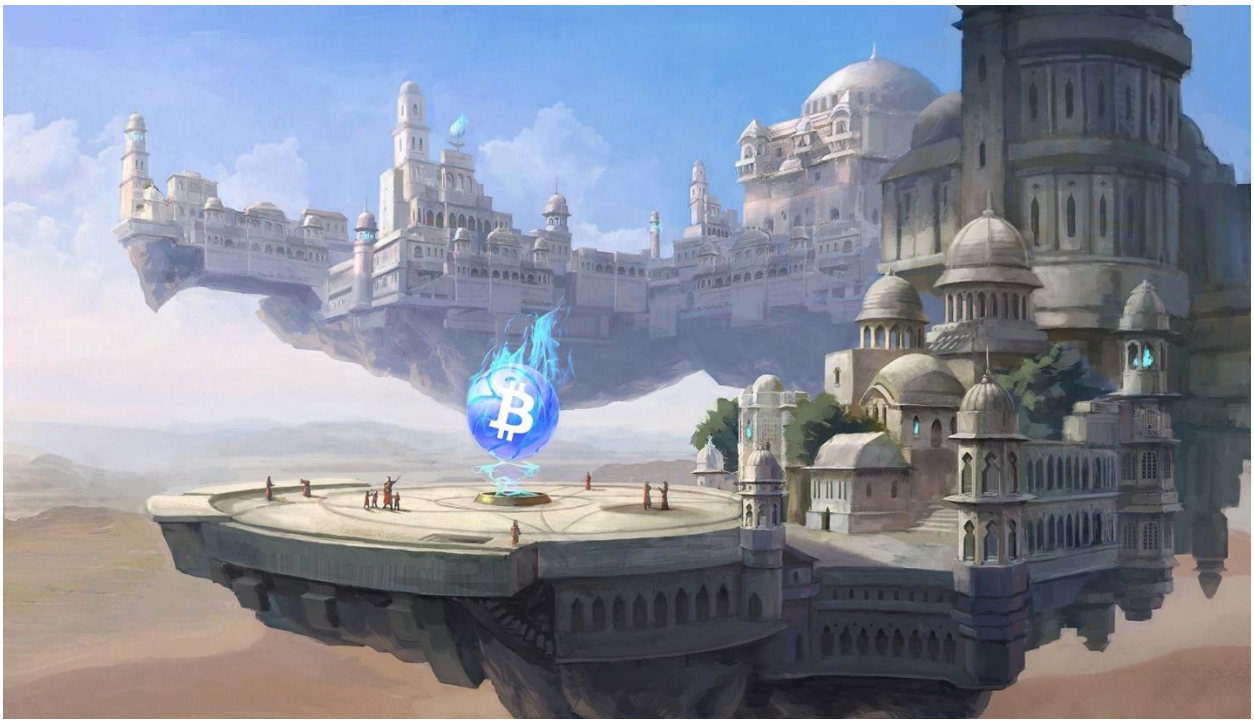
As always, thank you for reading my essay.

Dear Bitcoiners

An optimistic letter to friends and foes around the globe.

By Gigi

Posted March 31, 2020



The madness of this world became obvious in an instant. Everything is changing way faster than most of us ever imagined — but I'm not worried. To the contrary, I'm weirdly optimistic — because of Bitcoin, and because of you.

You probably don't know me; I probably don't know you. And that's perfectly fine. However, I know some of you — and I believe that I know some of you quite well, even if we have never met or met only briefly. I have read your writings, watched you debate each other, saw the things you've built, and listened to your voices for countless hours. I don't care if you identify as a bitcoiner, or as a maximalist, or as a pre-/shit-/multi-/whatever-coiner. I don't care if you fell down the rabbit hole years ago or if you just got the first glimpse of the honey badger den. I don't care about your political beliefs, sexual orientation, gender, religion, age, and countless other qualifiers that might be used to put you in a box. The fact that you are here, reading this, thinking about Bitcoin, ***caring*** about Bitcoin, is enough for me. That's why I'm bullish. Bullish on Bitcoin, and bullish on bitcoiners.

“Bullish on bitcoiners.” — Matt Odell

Bitcoin’s implications are so far-reaching, the innovation so profound, it boggles the mind. The inter-disciplinary nature of this beast attracts minds from countless areas of expertise: computer science, cryptography, mathematics, physics, economics, finance, trading, engineering, the list goes on and on. Bright minds, extraordinary characters, strong opinions, contrarians, idealists trying to change the world — all those and more make up the loose collective we might call bitcoiners.

Honey Badger Don’t Care

Don’t get me wrong: Bitcoin doesn’t need you; it doesn’t need any of us. It’s incentive systems have a way to make sure that Bitcoin will be fine, even if the set of people working on it and using it changes completely. It will be fine, just as it is now as the whole world grinds to a halt.

The current crisis — and the financial repercussions that will inevitably follow — will make it obvious that we need Bitcoin more than Bitcoin needs us. Again, don’t get me wrong: we must not be complacent. We must continue to care, continue to build, continue to educate, continue to proselytize, continue to argue, continue to debate. We find ourselves at the forefront of a battle of ideas, and in this battle, complacency kills.

“Ask not what bitcoin can do for you, but what you can do for bitcoin.”
— Adam Back

If you can contribute by coding, writing, educating, discussing, recording, creating, or simply hodling — great. But make no mistake: Bitcoin is bigger than all of us. And, dare I say it, the current failure of the legacy system is bigger than Bitcoin.

Yes, Bitcoin has the potential to fix many of the underlying issues of our corruptible and broken systems. But we will need a plethora of freedom-enabling technologies to win this war; tools that empower the individual by default, by offering strong privacy guarantees, encryption, and the freedom to use these tools without restrictions.

Shill Lightly

As this global pandemic sweeps through the globe, with hundreds of thousands infected, tens of thousands dead, and millions of people out of a job, priorities shift from trivial to existential. While difficult, it is more important than ever to stay humble and shill lightly. It is all too easy to alienate friends and family by offering an enthusiastic Bitcoin lecture every time you sit at the dinner table. While enthusiasm is laudable, I strongly believe that Bitcoin will be understood by everyone as soon as they are ready

— be it out of necessity or out of curiosity. Yes, the timeline just got accelerated. But this is still a marathon, not a sprint. And it might be one of many marathons.

“One of the facts of history is that battles do not stay won. Those that matter have to be waged again and again.” — Stanley Knowles

The powers that be will neither step away willingly nor silently. And since the battle for self-sovereignty and freedom is one that matters, it will have to be waged again and again.

Protecting An Idea Whose Time Has Come

Bad actors will continually try to undermine Bitcoin, as they have tried in the past. Unfortunately, we have good reason to believe that this will continue. And, unfortunately, we see the trend of undermining and maiming technology everywhere we look. If we look at the internet, for example, we see various interest groups waging war against net neutrality, politicians introducing nation-wide firewalls, websites geo-blocking content, people getting arbitrarily deplatformed, demonetized, or banned.

They say that nothing is as powerful as an idea whose time has come. I believe that Bitcoin’s time has come, and in hindsight, it will be obvious to everyone. Before it becomes obvious, however, swathes of people will try to distort what Bitcoin is and the ideas it represents.

“Ideas change the world, but they do it by assuming shape, they do it by taking concrete form.” — Stanley Knowles

While Bitcoin’s form is quite concrete since its inception, it is an abstract, intangible form, making it exceptionally hard to grasp. It will take some time until Bitcoin is as ubiquitous as the internet is now. This time — this window of confusion — will be used and abused by lawmakers and charlatans alike. However, it is also a window of opportunity. An opportunity to sharpen our tools, to prepare for the flood, to ship the future faster than they can ban it.

They Are Always Wrong

Undoubtedly, there are plenty of people who don’t want Bitcoin to succeed. They will do everything in their power to prolong the inevitable. They are wed to the current system, gaining from its inherent imbalance. Some are close to the monetary spigot, or willfully ignorant, or enemies of freedom in general. Others are outright evil, aiming to become the foot that stomps on your face, forever.

“They told us not to wish in the first place, not to aspire, not to try; to be quiet, to play nice, to shoot low and aspire not at all. They are always wrong. Follow

your dreams. Make your wishes. Create the future. And above all, believe in yourself." — Joseph Michael Straczynski

They will continue to tell us that what we are doing is a pipe dream, that what we are aiming for is impossible, that we can't operate outside of the current systems. They will restrict our freedoms: our freedom to transact, our freedom to save, our freedom to remain private. They will tell us that certain kinds of mathematics and software are illegal. They will continue to justify mass surveillance by trying to sell us the illusion of safety. And they will continue to be wrong.

Speak up. Be outraged. Use alternatives. Build alternatives. Don't settle for the status quo — we can do better. Bitcoin is what we make of it, and I can't imagine a better set of people to realize the full potential of this grand idea.

"There is nothing better to be on a shared mission with extraordinary people who can be radically truthful, and radically transparent with each other." — Ray Dalio

Stay vigilant. Stay radical. Stay true to yourself. As the world is grinding to a halt, and the fall of Rome becomes more likely than ever, strong characters, sound principles, and truthful conduct are imperative.

The stage is set, the drama is unfolding, and as the crescendo comes we must not give in to tyranny. The path will be twisted and bumpy, and I'm honored to walk it to the end, with you on my side. We got this.

Thanks to Hass, John, and Dennis for their valuable feedback.

Disclaimer:

WORDS

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

This Journal does not contain reference to any of the investment products or services currently offered by the operator of the journal, that means any business I am associated with. Bitcoin, shitcoins, and related technologies can be volatile. Don't buy what you can't afford to lose and please do your own research.

Bitcoin has paved the way for some VERY radical technology AND it's very confusing. Read more. Ask questions. The purpose of this Journal is to provide archive and curate the best commentary and culture in the bitcoin space.

Nothing within this Journal constitutes investment, legal, tax or other advice. This Journal should not be used as the basis for any investment decisions which a reader may be considering. Any potential investor in bitcoin or shitcoins, even if experienced and affluent, is strongly recommended to seek independent financial advice upon the merits of the same in the context of their own unique circumstances.

Share this journal early and often. Engage the authors and tell them what you think. We sharpen our position through discourse and debate.

DYOR | BTFD | HODL

I hope you enjoy this project. I'm on a mission to archive the great works of Bitcoin thinkers.
Onward!

Read **WORDS**

- @_joerodgers