WORDS

May 2020

A collection of commentary from the brightest minds in Bitcoin.

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

History

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

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

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

Support WORDS

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

Support WORDS

Spread the word

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

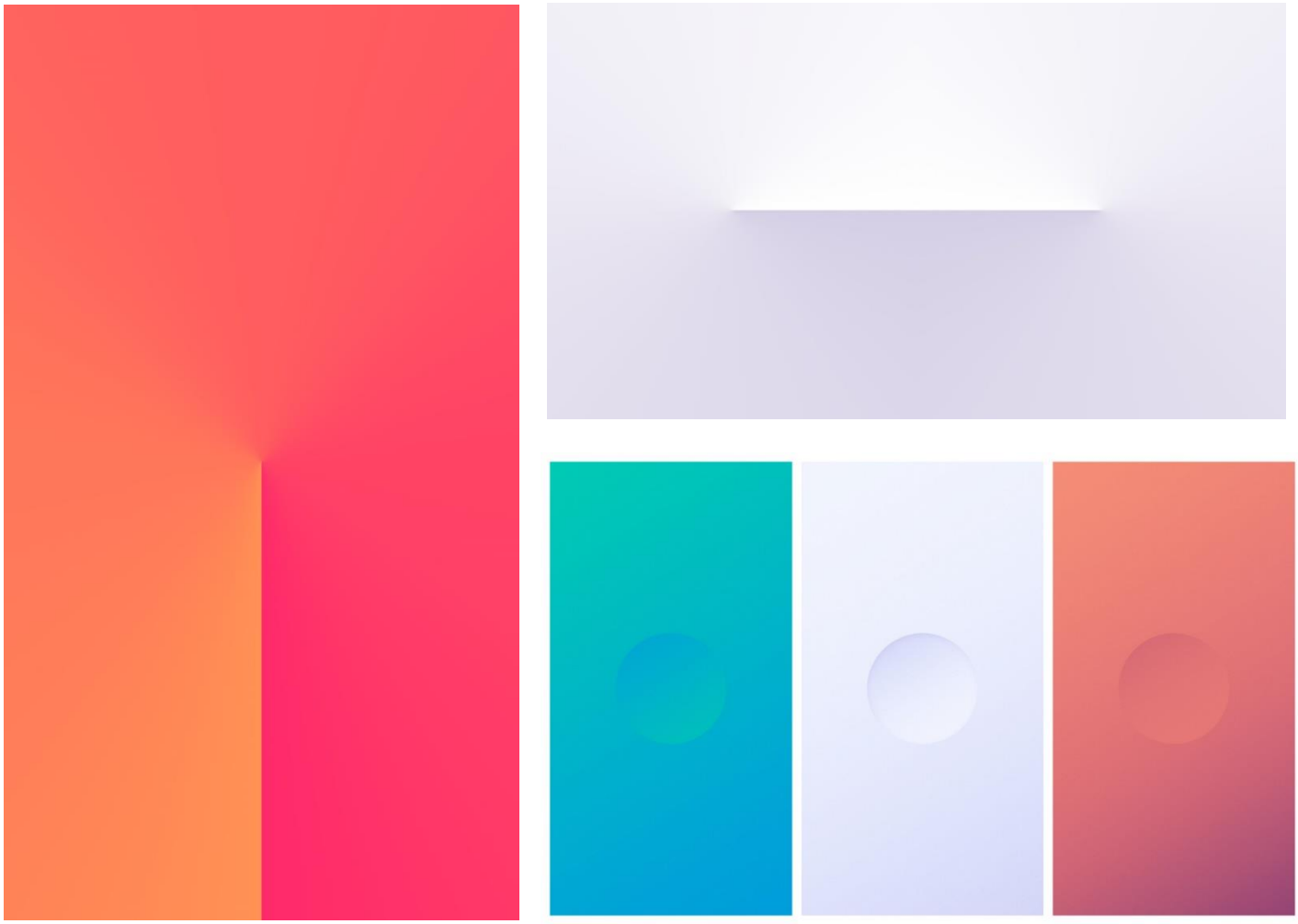
Our pledge

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

Cover Art by Van

A big thank you to Van for allowing me to use your work on the cover of this month's journal. Van is part of the crypto art movement and is exploring digitally scarce artwork through NFT platforms. Visit Van's website for more information.

Van is a digital artist and graphic designer from Italy with an interest in abstract digital art, whose work showcases new ways to mix and blend design and art with a touch of bright contrast colors.



Bitcoin is Common Sense

By Parker Lewis on Unchained Capital

Posted May 1, 2020

AUDIO VERSION BY Bitcoin Audible

“Perhaps the sentiments contained in the following pages, are not yet sufficiently fashionable to procure them general favor; a long habit of not thinking a thing wrong, gives it a superficial appearance of being right, and raises at first a formidable outcry in defense of custom. But the tumult soon subsides. Time makes more converts than reason.” – Thomas Paine, Common Sense (February 24, 1776)

These were the opening remarks of Thomas Paine’s call for American independence in early 1776. At the time, a declaration of independence was far from a certainty, but in Paine’s view, there was no question. It wasn’t a debate; there was only one path forward. Still, he understood that public opinion had not yet caught up and naturally remained anchored to the status quo, with a preference for reconciliation rather than independence. Old habits die hard. The status quo has a tendency of being defended, regardless of merit, merely by its anchoring in time to the way things have always been. However, truths have a way of becoming self-evident in time, more often due to common sense rather than any amount of reason or logic. One day, the truth is more likely to smack you in the face, becoming painfully obvious through some firsthand experience which opens up a perspective that otherwise would not have existed. While Paine was undoubtedly attempting to persuade an undecided populous with reason and logic, it was at the same time an appeal to not overthink that which stands in opposition to what is already self-evident.

In Paine’s view, independence was not a modern-day IQ test, nor was its relevance confined to the American colonies; instead, it was a common sense test and its interest was universal to “the cause of all mankind,” as Paine put it. In many ways, the same is true of bitcoin. It is not an IQ test; instead, bitcoin is common sense and its implications are near universal. Few people have ever stopped to question or understand the function of money. It facilitates practically every transaction anyone has ever made, yet no one really knows the why of that equation, nor the properties that allow money to effectively coordinate economic activity. Its function is taken for granted, and as a result, it is a subject not widely taught or explored. Yet despite a limited baseline of knowledge, there is often a visceral reaction to the very idea of bitcoin as money. The default position is predictably no. Bitcoin is an anathema to all

notions of existing custom. On the surface, it is entirely inconsistent with what folks know money to be. For most, money is just money because it always has been. In general, for any individual, the construction of money is anchored in time and it is very naturally not questioned.

But enter bitcoin, and everyone suddenly becomes an expert in what is and isn't money, and to the fly-by-night expert, it certainly is not bitcoin. Bitcoin is natively digital, it is not tied to a government or central bank, it is volatile and perceived to be "slow," it is not used en masse to facilitate commerce, and it is not inflationary. This is one of those rare instances when a thing does not walk like a duck or quack like a duck but it's actually a duck, and what you thought was a duck all along was mistakenly something entirely different. When it comes to modern money, ***the long habit of not thinking a thing wrong, gives it a superficial appearance of being right.*** In all perceived-to-be successful applications today, money is issued by a central bank; it is relatively stable and capable of near infinite transaction throughput; it facilitates day-to-day commerce; and by the grace of god, its supply can be rapidly inflated to meet the needs of an ever-changing economy. Bitcoin has none of these traits (some not presently, others not ever), and as a result, it is most often dismissed as not meeting the standards of modern-day money. This is where overthinking a problem can cripple the highest of IQs. Pattern recognition fails because the game fundamentally changed, but the players do not yet realize it. It is akin to getting lost in the weeds or failing to see the forest through the trees. Bitcoin is finitely scarce, it is highly divisible and it is capable of being sent over a communication channel (and on a permissionless basis). There will only ever be 21 million bitcoin. Rocket scientists and the most revered investors of our time could look at this equation relative to other applications in the market and be confounded, not seeing its value. While at the same time, if posed with a very simple question, would you rather be paid either in a currency with a fixed supply that cannot be manipulated or in a currency that is subject to persistent, systemic and significant debasement, an overwhelming majority of individuals would choose the former all day, every day.

On bitcoin: "It's probably rat poison squared" – Warren Buffett

"Bitcoin – there's even less you can do with it [...] I'd rather have bananas, I can eat bananas" – Mark Cuban

Money Doesn't Grow On Trees

As kids, we all learn that ***money doesn't grow on trees*** but on a societal level, or as a country, any remnant of common sense seems to have left the building. Just in the last two months, central banks in the United States, Europe and Japan (the Fed, ECB and BOJ) have collectively inflated the

supply of their respective currencies by $3.3 trillion in aggregate – an increase of over 20% in just eight weeks. The Fed alone has accounted for the majority, minting $2.5 trillion dollars and increasing the base money supply by over 60%. And it's far from over; trillions more will be created. It is not a possibility; it is a certainty. Common sense is that deep feeling of uncertainty many are experiencing that says, "this doesn't make any sense" or "this doesn't end well." Few carry that thought process out to its logical conclusion, often because it is uncomfortable to think about, but it is reverberating throughout the country and the world. While not everyone is connecting the equation to 21 million bitcoin, a growing number of people are. _Time makes more converts than reason. _Individuals don't have to understand how or why there will only ever be 21 million bitcoin; all that has to be recognized in practical experience is that dollars are going to be worth significantly less in the future, and then the idea of having a currency with a fixed supply begins to make sense. Understanding how it is possible that bitcoin has a fixed supply comes after making that initial connection, but even still, no one needs to understand the how to understand that it is valuable. It is the light bulb turning on.

For each individual, there is a choice to either exist in a world in which someone gets to produce new units of money for free (but just not them) or a world where no one gets to do that (including them). From an individual perspective, there is not a marginal difference in those two worlds; it is night and day, and anyone conscious of the decision very intuitively opts for the latter, recognizing that the former is neither sustainable, nor to his or her advantage. Imagine there were 100 individuals in an economy, each with different skills. All have determined to use a common form of money to facilitate trade in exchange for goods and services produced by others. With the one exception that a single individual has a superpower to print money, requiring no investment of time and at practically no cost. Given human time is an inherently scarce resource and that it is a required input in the production of any good or service demanded in trade, such a scenario would mean that one person would get to purchase the output of all the others for free. Why would anyone agree to such an arrangement? That the individual is an enterprise, and more specifically, a central bank expected to act in the public interest does not change the fundamental operation. If it does not make sense on a micro level, it does not magically transform into a different fundamental fact merely because there are greater degrees of separation. If

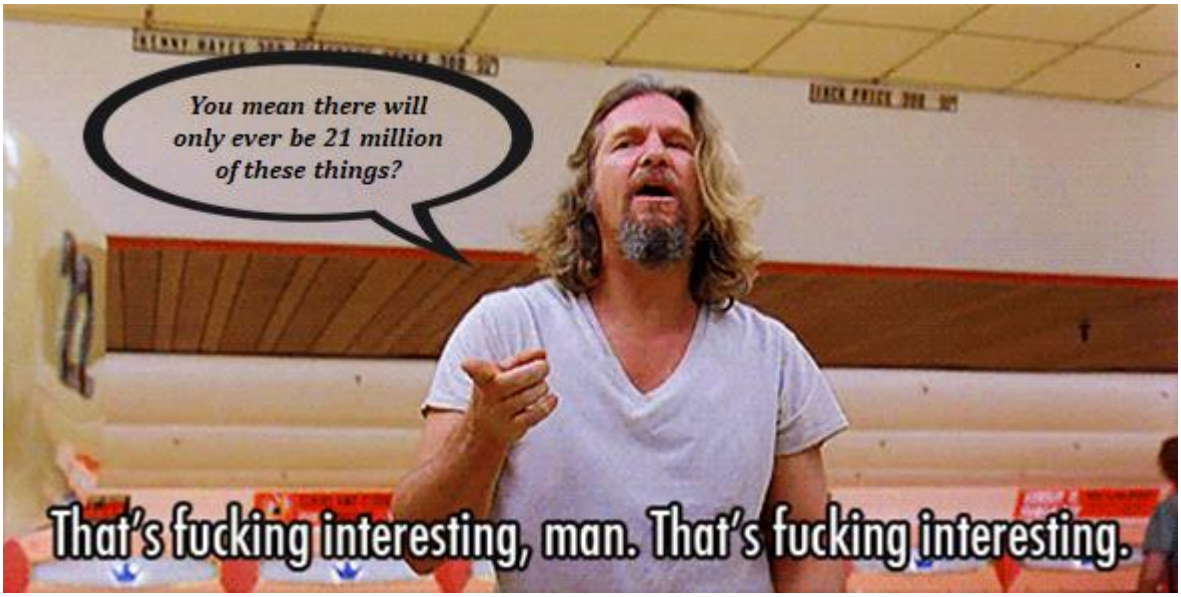
no individual would bestow that power in another, neither would a conscious decision be made to bestow it in a central bank.

Everything beyond this fundamental reality strays into abstract theory, relying on leaps of faith, hypotheticals and big words that no one understands, all while divorced from individual decision points. It is not that one individual is more trusted than another or one central bank relative to another; it is simply that, on an individual level, no individual is advantaged by someone else having the ability to print money, regardless of identity or interests. That this is true leaves only one alternative, that each individual would be advantaged by ensuring that no other individual or entity has this power. The Fed may have the ability to create dollars at zero cost, but ***money still doesn't grow on trees.*** It is more likely that a particular form of money is not actually money than it is that money miraculously started growing on trees. And at an individual level, everyone is incentivized to ensure that is not the case. While there is a long habit of not thinking this particular thing wrong, the errant defense of custom can only stray so far. Time converts everyone back into reality. At present, it is the Fed's "shock and awe" campaign contrasted by the simplicity in bitcoin's fixed supply of 21 million. There is no amount of reason that can replace an observed divergence in two distinct paths.

Defending Existing Custom

"There's money and there's credit. The only thing that matters is spending and you can spend money and you can spend credit. And when credit goes down, you better put money into the system so you can have the same level of spending. That's what they did through the financial system (referencing QE in response to the past crisis) and that thing worked."– Ray Dalio, CNBC September 19, 2017

Basic Bitcoin Common Sense



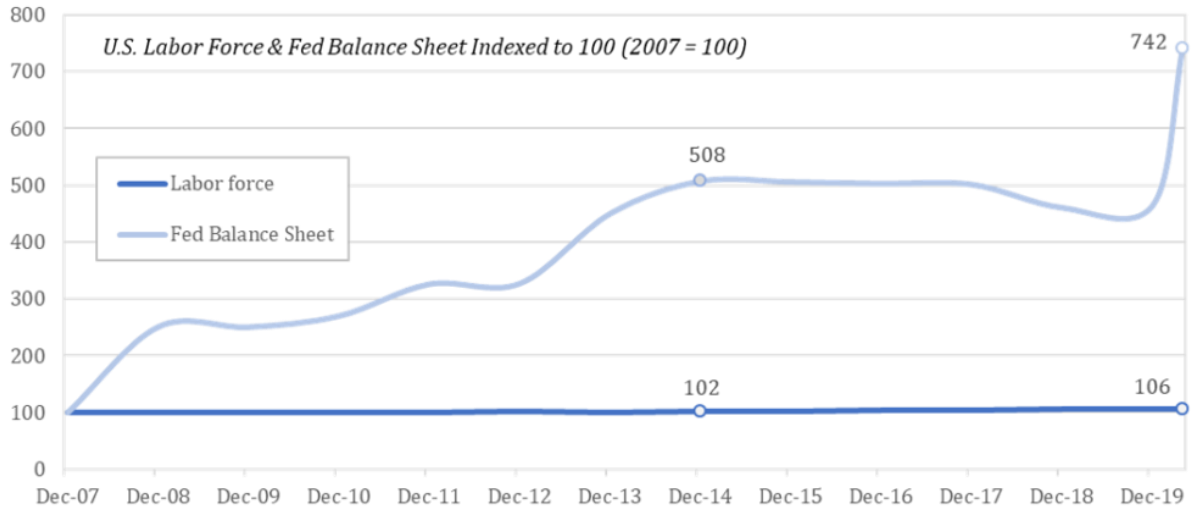
There is No Such Thing as a Free Lunch

As more people become aware of the Fed's activities, it only begins to raise more questions. $2,500,000,000,000 is a big number, but what is actually happening? Who gets the money? What will the effects be and when? What are the consequences? Why is this even possible? How does it make any sense? All very valid questions, but none of these questions change the fact that many more dollars exist and that each dollar will be worth materially less in the future. That is intuitive. However, at an even more fundamental level, recognize that the operation of printing money (or creating digital dollars) does nothing to generate economic activity. To really simplify it, imagine a printing press just running on a loop. Or, imagine keying in an amount of dollars on a computer (which is technically all that the Fed does when it creates "money"). That very operation can definitionally do nothing to produce anything of value in the real world. Instead, that action can only induce an individual to take some other action.

Recognize that any tangible good or service produced is produced by some individual. Human time is the input, capital production is the output. Whether it is software applications, manufacturing equipment, a service or an end consumer good, all along the value chain, an individual contributed time to produce some good or service. That time and value is ultimately what money tracks and prices. Entering a large number into the computer does not produce software, hardware, cars or homes. People produce those things and money coordinates the preferences of all individuals within an economy, compensating value to varying degrees for time spent.

When the Fed creates $2.5 trillion in a matter of weeks, it is consolidating the power to price and value human time. Seems cryptic but it is not a suggestion that the individuals at the Fed are consciously or deliberately operating maliciously. It is just the root level consequence of the Fed's actions, even if well intentioned. Again, the Fed's operation (arbitrarily adding zeros to various bank account balances) cannot actually generate economic activity; all it can do is determine how to allocate new dollars. By doing so, it is advantaging some individual, enterprise or segment of the economy over another. In allocating new dollars that it creates, it is replacing a market function, one priced by billions of people, with a centralized function, greatly influencing the balance of power as to who controls the monetary capital that coordinates economic activity. Think about the distribution of money as the balance of control influencing and ultimately determining what gets built, by whom and at what price. At the moment of creation, there exists more money but there exists no more human time or goods and services as a consequence of that action. Similarly, over time, the Fed's actions do not create more jobs, there are just more dollars to distribute across the labor force, but with a different distribution of those holding the currency. The Fed can print money (technically, create digital dollars), but it can't print time nor can it do anything but artificially manipulate the allocation of resources within an economy.

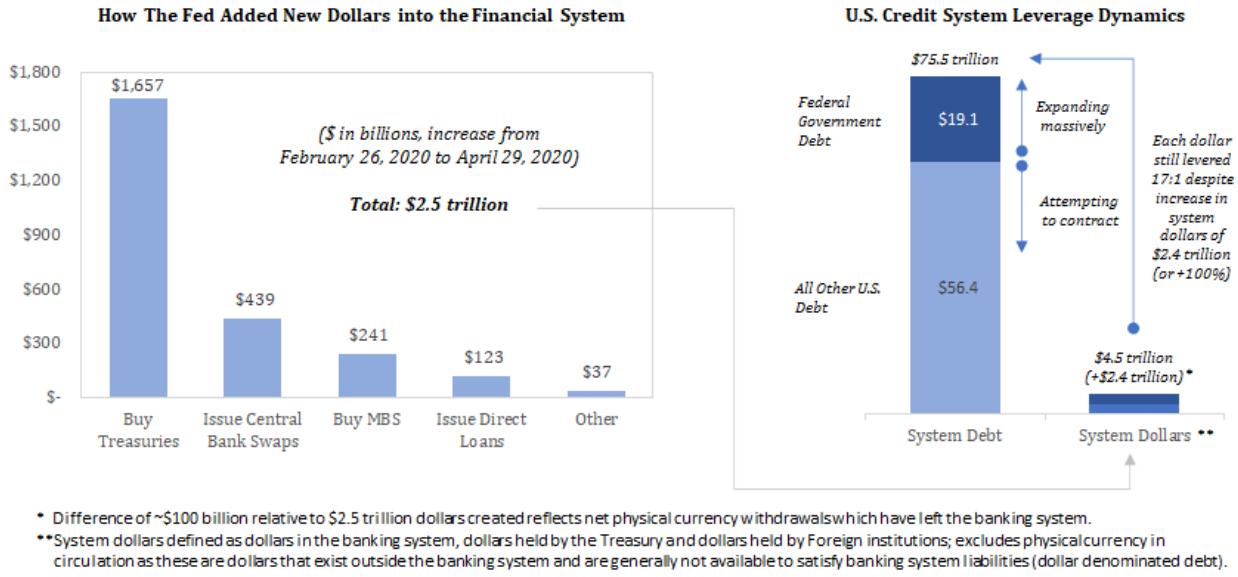
No Free Lunches, Just More Dollars



Since 2007, the Fed balance sheet has increased seven-fold, but the labor force has only increased 6%. There are roughly the same number of people contributing output (human time) but far more dollars to compensate for that time. Do not be confused by impossible-to-quantify theory concerning the idea of a job saved versus a job lost; this is the U.S. labor force, defined by the Bureau of Labor Statistics as all persons 16 years of age and older, both

employed and unemployed. The inevitable result is that the value of each dollar declines, but it does not create more workers, and all prices do not adjust ratably to the increase in the money supply, including the price of labor.

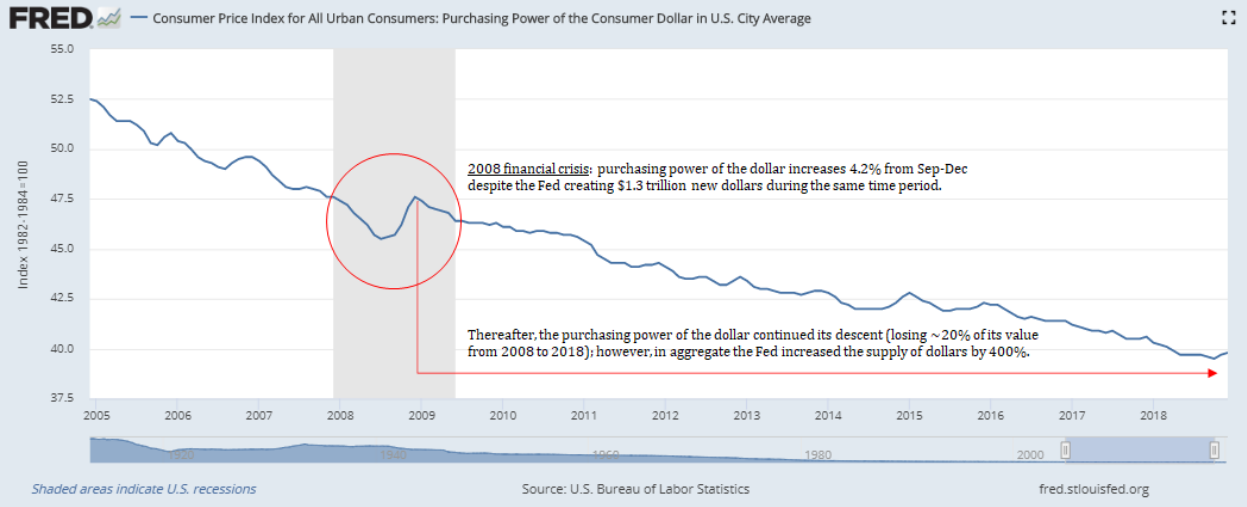
In a theoretical world, if the Fed were to distribute the money in equal proportion to each individual that held the currency previously, it would not shift the balance of power. In practical application, the distribution of ownership shifts dramatically, heavily favoring the holders of financial assets (which is what the Fed buys in the process of creating new dollars) as well as those with cheap access to credit (the government, large corporations, high net-worth individuals, etc.). In aggregate, the purchasing power of every dollar declines, just not immediately, while a small subset benefits at the cost of the whole (see the Cantillon Effect). Despite the consequences, the Fed takes these actions in an attempt to support a credit system that would otherwise collapse without the supply of more dollars. In the Fed's economy, the credit system is the price setting mechanism as the amount of dollar-denominated debt far outstrips the supply of dollars, which is also why the purchasing power of each dollar does not immediately respond to the increase in the money supply.

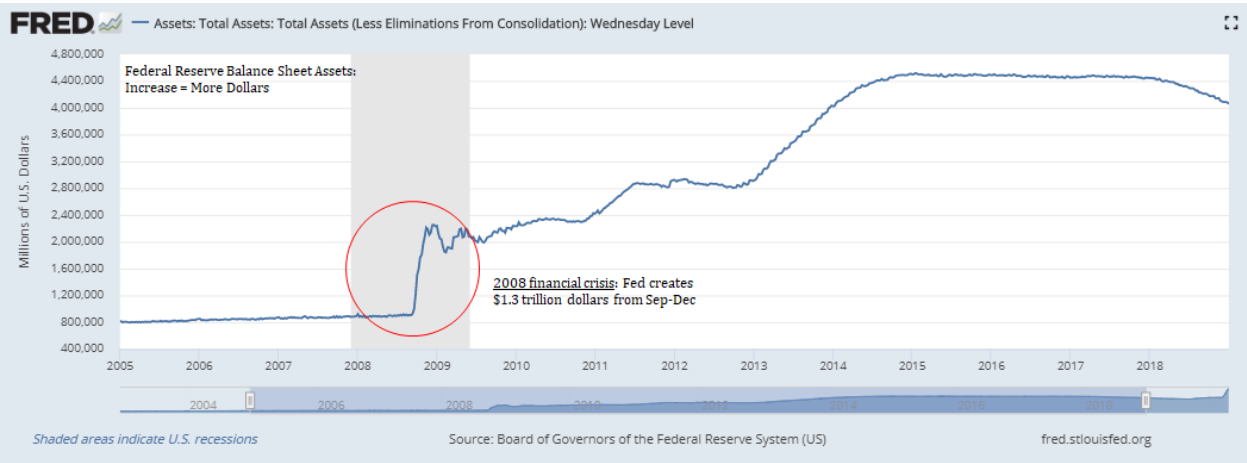


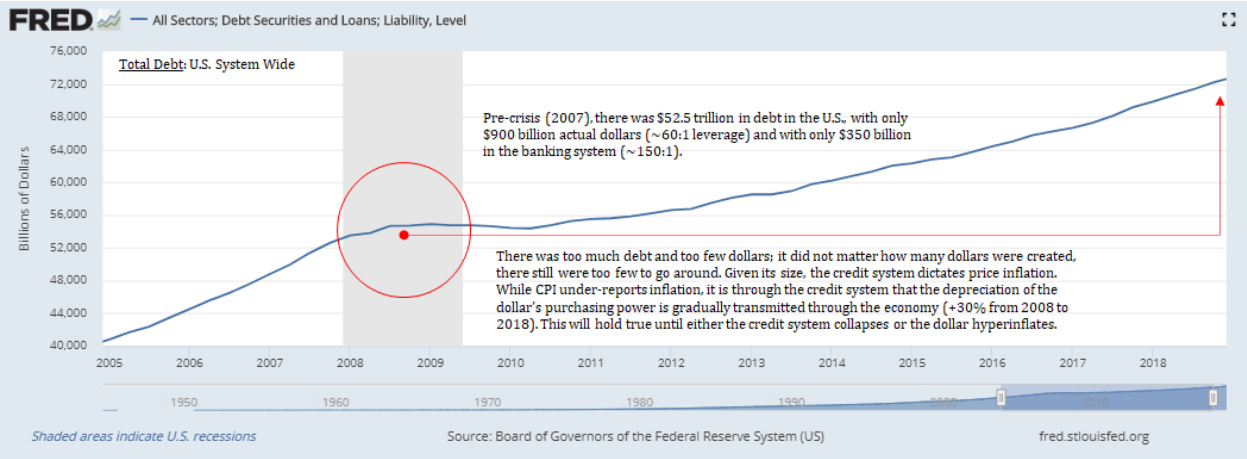
* Difference of ~$100 billion relative to $2.5 trillion dollars created reflects net physical currency withdrawals which have left the banking system.
** System dollars defined as dollars in the banking system, dollars held by the Treasury and dollars held by Foreign institutions; excludes physical currency in circulation as these are dollars that exist outside the banking system and are generally not available to satisfy banking system liabilities (dollar denominated debt).

Instead, the effects of increasing the money supply are transmitted, over time, through an expansion of the credit system. The credit system attempting to contract is the market and the individuals within an economy adjusting and re-pricing value; the Fed attempting to reverse that natural course by flooding the market with dollars is, by definition, overriding the market's price setting function, fundamentally altering the structure of the economy. The market solution to the problem is to reduce debt (expression of preference) and the Fed's solution is to increase the supply of dollars such

that existing debt levels can be sustained. The goal is to stabilize the credit system such that it can then expand, and it is a redux to the 2008 financial crisis, which provides a historical roadmap. In the immediate aftermath of the prior crisis, the Fed created $1.3 trillion new dollars in a matter of months. Despite this, the dollar initially strengthened as deflationary pressures in the credit system overwhelmed the increase in the money supply, but then, as the credit system began to expand, the dollar's purchasing power resumed its gradual decline. At present, the cause and effect of the Fed's monetary stimulus is principally transmitted through the credit system. It was the case in the years following the 2008 crisis, and it will hold true this time so long as the credit system remains intact.

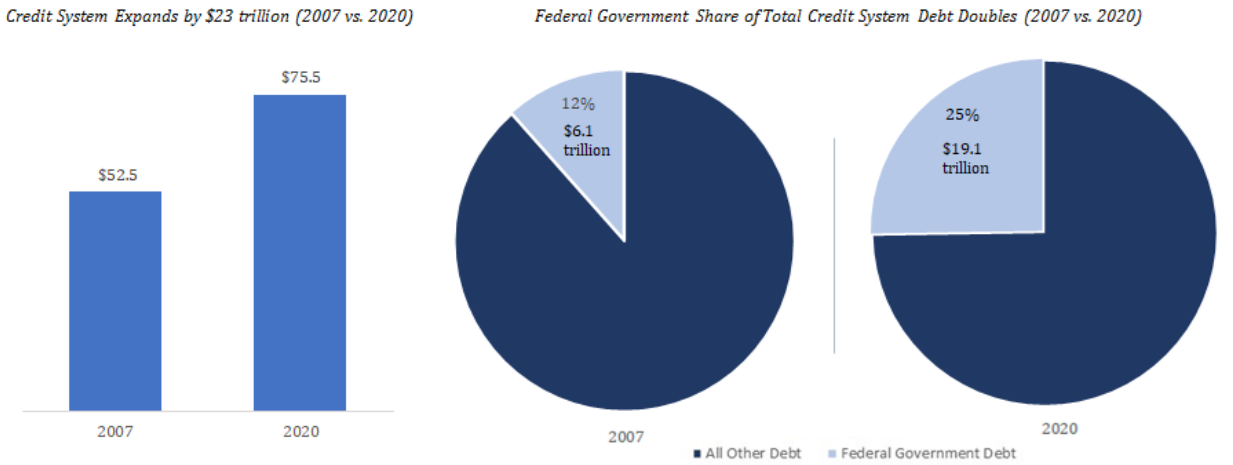






How the effects manifest in the real economy is very complicated, but it does not take any sophistication to recognize the general direction of the end game or its foundational flaws. More dollars result in each dollar becoming worth less, and the value of any good naturally trends toward its cost to produce. The marginal cost for the Fed to produce a dollar is zero. With all the bailouts from both the Fed and Congress, whether to individuals or companies, someone is paying for everything. It is axiomatic that ***printing money (or creating digital dollars) does nothing to generate economic activity***; it only shifts the balance of powers as to who allocates the money and prices risk. It strips power from the people and centralizes it to the government. It also fundamentally impairs the economy's ability to function as it distorts prices everywhere. But most importantly, it puts the stability of the underlying currency at risk, which is the cost that everyone collectively pays. The Fed may be able to create dollars for free and the Treasury may be able to borrow at near-zero interest rates as a direct result, but there is still no such thing as a free lunch. Someone still has to do the work, and all printing money does is shift who has the dollars to coordinate and price that work.

> *"The emitting of paper money by the authority of Government is wisely prohibited by the individual States, by the national constitution; and the spirit of that prohibition ought not be disregarded by the Government of the United States. Though paper emissions, under a general authority, might have some advantages not applicable, and be free from some disadvantages which are applicable to the like emissions by the States, separately, yet they are of a nature so liable to abuse – and it may even be affirmed, so certain of being abused – that the wisdom of the Government will be shown in never trusting itself with the use of so seducing and dangerous an expedient. In times of tranquility, it might have no ill consequences; it might even be managed in a way to be productive of good; but, in great and trying emergencies, there is almost a moral certainty of its becoming mischievous. The stamping of paper is an operation so much easier than the laying of taxes, that a government, in the practice of paper emissions, would rarely fail, in any such emergency, to indulge itself too far in the employment of that resource, to avoid, as much as possible, one less auspicious to present popularity. If it should not even be carried so far to be rendered an absolute bubble, it would at least be likely to be extended to a degree which would occasion an inflated and artificial state of things, incompatible with the regular and prosperous course of the political economy. – Alexander Hamilton, The Writings 590-91.*



The Moon is a Harsh Mistress, by Robert Heinlein

"Gospodin," he said presently, "you used an odd word earlier–odd to me, I mean..."

"Oh, tanstaafl. Means there ain't no such thing as a free lunch. And isn't," I added, pointing to a FREE LUNCH sign across room, "or these drinks would cost half as much. Was reminding her that anything free costs twice as much in long run or turns out worthless."

"An interesting philosophy."

"Not philosophy, fact. One way or other, what you get, you pay for."

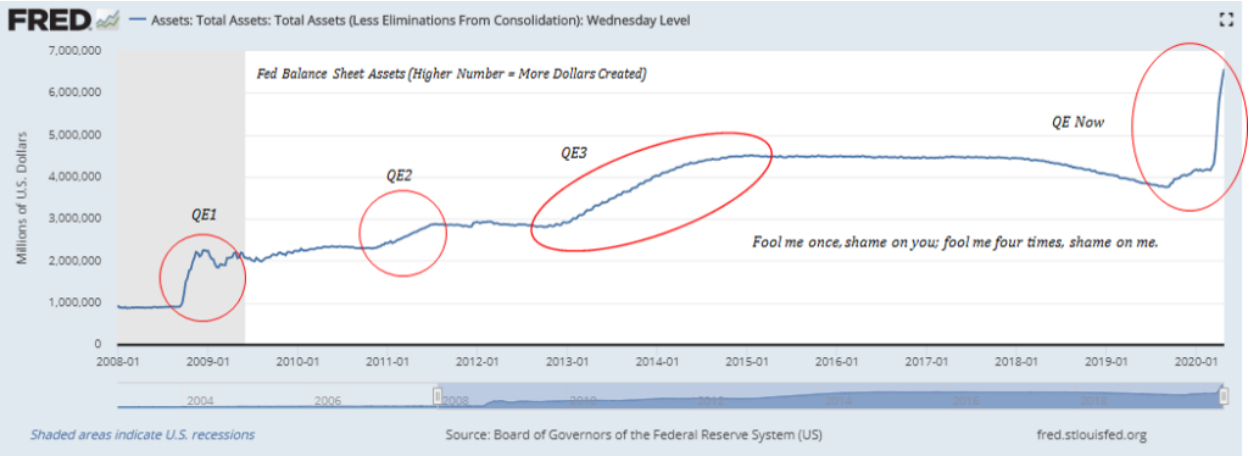
Bitcoin is Common Sense

Among its perceived flaws as a currency, bitcoin is viewed by many to be too complicated to ever achieve widespread adoption. In reality, the dollar is complicated; bitcoin is not. It becomes very simple when abstracted to the least common denominator: 21 million bitcoin; and who controls the money supply: no one. Not the Fed or anyone else. At the end of the day, that is all that matters. Bitcoin is in fact complicated at a technical level. It involves higher level mathematics and cryptography and it relies on a "mining" process that makes very little sense on the surface. There are blocks, nodes, keys, elliptic curves, digital signatures, difficulty adjustments, hashes, nonces, merkle trees, addresses and more.

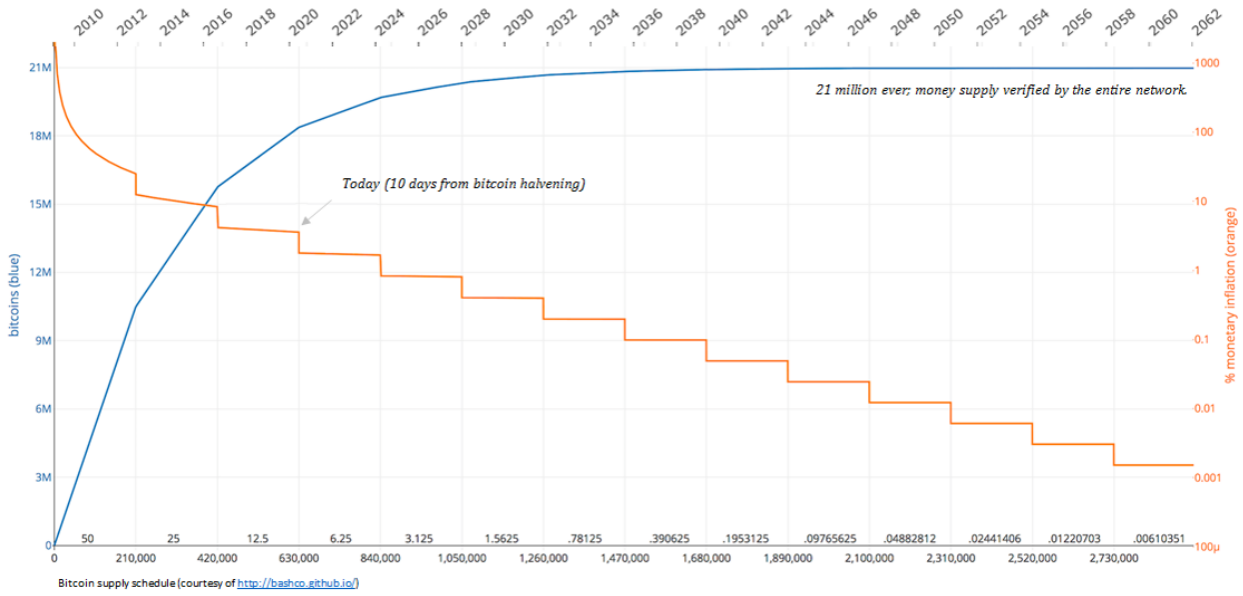
But with all this, bitcoin is very simple. If the supply of bitcoin remains fixed at 21 million, more people will demand it and its purchasing power will increase; there is nothing about the complexity underneath the hood that will prevent adoption. Most participants in the dollar economy, even the most sophisticated, have no practical understanding of the dollar system at a technical level. Not only is the dollar system far more complex than bitcoin, it is far less transparent. Similar degrees of complexity and many of the same

primitives that exist in bitcoin underly an iPhone, yet individuals manage to successfully use the application without understanding how it actually works at a technical level. The same is true of bitcoin; the innovation in bitcoin is that it achieved finite digital scarcity, while being easy to divide and transfer. 21 million bitcoin ever, period. That compared to $2.5 trillion new dollars created in two months, by one central bank, is the only common sense application anyone really needs to know.

Exhibit A – Dollar Supply



Plus Exhibit B – Bitcoin Supply



Equals Exhibit C – Purchasing Power of Bitcoin Relative to Dollars

There is a lot happening in the background, but these three charts are what drives everything. People all over the world are connecting these dots. The Fed is creating trillions of dollars at the same time the rate of issuance in bitcoin is about to be cut in half (see the bitcoin halvening). While most may not be aware of these two divergent paths, a growing number are (knowledge distributes with time) and even a small number of people figuring it out ultimately puts a significant imbalance between the demand for bitcoin and its supply. When this happens, the value of bitcoin goes up. It is that simple and that is what draws everyone else in: price. Price is what communicates information. All those otherwise not paying attention react to price signals. The underlying demand is ultimately dictated by fundamentals (even if speculation exists), but the majority do not need to understand those fundamentals to recognize that the market is sending a signal.

Once that signal is communicated, then it becomes clear that bitcoin is easy. Download an app, link a bank account, buy bitcoin. Get a piece of hardware, hardware generates address, send money to address. No one can take it from you and no one can print more. In that moment, bitcoin becomes far more intuitive. Seems complicated from the periphery, but it is that easy, and anyone with common sense and something to lose will figure it out; the benefit is so great and money is such a basic necessity that the bar on a relative basis only gets lower and lower in time. Self-preservation is the only

motivation necessary; it ultimately breaks down any barriers that otherwise exist.

The stable foundation that underpins everything is a fixed supply which cannot be forged, capable of being secured without any counterparty risk and resistant to censorship and seizure. With that bedrock, it does not require a lot of imagination to see how bitcoin evolves from a volatile novelty into a stable economic juggernaut. A hard-capped monetary supply versus endless debasement; a currency that becomes exponentially more expensive to produce compared to a currency whose cost to produce is anchored forever at zero by its very nature. At the end of the day, a currency whose supply (and derivatively its price system) cannot be manipulated. Fundamental demand for bitcoin begins and ends at this singular cross-section. One by one, people wake up and recognize that a bill of goods has been sold, always by some far away expert and never reconciling with day-to-day economic reality.

With bitcoin as a backdrop, it becomes self-evident that there is no advantage either in ceding the power to print money or in allowing a central bank to allocate resources within an economy, and in the stead of the people themselves that make up that economy. As each domino falls, bitcoin adoption grows. As a function of that adoption, bitcoin will transition from volatile, clunky and novel to stable, seamless and ubiquitous. But the entire transition will be dictated by value, and value is derived from the foundation that there will only ever be 21 million bitcoin. It is impossible to predict exactly how bitcoin will evolve because most of the minds that will contribute to that future are not yet even thinking about bitcoin. As bitcoin captures more mindshare, its capabilities will expand exponentially beyond the span of resources that currently exist. But those resources will come at the direct expense of the legacy system. It is ultimately a competition between two monetary systems and the paths could not be more divergent.

Bananas grow on trees. Money does not, and bitcoin is the force that reawakens everyone to the reality that was always the case. Similarly, there is no such thing as a free lunch. Everything is being paid for by someone. When governments and central banks can no longer create money out of thin air, it will become crystal clear that backdoor monetary inflation was always just a ruse to allocate resources for which no one was actually willing to be taxed. In common sense, there is no question. There may be debate but bitcoin is the inevitable path forward. Time makes more converts than reason.

“You can fool all the people some of the time, and some of the people all the time, but you cannot fool all the people all the time.” – Abraham Lincoln

"These proceedings may at first seem strange and difficult, but like all other steps which we have already passed over, will in a little time become familiar and agreeable: and until an independance is declared, the Continent will feel itself like a man who continues putting off some unpleasant business from day to day, yet knows it must be done, hates to set about it, wishes it over, and is continually haunted with the thoughts of its necessity." – Thomas Paine, Common Sense

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.

Citadels and Pandemics

By Yuri de Gaia

Posted March 25, 2020

An overview of how a citadel would act in case of a global emergency, like a pandemic.

With the ongoing COVID-19 pandemic and a global financial collapse, it is interesting and, often, frightening to watch how various governments react to the event. As covered in ***Perspective Matters***, the spread of the virus is used by opportunistic elites to grab more power. This is not unexpected. At the end of the day, just like the purpose of the police is not to "serve and protect" but rather enforce the law, the purpose of the government is not to provide social services, but to exert control over the population. Any crisis is an opportunity to do so. A question arises, then: How would a citadel deal with such a situation? My thoughts are below.

Asteria's Measures

First and foremost, you must remember that ***Asteria***, our model citadel, is a private for-profit entity that has ***contractual*** obligations before its citizenry (as opposed to an invisible ***social contract*** in nation-states). Therefore, any abnormal measures must be covered in the ***Force Majeure Clause*** of the service agreement. This means that, upon signing up, a prospective citizen gives his consent to such measures voluntarily.

Secure Borders

Being a sovereign entity or, at the very least, a special administrative zone, Asteria has strong borders. In our case, it is an island, so Nature herself provides the necessary separation from the outside world. As walls are not needed, watchtowers and border control posts are enough to secure the city

from intruders. As seen from the examples of Singapore and Hong Kong, city-states, being smaller and more centralized, have the advantage of fast decision making and execution of new directives. In case of a real pandemic, Asteria will have no trouble locking down its borders at a moment's notice. Nobody goes in, nobody goes out.

Quarantine

While quarantine is, arguably, not the best solution for flu-like pandemics, resulting in far more damage to the lives of people than the actual disease might claim, it may be necessary in plague-esque scenarios. Again, the city's small size and efficient governing body is able to make swift changes to day-to-day lives. They do not have to be as harsh as those in Singapore, but you must understand that, when fear is instilled in people's minds, their rational faculties are no longer operational.

Market-Based Solutions

Except for the core services of the citadel, as defined in the contract, the majority of the activities in Asteria are market-based. Free enterprise is what propels the city to new heights at an accelerating pace. This concerns medical facilities and scientific labs. In a genuine ***laissez-faire*** manner, there is no need to wait for a government edict to start working on possible solutions to the pandemic. In light of self-interest and that of the citadel, which is a cherished home, multiple teams will start working on test kits and possible cures as soon as they hear the news.

"Hong Kong, Japan, and Singapore all developed their own tests for Covid-19 as soon as the genetic sequences for the virus were published, and ramped up production of the materials necessary for those tests. (That's a sharp contrast with the US, which still doesn't have enough tests for nationwide use, and may actually be running out of the materials necessary to make them.)"—Wired

Emergency Supplies

As Asteria is a financial success today and cares a lot about the future, it takes care to stockpile at least 3 years' worth of provisions in disaster storage facilities. If the city has to be isolated for prolonged periods, the citizens will have enough food and water to survive. Being an island nation helps procure fresh seafood, of course, but prudent minds do not rely on Just-in-Time logistics.

Emergency Fund

Besides food and water, Asteria's management company is smart enough to have put aside an emergency bitcoin fund. This money allows the city to purchase any goods or services that it may lack during the pandemic. If a test kit or a cure is developed elsewhere, Asteria can use the funds to bid a high enough price to be one of the first in line to receive the product, as is her responsibility before the citizenry. It is not a secret that money talks even when the world is in dire straits.

Escape Plan

In the unlikely situation where the only way to survive is to leave the infected behind, as devastating as it may be, the citadel may enact its emergency evacuation plan. In Asteria's case, the plan involves a fully equipped and stocked-up ***ark***, that can sail the open sea for a few months and even submerge for extended periods.

The longest submerged and unsupported patrol made public is 111 days (57,085 km 30,804 nautical miles) by HM Submarine ***Warspite*** (Cdr J. G. F. Cooke RN) in the South Atlantic from 25 November 1982 to 15 March 1983.—Guinness World Records

Inland citadels may devise other ways of escape, such as by road, tunnels or aircraft.

Bunker

If neither staying in the city or escaping is possible, a bunker space may be the most appropriate option for self-isolation. It may be located underground or built as an artificial structure adjacent to the island.

Nature Does Not Wait

I have written all of this to show that a citadel, being an alternative way of structuring the way we live together, may be a lot more efficient when it comes to scenarios in which fast decision-making is of extreme importance. Just like slow, overly bureaucratic national companies of today have no chance competing with private-enterprise alternatives, nation-states will be at a disadvantage compared to citadels when it comes to acts of God. Nature does not wait for committees with their rubber stamps. When things get serious rapidly, decision-making and action must be swift. An efficiently managed citadel, therefore, would be a better place to be in considering the alternatives.

Cryptocurrencies as Cyberstatism

By Frank Braun

Posted January 6, 2020

2020-01-06 [read as txt or PDF]

Prelude

(Note: Most of this prelude has been put on Twitter before, the impatient reader might want to skip to section Cyberstatism) I have been wondering for a long time why cryptocurrencies in general and Bitcoin especially became so, for lack of a better word, toxic. Maybe it's just my personal experience and that experience is totally subjective, but to me it seems that the level of hostility experienced (mostly) online in Bitcoin is way stronger than:

1. It was in the beginning. I have been "around" Bitcoin since the very early days and I didn't experience it like that at all during that time. It seemed to be more of a collaborative effort driven by the excitement of building something new and potentially revolutionary.
2. The level of hostility which can be witnessed in other tech oriented online communities. Nerds are kind of famous for strongly voiced opinions, especially regarding their favorite tech, may it be an editor, operating system, or programming language.

However, the toxicity level in cryptocurrencies in general and Bitcoin especially seems to be off the charts compared to other tech projects. It seems to be have become almost impossible to have rational discussions about technical details that do not devolve into flame wars.

My first hypothesis for why that is the case was:

Toxicity is the consensus mechanism in Bitcoin.

The reasoning being that while proof-of-work is a great mechanism to reach consensus in the distributed ledger for **already agreed** upon rules, it is terrible to reach consensus for **rule changes**.

If not most of all miners and users agree on a rule change it will lead to a fork.

Forks lead to a fracturing of the user base **without** solving future conflicts. The BTC/BCH fork was such a case. The BCH/BSV gives empirical evidence that a fork doesn't solve that problem permanently.

Forks are economically bad, because they lead to a fracturing of the user base and developers, bring uncertainty for new and existing users, etc.

So basically the only good rule change mechanism Bitcoin has is to reach nearly 100% consensus between miners and users **upfront**, which makes it extremely hard to make even very desirable upgrades.

This solidifies the Bitcoin protocol and makes it attackable by altcoins (in terms of additional features).

It has been argued that a solidification of the Bitcoin protocol is not necessarily a bad thing, especially given the "digital gold" and Bitcoin as a store-of-value narrative.

So an economically sound consensus mechanism (for rule upgrades / governance) seems to be toxicity.

Toxicity keeps the community together and bashes all outsiders (for example, this leads to terms like "Bcash" and "shitcoins").

However, toxicity alienates outsiders and prevents upgrades, making Bitcoin effectively the orthodoxy of cryptocurrencies.

So either the Bitcoin protocol is good enough as it is to build innovation on top of it (there will likely not be any major changes to the protocol) or it will be out-competed in terms of features.

Granted, given Bitcoin's first mover advantage, brand recognition, and its position as the major cryptocurrency and default trading pair on most exchanges might give Bitcoin a position which is uncatchable far into the future.

Newer cryptocurrencies like Decred put a consensus mechanism in place which is extremely fork resistant (see Detailed analysis of Decred fork resistance), which might be the reason why the discussions over there seem to be much more civil, they actually can resolve disagreements without a fork.

But it might also be that it's just because their community and position in the market is much smaller.

Cyberstatism

The argument above might explain parts of the picture, but further discussing and thinking about the problem let me come to the following, for a libertarian rather uncomfortable, conclusion: *Cryptocurrencies are a form of Cyberstatism.*

Let me try to explain what I mean by that phrase.

Cryptocurrencies like Bitcoin are a form of Fiat money in the sense that they create money "out of thin air" which doesn't have intrinsic value to begin

with. Granted, most cryptocurrencies do not suffer from the inflation problem of government fiat money (cryptocurrencies usually have a fixed monetary supply) and energy has to be expended in order to "print" them (through mining).

However, cryptocurrencies like Bitcoin lack intrinsic value when they are started. The famous Bitcoin pizza purchase is often viewed as the point in time where Bitcoin switched from being a curiosity to becoming useful and valuable as a medium of exchange.

If you look at cryptocurrencies from the lens of fiat money, different cryptocurrencies competing with each other could be viewed as a zero-sum game. They are all competing to become "cybermoney" (a term from The Sovereign Individual), just like states compete over a fixed amount of available ***territory***.

If the market for cybermoney is fixed, this is a zero-sum game and competing cryptocurrencies indeed show signs of competing states.

Politics becomes the main mechanism of resolving conflicts, not competition of different products on a free market.

Coins forking off become secession movements and are fought strongly as such (e.g., BTC/BCH and BCH/BSV).

People heavily invested into certain coins (emotionally and/or financially) start to behave like nationalists, fighting for ***their*** coin and ***against*** the other coins. Financial investment only makes that a stronger force, because it makes economic sense (if the coins "captures" more territory the value of the investment will go up).

Like with states, the biggest player often becomes the biggest bully…

Conclusion

This is just a theory and I'm sure I will get my fair share of hate for it. If, however, there is some truth to the argument I'm wondering what the conclusion is, given that I find it rather worrisome from a libertarian perspective.

First of all, the competition to become "cybermoney" is **not** a zero-sum game. The real competitor is government-issued fiat money and upcoming state- and corporate-issued cryptocurrencies like Facebook's Libra. That's where the actual war is fought and where it is determined if the world will see an alternative to fiat and these centrally controlled coins. Since there is a "war on cash" going on, there seems to be a limited amount of time left to establish one or more decentralized cryptocurrencies as a valid alternative **for payments**.

Furthermore, exchangeability between different cryptocurrencies independent from centralized exchanges is of paramount importance. The Decred DEX and Bisq are very important steps in that direction. What is also needed is a wider availability of over-the-counter exchanges that allow to trade cash for crypto in person.

If all cryptocurrencies can be easily exchanged for one another in a decentralized fashion, they can compete with each other more like different products on a free market and form a “cyberbloc” against the real enemy. There is no need to look at the competition between different cryptocurrencies as a zero-sum game.

Given the two, focus on the real competition and better exchangeability between different cryptocurrencies, it might be possible to make a real dent into the system of government issued fiat money.

Do you like my work and want to give back?

Donate bitcoin: 3FguRzVXe24cicayb2tmVnHVu4Sp1rULNC

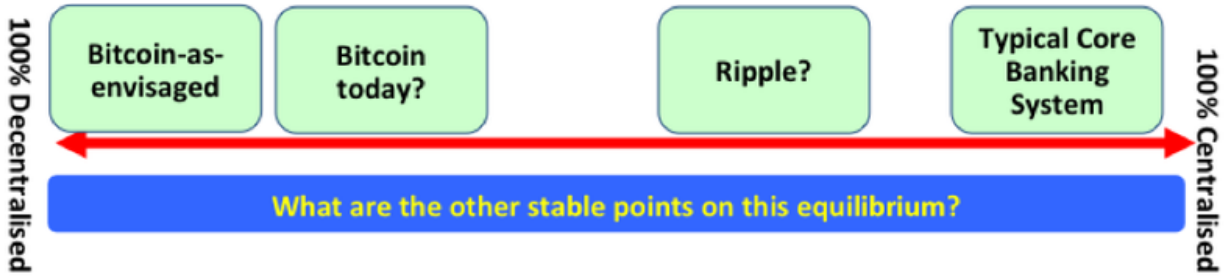
Few Words on Decentralization and Anonymous Payments

By nopara

Posted May 6, 2020

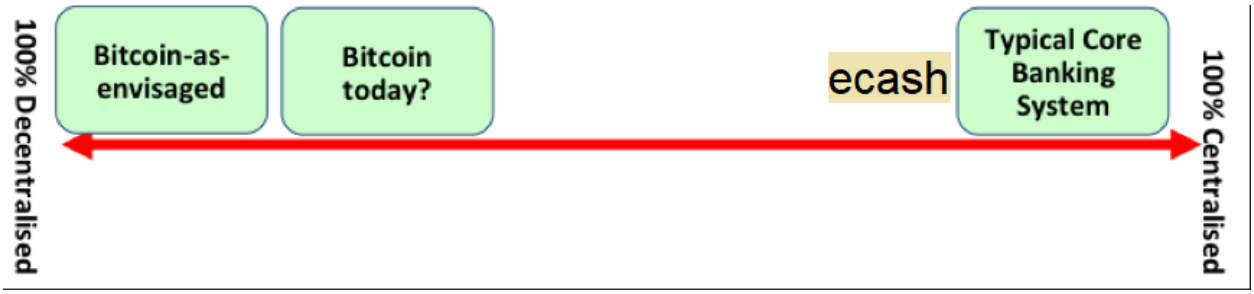
Something is centralized and something else is decentralized. Such binary thinking is prevalent in the Bitcoin community. Here I'd like to present a scale that describes reality in a better way. Our contenders are: **Legacy Banking System**, **Chaumian E-Cash**, **Wasabi Wallet**, **JoinMarket, Bitcoin,** and **Bitcoin-as-envisaged.**

I recall an article that brainstormed on a decentralization scale in the context of payment systems. I am intending to do the same in the context of anonymous payment systems. The article can be summarized with the following depiction:



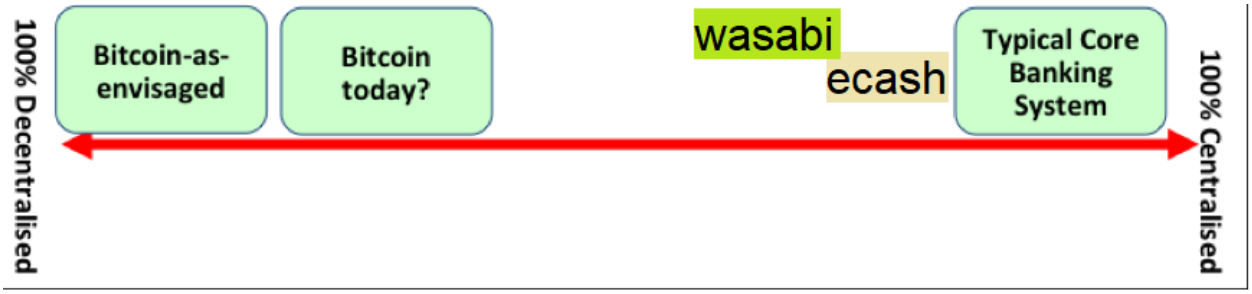
Chaumian E-Cash

Chaumian E-Cash (shall I say as-envisaged?) is a centralized anonymous payment system. I argue calling it centralized does it a disservice, because it is more decentralized than our legacy banking system. While in the legacy banking system the information of who pays who is centralized, too, in ecash it is not the case. Only the receiver and the sender of the payment knows who pays who. While the data is (not always), the information isn't stored in a central location, like in the traditional banking system. This is important, because an ecash bank cannot pinpoint a specific user to steal its money, which increases its censorship resistance. There just isn't as many things to censor.



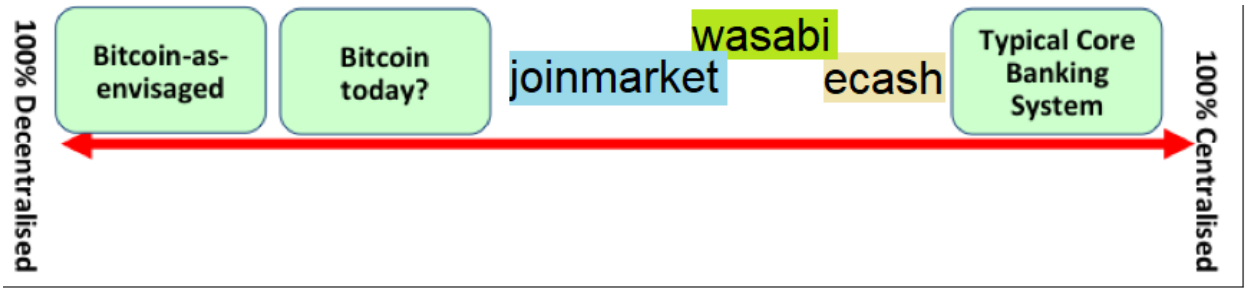
Wasabi Wallet

Wasabi Wallet is a Bitcoin wallet that uses Chaumian CoinJoin to bring privacy for its users. The main difference between ecash and Wasabi is that the latter cannot steal funds of its users. The users have complete control over their money, thus it decentralizes security. Thus it's more decentralized than an ecash bank.



JoinMarket

JoinMarket just like Wasabi also utilizes a CoinJoin protocol. However Wasabi uses a server, called the Coordinator, which has more responsibilities than JoinMarket's server, which simply acts as a bulletin board. For example Wasabi coordinator could potentially blacklist UTXOs from participating in the mix. In fact this is by design, it's doing it all the time as this is how Denial of Service protection filters out the malicious actors. Thus the argument is made the JoinMarket is more decentralized than Wasabi Wallet.



Bitcoin vs Bitcoin-as-envisaged

While compared to JoinMarket Bitcoin does not require a bulletin board to work, it isn't as decentralized as we would like it to be, since the dream decentralization of Bitcoin would be if every single Bitcoin user would be also a Bitcoin miner. But even that's not ultimate decentralization. **The ultimate decentralization would be if every single person on this planet would have equal chance of mining the next block in the Blockchain and no one would ever learn payment information unless they were authorized to do so by the transacting parties.** But even if we'd reach this novel goal, we'd surely encounter terrific scaling issues after space colonization.

Nuances

I'm going to destroy everything I built up so far.

In this article I showed you why calling things centralized and decentralized is more often a rhetoric rather than an argument and presented you a more accurate model: a scale of decentralization. In this section I'm going to hopefully convince you that even this scale of decentralization is a wrong model that suffers from a number of nuances that I conveniently skipped through.

- Could one make a case that data mining payment information from the Bitcoin blockchain is easier than figuring out anything about Chaumian e-cash payments, thus the latter has a more decentralized way of handling payment information? "Chaumian E-Cash Analysis Companies" will never emerge, but "Blockchain Analysis Companies" do have a role to play.
- The peer discovery of Bitcoin is another rabbit hole I didn't want to go into.
- Where would you put on the scale, services like Blockchain.info's SharedCoin and Samourai Wallet where a central entity learns everything? The payment information is centralized there, so they would have a place behind Wasabi, however in ecash the payment information isn't centralized, so would you put them behind ecash, too? Or you'd prefer the security aspect of centralization, as in these schemes the security is decentralized compared to ecash.
- Where would you put Traditional Bitcoin Mixers? They'd obviously be between ecash and legacy banking, because not only the payment information is centralized, but also the security aspect. But do they win the decentralization game against traditional banks?
- How about Bitcoin exchanges or Bitcoin casinos? Is there any difference between them and Traditional Bitcoin Mixers? Is the fact

that the latter does not intend to store bitcoins only tunnel them through their system makes it more decentralized?
- There's also a rabbit hole on the information asymmetry of JoinMarket. There the taker of the CoinJoin learns the mapping so in this regard is it less decentralized than Wasabi and ecash? Oh, wait this gets more complex, the takers of JoinMarket are decentralized in the first place, so does learning the mapping even matter?

Conclusion

Decentralization a meme. In practice it's a nuanced topic and not at all a zero sum game.

Tweetstorm: The 4th Bitcoin Epoch

By John Vallis

Posted May 7, 2020

The 4th Bitcoin epoch, and you. A thread. 1/23

1/ Pumped for the halving? I sure as shit am. It's an important occasion, marking the next step in bitcoin's inevitable march to becoming not only the hardest money ever, but the first instantiation of objectively verifiable absolute scarcity that humanity has ever engaged with.

2/ As such, each step in this process, and in particular the early ones, are a big deal. If demand remains constant, and supply is cut, there should be upwards pressure on price. Happy days! But this is not the only story here.

3/ As many who have engaged with bitcoin have noticed, bitcoin changes you. Of course, as everyone comes at bitcoin from a different perspective, the changes experienced are not uniform, but there are many similarities.

4/ What are these changes? Some include improving ones health/fitness, being more productive, reducing waste or excess, studying/learning more, dropping negative relationships, starting a family, saving more, thinking longer-term, challenging assumptions, gaining confidence..

5/ ..accessing greater energy and enthusiasm, being more hopeful for the future, connecting with more like-minded individuals, taking more personal responsibility, just to name a few.

6/ These are significant lifestyle changes, not to be dismissed casually. From an evolutionary perspective, these changes could very well be making those who adopt them more 'fit'. Put another way, bitcoin may indeed be accelerating human evolution.

7/ Wow. But what is it about interacting with bitcoin that inspires such changes? Tough question. But it seems that as we engage with it, and the more we understand it, the more we begin to realize what it represents.

8/ That is to say, recognizing the implications of its inherent properties, we begin to change how we see the world, and thus how we see ourselves in reference to it. This is powerful, as how we see ourselves contributes greatly to who we become.

9/ It's hard to say why bitcoin's properties inspire the particular changes they do. Is it just because we are interacting with the concepts of scarcity, trust, immutability, freedom, security etc. in a way we never have before? Perhaps.

10/ But this is the halving after all, so let's focus on scarcity. What kind of affect should we expect from encountering absolute scarcity for the first time?

11/ This is such a dramatically new concept for our consciousness to contend with, that it's hard to imagine it wouldn't fundamentally shift our perspective in some (or several) ways.

12/ So if bitcoin's properties are changing us, despite not knowing exactly why or how, what then should we expect when bitcoin becomes more scarce? The obvious answer, is that we should expect to see a commensurate change in ourselves too.

13/ Though this process is far from fully understood, I'm going to speculate that as bitcoin 'hardens', so too shall bitcoiners.

14/ Our conviction, determination, focus, energy, passion, enthusiasm, purpose, and desire to understand and engage this thing will all 'harden', and the behavior changes that have been inspired by bitcoin already will continue to compound.

15/ What's my point with all of this? I guess it's to say that the missing half of the 'halving story', is us!

16/ What if the halving is not just an inflection point for bitcoin's price, but also for the process of our becoming? A point that represents a very specific shift from the person you were in the last four years, to the one you will become over the next four?

17/ For hardcore bitcoiners, this change will likely happen regardless of whether we decide to recognize it or not, as bitcoin will continue to assert it's nature through us. Hwvr, as is often true, I think there is even more to be gained by consciously engaging in this process.

18/ Bitcoiners represent the tip of the spear in what is ultimately a revolution in human action, guided by those behaviors which bitcoin either permits or prohibits.

19/ Whether we like it or not, we are living proof of the merits of this protocol for improving the lives of individuals everywhere.

20/ I'm not here to tell you how to act, that's entirely up to you. I guess I'm just asking, if this revolution isn't about changing how we can and desire to act and interact, then what is it about?

21/ And if we believe it is about that, then those occasions (halvings) which represent a step change in how we are influenced by this protocol, are probably significant events for each of us.

22/ It's a coming of age of sorts. The 3rd epoch was fun, but nothing compared to what the 4th epoch will be, and who we will necessarily become to meet the challenges and opportunities which it represents. Strap in Bitcoiners, and Happy Halving! LET'S GOOOOOOOO!

Where are the coins?

By Fabian Jahr

Posted May 8, 2020

EDIT: An earlier version of this post linked to a BitcoinTalk post that speculated on the cause of BIP30 being the introduction of LevelDB. Pieter Wuille kindly informed me that LevelDB was introduced after BIP30 occured , which means that post was definitely false.

The third Bitcoin halving is coming up quickly as I write this. I thought this would be a great time to write down what I learned about the amount of BTC in the UTXO set. Everyone is talking about coin supply at the moment but detailed, granular information on this topic seemed to be hard to find. Strangely, I only found this excellent StackExchange answer by Pieter Wuille very late into writing this article and there is a lot of overlap. If you like this post I recommend you read Pieter's as well since it basically approaches the same question from the angle of future total coin supply and it's a quick read.

My insights on the current coin supply and the UTXO set mostly stem from my work on #18000. There I am working on an index for coin statistics with the main goal to make the RPC command `gettxoutsetinfo` faster. Even much earlier before starting the work on #18000, I remember being thrown off by `gettxoutsetinfo` because of the `total_amount`. To my surprise, it was a very crocket number and that has not changed. At the time of this analysis, the blockheight is `629038` and the `total_amount` reported is `18362804.82079165`.

This is weird because one of the first things most people learn about Bitcoin is that supply is pre-determined through the inflation schedule. It prescribes that the block rewards were 50 BTC initially, then 25 BTC, currently still 12.5 BTC. So the number should be evenly divisible by 12.5 theoretically but it is clearly not. In short, the reason for that discrepancy is that `gettxoutsetinfo` does not report the theoretical number of the inflation schedule but the actual number of unspent coins that the node knows about. Among others, the most intuitive reason for this is to save disc space. If these unspendable outputs would not be removed they could bloat the UTXO set and take up disc space on every full node, forever.

The UTXO set

I want to briefly recap what the UTXO set (unspent transaction output set) is and why it exists to make a bit more sense of what is coming next. You probably know that Bitcoin has a blockchain and that every (fully-validating)

node in the network is validating the whole blockchain. Simply put, the UTXO set is both the product of that validation process and helps speed it up as well. Each Bitcoin transaction has outputs and all non-coinbase transactions consume previous outputs as inputs. Outputs can only be spent once and need to be spent in full. If that is not the case a transaction, and a block that contains such a transaction, is invalid. For every valid block in the chain, all the unspent outputs created in a block are written into a database, the UTXO set. At the same time, every output that gets consumed by a transaction in a block as an input is considered spent and gets removed from the UTXO set. The UTXO set helps to speed up the transaction validation processes considerably since it gives a very quick overview of all the outputs that are valid and can be spent.

Now, the RPC `gettxoutsetinfo` iterates over all these unspent outputs in the database and aggregates the total amount. One might say, `getutxosetinfo` would have been the better name to match today's widely used terminology. But as we already established earlier, there seems to be some kind of a 'leak' since it reflects fewer bitcoins than expected.

So how many coins are lost exactly and where are they? During my initial search for the answer, I only found some high-level ideas but not a detailed analysis of this. That's what I am trying to provide here.

The amount of missing coins

The Bitcoin supply schedule started with 50 BTC for every new block, with the reward halving every `210,000` blocks. That means we should currently have:

```
210000 * 50 + 210000 * 25 + ((629038 + 1) - 420000) * 12.5
= 10500000 + 5250000 + 2612987.5
= 18362987.5 BTC
```

Where does the +1 come from? It's the Genesis block which is special because it is hardcoded into the codebase and located at index 0 of the blockchain. It also has a coinbase reward. So we are missing exactly:

```
18362987.5 - 18362804.82079165 = 182.67920835 BTC
```

Finally, where did these coins go?

Genesis Block

We just added it in with the +1 in the last paragraph and now we are taking it out again. Well, this post is about going into the details so it would be wrong to ignore this. The Genesis block has a coinbase reward but it is not spendable, and that's why it also not part of the UTXO set. It is not spendable because Satoshi's implementation is skipping the Genesis block in validation, meaning it is also not adding the coinbase output to the UTXO set. They

probably did this because block validation generally includes checking that the block has a valid ancestor, the previous block in the chain, as well. And if they had not skipped validation altogether they would have needed to code a special exception there which would have been more difficult. But that is speculation.

```
182.67920835 - 50 = 132.67920835 BTC
```

Status: **132.67920835 BTC still missing!**

BIP 30

BIP 30 describes a bug from the early days of Bitcoin. It turned out that there was no measure against duplicate transaction ids (TXIDs) in the earlier versions of Bitcoin. This was probably overlooked because a normal user can not simply create a transaction with a specific TXID. Each transaction depends, among other things, on the TXIDs of the outputs it spends. Since the TXID is a SHA256 hash and the previous TXIDs make it's content unique, achieving a duplicate id would require the user to find a hash collision in SHA256, breaking one of the main security assumptions in Bitcoin itself.

But there is an exception to that. Coinbase transactions don't have parent tx's, so their input is all zeros, which means the content of the SHA256 hash is not necessarily unique. So, unfortunately, a duplicate coinbase transaction id used to be both possible and valid and it happened twice in bitcoins history before it could be fixed:

- Block 91722 coinbase TXID is repeated in Block 91880
- Block 91812 coinbase TXID is repeated in Block 91842

The implementation of BIP 30 in the Bitcoin Core code base still has the overriding blocks hardcoded into the codebase.

The reason why this is a problem may not be completely obvious but the term 'transaction ID' gives a hint. TXIDs also serve as the identifier for coins that are stored in the UTXO set. In this case, an existing output of the last coinbase got overridden by the next tx with the same TXID.

As a fix, transactions with TXIDs that are already present in the UTXO set, i.e. that have existed before and still have unspent outputs, are declared invalid. TXIDs can reappear but only after all outputs have been spent. But the rewards of the two overridden coinbase transactions mentioned above were lost forever. Since the block subsidy was 50 BTC at the time, that's 100 BTC lost.

```
132.67920835 - 100 = 32.67920835 BTC
```

Status: **32.67920835 BTC still missing!** By the way, the more long term fix for this issue was implemented with BIP34. It prescribed the introduction of a

new block version (v2) which required coinbase transactions to start with the height of the current block. Since this part made coinbase transactions unique it is now virtually impossible to introduce a duplicate coinbase transaction by accident.

OP_RETURN

For somewhat more experienced bitcoin users this opcode might come to mind first when they think of unspendable or 'burned' outputs. Producing those is the whole purpose of OP_RETURN. Yes, the use of OP_RETURN means that the output is automatically marked invalid and cannot be spent anymore. Because of that, these outputs are also not included in the UTXO set.

Looking at the blockchain I found `3.72417931 BTC` have been "burned" with the use of OP_RETURN. That number still expands steadily, by the way, so the OP_RETURN opcode is still frequently used. I imagine services like OpenTimestamps are responsible for most of it today.

```
32.67920835 - 3.72417931 = 28.955029039 BTC
```

Status: **28.95502904 BTC still missing!**

Script too large

Another reason for an output to be marked as not spendable in the future is a script size that is too large. The threshold is defined in `MAX_SCRIPT_SIZE` and set to 10000 bytes.

I did not find evidence of any specific cases of this, but since the rule was explicit in the code, I figured I should look into it. But it appears there were no coins that were excluded from the UTXO set specifically for this reason.

Status: **28.95502904 BTC still missing!**

Unclaimed Miner Rewards

This may sound weird at first, but there is a possibility that miners don't claim their full block reward in a block they mined. The mining reward in the coinbase transaction is not checked against a specific value but rather to not exceed the valid block reward. So a block with a reward smaller than the sum of the current block subsidy and the total fees would still be valid. But for a miner who has mined a block with a smaller reward, there is also no way to claim these funds later. After the block is included in the blockchain these coins are also lost forever and will never appear in the UTXO set.

Why would a miner do this? I can not think of any good reason, it seems much more likely that this is always the result of a bug.

Thankfully Pieter Wuille lists some known incidents in his StackExchange answer saving me from writing more custom code and hours of research:

- Block 124724 tried to intentionally claim 0.00000001 BTC less than allowed, but accidentally also failed to claim the fees, losing 0.01000001 BTC.
- Between block 162705 and block 169899, 193 blocks claimed less than allowed due to a bug, resulting in a total loss of 9.66184623 BTC.
- Between block 180324 and block 249185, another 836 blocks claimed less than allowed, resulting in a total loss of 0.52584193 BTC.
- Block 501726 had no transaction outputs (except a 0-value commitment), losing the entire 12.5 BTC subsidy.
- Block 526591 didn't claim half of the block reward, losing 6.25 BTC.

Pieter describes a loss of `28.94768817 BTC` in his answer. I found a few more satoshis that miners lost, most likely by miscalculating the total fee. My analysis showed `28.95502904 BTC` went missing this way, which is `734087 sats` more than Pieter accounted for.

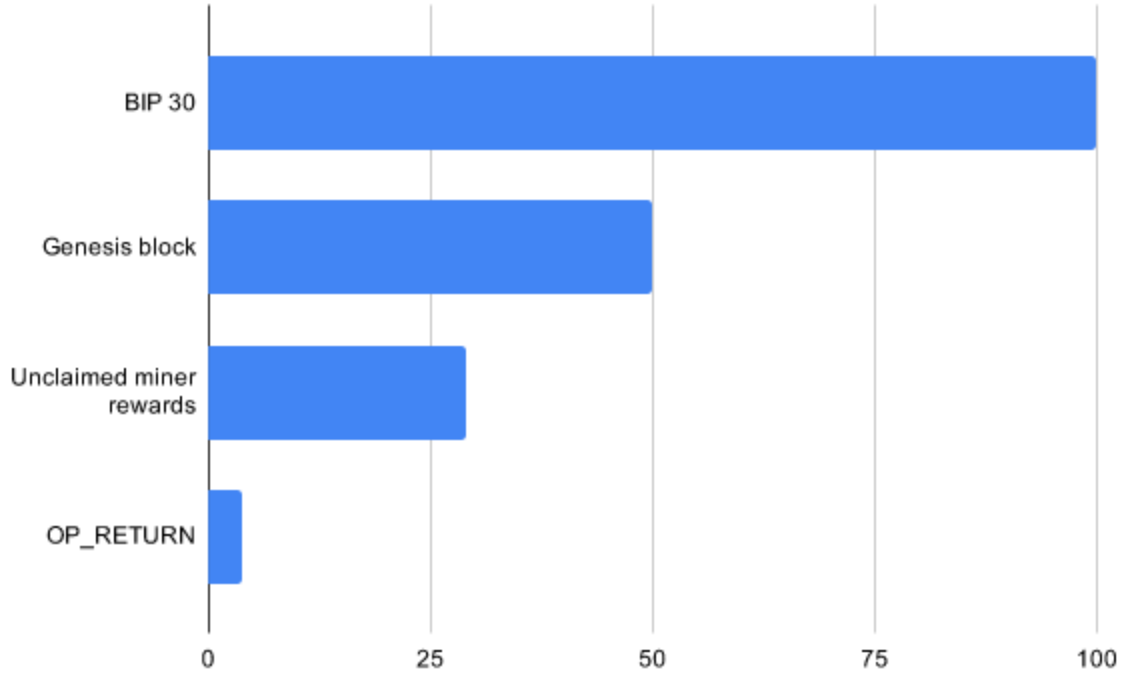
```
28.95502904 - 28.95502904 = 0 BTC
```

Status: **0 BTC still missing!**

Other unspendable outputs

These are not all the outputs that are known to be unspendable. There are several more types of outputs that are impossible to spend (see the list in this BitcoinTalk post by user DeathAndTax for example). However, these are still included in the UTXO set. An update on the numbers of these other unspendable outputs would certainly be interesting as well.

Final thoughts



Pfew, I am really happy that worked out evenly at the end ;) So now you know why the `total_amount` is not the number you probably expected at first. I found it very satisfying to explore these internals of Bitcoin Core, especially because it had been an open question for me from the very first time I spun up a node. I hope you enjoyed reading this post as much as I enjoyed figuring these things out and writing them down.

Special thanks to James, Max, Freerk, Felix and Elaine for reading and providing feedback on an earlier version of this post.

You can find the custom code I used to collect these numbers here.

How Does Quantitative Easing (QE) Affect the Price of Bitcoin?

By Pedro Febrero on Quantum Economics

Posted May 11, 2020

With QE on the rise, is Bitcoin poised to fill the gap?

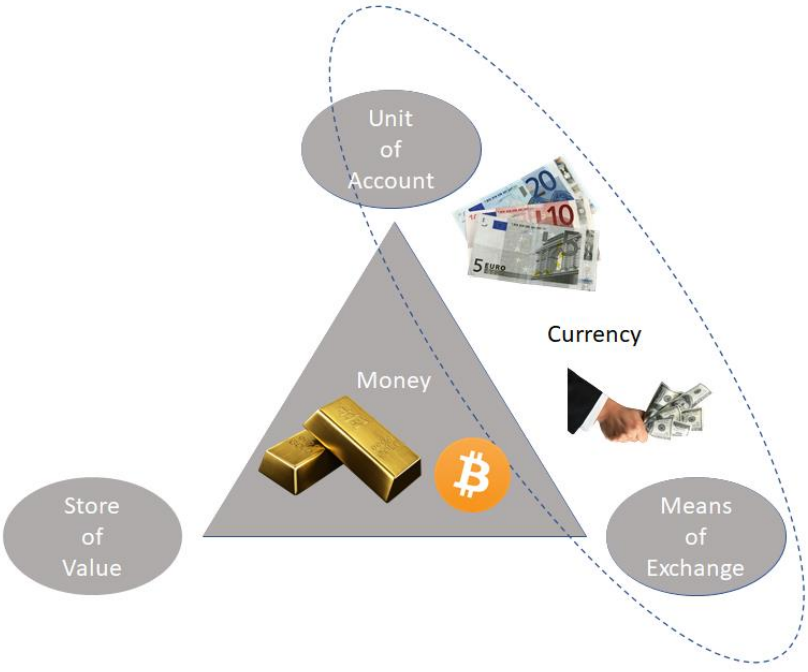
Since the 2008 financial crisis, expansive monetary policies have barely kept the struggling economy alive. With infinite QE on the rise, the only solution in sight seems to be a return to a hard money standard. Will Bitcoin fill in the gap?

In this article, we aim to explore the impact that quantitative easing (QE) has on the price of Bitcoin. To achieve that goal, we will first look into the effects of massive currency creation, how QE works and why it's so dangerous in the long-term.

Finally, we'll connect the dots by showing how QE and other expansive monetary measures have influenced the price of traditional assets and commodities, including bitcoin. We'll conclude the piece by sharing our thoughts on why the return to a hard-money asset is the long-term solution to this particular economic crisis.

How money differs from currency

Image: Author



A great starting point for our analysis is to discuss the key differences between money and currency. Since we'll be looking into topics such as hard money and QE, we should, beforehand, briefly explain what makes money different from currency.

Let's begin by defining what hard money is.
Investopedia defines hard money as _"a physical

currency, such as coins made out of precious metals including gold, silver or platinum." _A better definition could perhaps be a form of money that requires a significant amount of energy to produce.

To make the topic more understandable, we've developed the picture above. It visualizes what money is (or should be): an asset or commodity, like gold and Bitcoin, that grants its holders the power to store value, exchange value and measure value. Unlike currency, which is great to exchange and measure value, one of money's most important traits is its ability to store value across long periods of time.

A very good example follows. In ancient Rome, an average centurion soldier would get paid just over 1,077g of gold per year (in sestertii equivalency), which in today's terms means close to $61,000. In terms of purchasing power, two months' salary was enough money for a centurion to acquire one year's worth of bread, much like today, according to some researchers.

Hence, we can conclude that gold has maintained purchasing power since the ancient Roman times.

If we wonder what characteristics allow money to store value during very long periods of time, we come to the conclusion it's mainly due to skin in the game and proof-of-work. In other words, any commodity that desires to be treated as money should be quite hard to acquire (skin in the game) and should have a limited supply, granted lots of energy is required to mint a new unit (proof-of-work). That's why gold coins and units of bitcoin are treated as hard money, since they are kinds of currency that are rare and difficult to produce.

Unfortunately, since 1973, the equivalence or standard between currency and money has deteriorated. With the introduction of a global fiat standard, the relationship between the U.S. dollar and gold was relinquished. Effectively, all fiat currencies use the greenback as reserve money, even though those same dollars could be printed at any time by a central bank.

The problem is when economies mix the concept of money and currency. As it is discussed in money theory, base currency should only inflate as much as the real economy requires, and credit money should expand based on hard money reserves. However, since the world's reserve currency is the U.S. dollar, not gold, central banks could incur a massive expansion of credit through low reserve requirements, simply because paper, or digital numbers on a ledger, aren't that hard to produce.

Hence, the world entered a downward spiral of nontraditional monetary policies, including quantitative easing, zero interest rates and negative interest rates. The allocation of capital was displaced from the real productive

economy into the financial economy, making waves for a period of highly leveraged stock markets.

What is the relation between fiat currency, QE and financial markets?

This chart shows the S&P 500 and the Dow Jones Industrial Average, 2008–2020 (Source: https://www.tradingview.com/x/O5sPX7vu/)

QE is a brand new monetary policy introduced by central banks worldwide in response to the 2008 financial crisis.

Investopedia describes QE as the following:

"Quantitative easing (QE) is a form of unconventional monetary policy in which a central bank purchases longer-term securities from the open market in order to increase the money supply and encourage lending and investment. Buying these securities adds new money to the economy, and also serves to lower interest rates by bidding up fixed-income securities. It also greatly expands the central bank's balance sheet"

To give another perspective, we see QE as the tool that allows central banks to purchase assets for free in order to indirectly sponsor corporations into spending. QT, on the other hand, translates to quantitative tightening. This is the exact opposite process, where central banks aim to decrease the assets held, which normally places downward pressure on asset prices.

Without the possibility of creating infinite currency and artificially suppressing interest rates, it would be impossible for central banks to finance their own economies directly. That means government spending would be considerably more restricted to actual money reserves and economic growth,

and malinvestment would be costly, since there would be no direct way to bail out failing corporations.

In sum, if governments can't debase a currency, they can't print infinite currency, meaning bailouts can only happen through costly debt or increased taxes on income, products or companies. Therefore, had QE not been invented, companies would likely be more careful and would be less likely to misallocate their capital.

Since QE has begun, the global asset markets have skyrocketed in price. The above chart shows precisely what we mean. Did you notice how after each QE round (pink columns), the markets tend to appreciate in value?

From November 2008 to November 2010, between QE 1 and QE 2, both the SPX and the DJI increased, on average, close to 60%. Additionally, from QE 2 to QE 3, which started in September 2012, both markets rose more than 20%.

However, the biggest appreciation took place between September 2012 and 18th February 2020. Both indices increased over 130%, an astonishing accomplishment according to price history. Not surprisingly, during the period of QT, from 2018 until early 2019, both the SPX and DJI had the exact opposite behaviour. Both indexes dropped substantially, between 16% to 20% respectively.

Bitcoin was born amidst the financial crisis, in January 2009, and has gained substantial value since its inception. Undoubtedly, the easing of cash to purchase financial assets may have played a significant role in the optimism surrounding BTC, as we'll discuss near the end.

Nevertheless, before we dive into Bitcoin, we shall look into how QE influenced the markets in Europe and the United States. Only after we evaluate the impact of QE on asset prices and how it relates to each jurisdiction's Gross Domestic Product (GDP), we may begin to unravel the answer we seek.

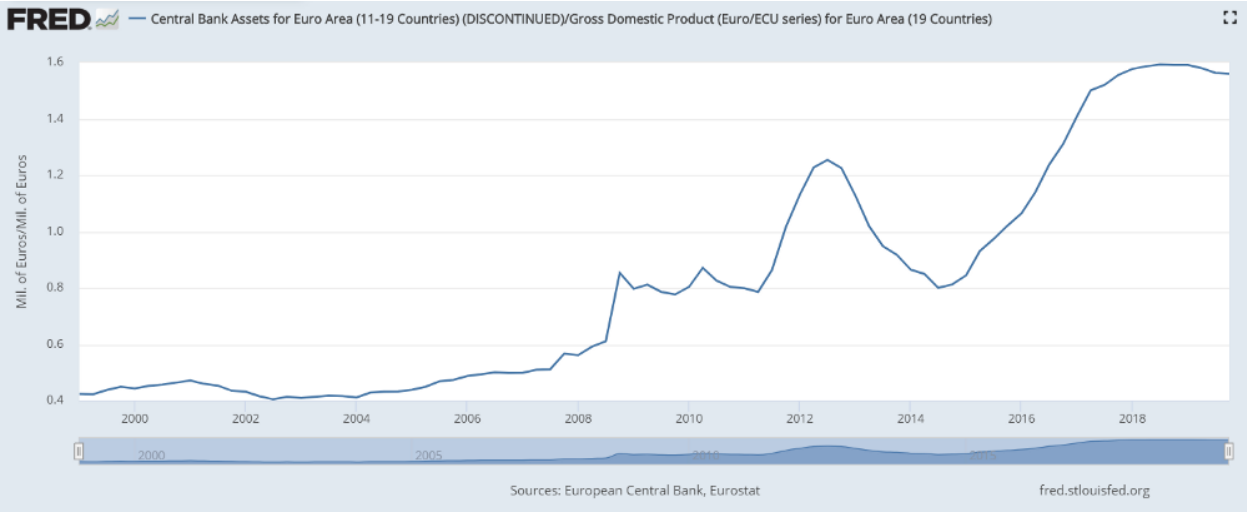
Additionally, in order to make our analysis easy to understand, we'll look into the effects of the Fed's and the ECB's money printing on consumer behaviour by comparing the velocity of money to its total supply.

Hopefully, by the end, we'll be able to extrapolate the short-term and long-term effects of QE and other expansive monetary policies on the price of Bitcoin.

Now, we'll start by looking into the ECB's QE programme, immediately followed by the Fed's.

Let's have some fun, shall we?

European Central Bank QE



This chart shows the total assets held by the ECB.
(Source: https://fred.stlouisfed.org/series/ECBASSETS#0)

First, let us dive deep into QE, by looking at the European Central Bank's (ECB's) QE program.

Much like in the United States, its QE measures started amidst the 2008 Financial Crisis. The ECB's first round of purchases took place in Q2 2008, and the institution acquired assets worth more than 20% of the European Union's total GDP.

A few years later, in late 2011, there was a second round of massive purchases. Essentially, from Q2 2011 until Q2 2012, the ECB bought assets worth 50% of the EU's total GDP.

By the beginning of 2013, the assets accumulated by the ECB were worth more than 120% of the entire eurozone GDP.

But wait, there's more.

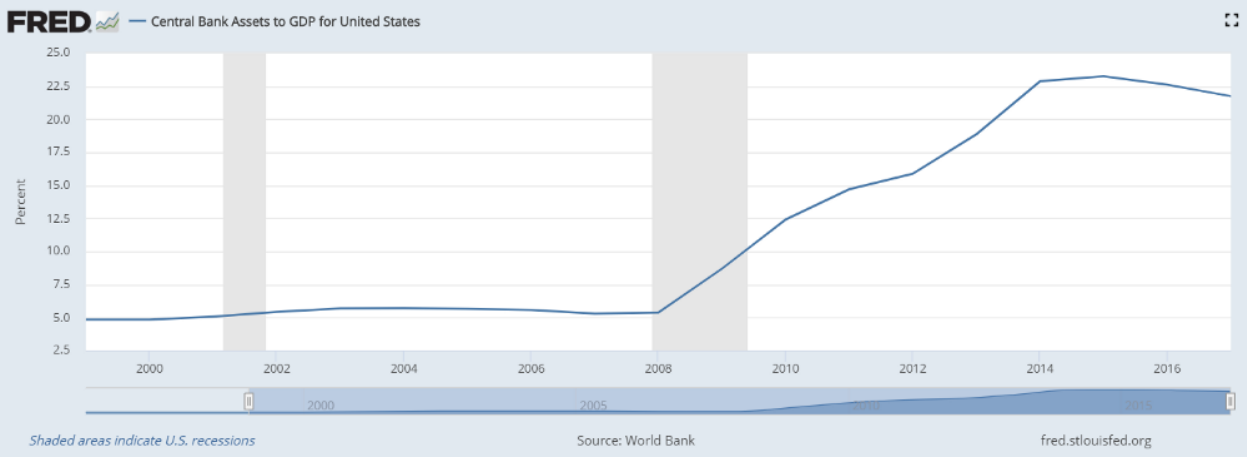
Soon afterwards, the ECB reduced its balance sheet significantly, reaching the same levels it had in Q2 2011 by mid-2014, at around 80% of total eurozone GDP.

However, the most aggressive buying of assets started soon after. If not, how could they expedite the massive financing of private corporations? Through large scale purchases, the ECB took the total value of the assets it owned from roughly 80% of total eurozone GDP in mid-2014 to around 134% in early 2019.

In other words, while the eurozone GDP was close to €3.5 trillion, assets held by the ECB were valued at €4.7 trillion.

In total, the ECB doubled the value of assets it held in the span of five years.

U.S. Federal Reserve QE



This chart shows the total assets held by the Fed.
(Source: https://fred.stlouisfed.org/series/DDDI06USA156NWDB)

In the introduction, we already discussed the effects QE has on major stock indices, namely he S&P 500 and the Dow Jones Industrial Average. To complement the initial discussion, we'll measure the impact the Fed's QE has on total U.S. GDP, much as we did in the previous section with the ECB.

When QE started in late 2008, assets held by the Fed went from roughly 5% of total U.S. GDP to about 12.5% in early 2010. Soon after, the Fed slowed its pace and only increased its balance sheet by approximately 5% between 2010 and early 2012.

However, things were not looking great for the financial markets and the economy in general. Hence, from 2012 until early 2014, the Fed acquired assets worth more than 7.5% of U.S. GDP.

At its peak, the Fed held assets worth close to 25% of U.S. GDP.

Essentially, the only way markets around the world could appreciate, especially in Europe, the US and Japan — where the BoJ currently holds assets worth over 100% of the total of GDP — was through currency manipulation.

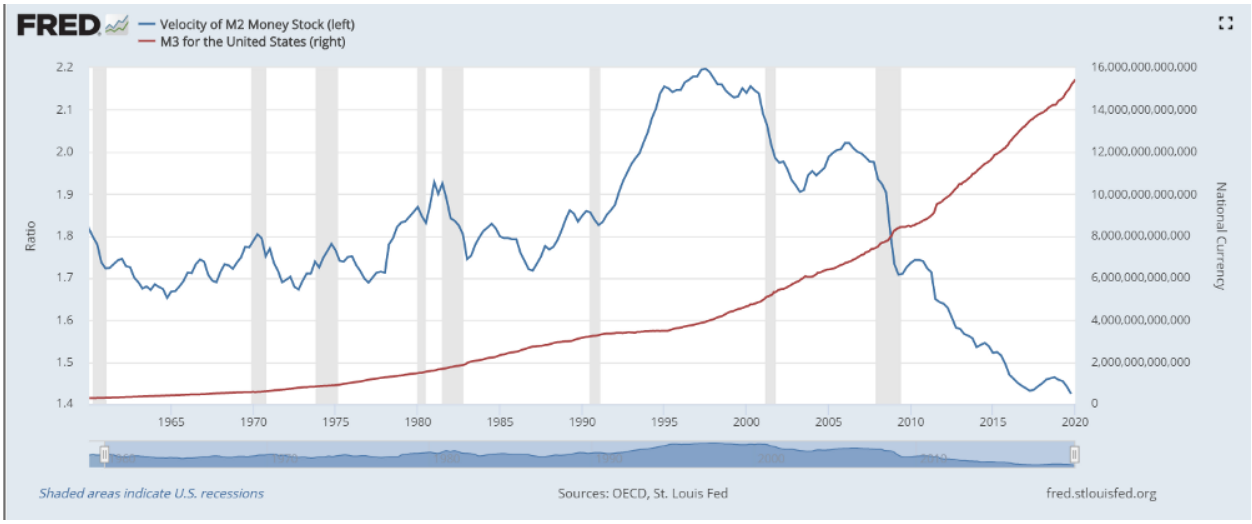
In fact, without the massive repurchasing of global assets, many companies would not be able to survive, for example Boeing, American Airlines or even Hilton. Over a period of two years, Boeing spent $11.7 billion on share repurchases, according to CNN. In addition, American Airlines Group devoted $1.1 billion to such transactions and Hilton announced $2 billion worth of buybacks.

The issue is the fact most of that cash seems to have come directly from the Fed. Curiously, Boeing is now requesting $60 billion in federal assistance, the rest of the airline industry another $50 billion and, finally, the hotel industry is asking for around $150 billion in federal assistance as well.

What this translates into is corporations using near-free cash to provide benefits to shareholders, instead of reinvesting that capital into their business.

Next, we'll analyse the relationship between the money supply and the velocity of money. Our goal is to predict the current and future behaviour of consumers — if they are either hoarding or spending U.S. dollars — and how that may affect short-term and long-term asset and consumer prices.

The relationship between velocity and supply



This chart shows the velocity of money (left, blue) and the total money supply M3 (right, red).
(Source: https://fred.stlouisfed.org/series/MABMM301USM189S#0)

Proponents of Modern Monetary Theory (MMT) and followers of the Keynesian and Chicago schools of economics, like the Bitcoin critic and Nobel Prize winner, Nouriel Roubini, firmly believe it's possible to print our way out of a financial crisis. However, historical data tells a rather different tale.

Before discussing the chart above, let us summarize our findings so far.

In the previous three sections, we concluded that:

- Europe (ECB) is printing large quantities of currency. At the time of writing, it has confirmed additional QE measures, without an end in sight.

- In 2019, the assets held by the ECB were worth 130% of the total eurozone GDP.
- The United States (Fed) is printing large quantities of currency as well. Much like in Europe, it's currently breaking all-time highs in terms of available supply. **Infinite** QE measures have been guaranteed in response to the recent COVID-19 crisis.
- In 2019, the FED held assets totaling 25% of the country's GDP.
- Since QE 1 started in late 2008, both the SPX and DJI have climbed more than 300%.

Let's get back to the pretty picture.

The chart above shows the velocity of money compared to the total supply of currency.

The velocity of money (VoM) is measured by looking at how often each unit of currency exchanges hands during a quarter. To calculate the VoM, we simply divide GDP by the money supply. We can see three distinct phases in the chart.

- Between 1950 and 1990, the VoM ratio drifted between 1.7 and 1.9, meaning between 170% to 190% of the entire money supply's value was being exchanged every quarter.
- In the 1990s, the VoM ratio started rose above 2.0, which means that more than 200% of the entire money supply's worth was being exchanged on a quarterly basis. The figure stayed above 2.0 for much of the 2000s.
- Finally, starting in the late 2000s, the VoM ratio dropped significantly, falling over 35%. It went from a high of 2.2 to a current low of about 1.44, meaning only around 144% of the entire money supply's worth is currently being exchanged per quarter.

Hence, we can safely say a smaller percentage of monetary units are being exchanged today than in 1950, which means that either corporations (or people) are hoarding cash because they're scared, or the number of monetary units has flooded the economy.

Could it be both?

The long-term impact of QE on consumer prices

We concluded in the previous section that less of the money supply is being spent. The downturn started at the eve of the "internet bubble," in the late 1990s, and VoM continued to fall further until today. There have been a few attempts to recover consumers' and corporations' confidence in the

economy, but none have succeeded. The problem will only get worse. What do you think will happen when the economy picks up and the saved-up money reenters consumer markets?

To answer that question, we need to take another look at the chart. But now, let's analyse the increase in money supply (red).

Over the course of almost 50 years, from 1950 until 1998, the money supply increased 13x, from $300 billion to nearly $4 trillion (red line on the chart above). Still, what happened next is astonishing. From 2000 until 2020, the money supply quadrupled. It went from around $4 trillion to over $16 trillion, where it awaits the next pump. We can conclude that since 1950, money supply has grown around 285% every decade.

If the trend continues over the next 10 years, there should be at least $32 trillion in circulation. In 20 years, we're talking about $64 trillion. Does it mean the United States will produce $64 trillion in goods and services?

The only safeguard against massive inflation in the short-term is that newly minted currency most likely won't be going directly to the people.

As we discussed in sections one and two, money is going to the acquisition of assets (stock, corporate bonds, etc). Therefore, a great number of dollars are not going directly into the economy. Rather, those dollars are flowing into companies' balance sheets.

In response to the coronavirus, most governments are discussing the possibility of handing out some sort of Universal Basic Income (UBI) scheme. The logic is simple: every citizen will be given a monthly recurring payment (most likely in a digital form), during a fixed period of time.

Note that the Fed will have to deal with massive unemployment, while at the same time it won't likely lower interest rates since they're already at 0%. Therefore, there should be low expectations people will increase expenditure on consumer products in the short-term. The most likely scenario is deflation. However, soon afterwards comes the storm.

If consumer confidence picks up and people start spending again, will the dollar hold its value? This is, how will the Fed be able to avoid price gouging if additional dollars suddenly flood the market? If companies aren't able to export U.S. dollars abroad, what will happen to the currency?

What history shows is a straightforward path.

My first supporting argument is rather obvious: there hasn't been a single fiat currency which has survived throughout history. Eventually, currencies either disappear due to hyperinflation or due to monetary aggregation, like the euro.

My second supporting argument is to consider what has happened to currencies during periods of crisis. Remember the German mark that got blown away by being hyperinflated from 1918 to 1923? That's a great example.

Essentially, the German government wasn't able to maintain stable prices because too much currency had been printed into the hands of the general population, who after the war had enough confidence in the economy recovering, and thus started spending again.

If we take into account probabilities and history, the most likely end-result of continuous QE is hyperinflation and loss of purchasing power.

Moreover, how much would the economy suffer if QE stopped? Could there be massive deflation followed by hyperinflation? Could Bitcoin behave as a store-of-value (SoV) asset? Or would we see a continuous sell-off by investors, traders and hodlers?

Bitcoin's current price trajectory

To understand how QE has impacted BTC, we should look into two key metrics: price and volume.

Logarithmic chart of Bitcoin from Bitstamp, 2012–2020 (Source: https://www.tradingview.com/x/5xsBmoK5/)

The graph above helps us paint a clear picture of the BTC/USD price performance.

Essentially, it allows us to expand on the idea that investors and traders see bitcoin as a purely speculative asset, almost like forex or stock — which makes sense considering the low volume and liquidity. Even though Bitcoin

is seen by hodlers as a hard currency, defined by Investopedia as money that is both issued and seen as politically and economically stable due to low market liquidity, volatility is still quite high.

So far, bitcoin has fallen from a recent high of $10,400 in mid-February 2020 to around $6,800 in late March 2020, according to Bitstamp. That's a 35% drop in price.

Volume-wise, there has been a significant drop since mid-2019. The trend seems to have stabilized since March 2020, as a few weekly green candles have been popping up.

Still, the cryptocurrency has outperformed most assets, except for precious metals such as gold, a classic SoV commodity.

On one hand, QE seems to positively impact bitcoin's price. Since bitcoin's inception, in 2009, there have been two rounds of QE. The first was in November 2010 and the second in September 2012, as we've discussed in section two.

Both corresponded with fantastic price appreciation. While during QE 2 BTC/USD increased from less than one dollar to over $40, during QE 3 the price increased from around $10 to over $1000 in early 2014.

On the other hand, QE may be ineffective during shutdowns, since the economy is not producing goods and companies are not spending. Therefore, we could see bitcoin turn bearish, as short-term traders and investors leave the market.

If we look at the QT period, from 2018 to 2019, BTC/USD dropped substantially, from a high of $19,700 to a low of $3,100. In percentage terms, we're looking at an 85% drop in price, which seems to have been heavily influenced by less liquidity entering the financial markets.

Nonetheless, Bitcoin has maintained a positive price trajectory over the past 10 years, which has been heavily influenced by expansive monetary policies such as QE.

To make our analysis whole, let's see how gold has evolved during the same period.

The impact of QE on future Bitcoin's price

This chart shows the price of gold CDFs, 2000–2020 (Source: https://www.tradingview.com/x/l1N9qpbw/)

We will conclude this piece by explaining how QE affects, directly and indirectly, the price of Bitcoin, as well as to hypothesize on the impact of other expansive measures, such as UBI. To do that, we'll look into the price of gold — which is, theoretically, the most similar asset to BTC in terms of characteristics.

Since QE began, gold has experienced a major bull run, which took its price from just over $700 per ounce, in late October 2008, towards a record high close to $1890 per ounce in mid-August 2011, according to the Tennessee Valley Authority (TVC). Gold's price increased by 170% between this period.

However, soon after, the price dropped over 20%, and not even QE 3 was able to push it toward another bull run. From October 2012 till early January 2016, gold went from $1770 per ounce to just over $1055, representing a 41% drop in price. It was only after 2016 gold started to pick up the pace again. At the moment of writing, in late March 2020, gold is sitting just over $1620, meaning it increased 53% in price.

The reason why we believe gold took a massive hit was a booming stock market and housing market. Moreover, consumers' confidence in the Fed to maintain the booming market reached its highest since 2000, in late 2018. Only after QT measures were implemented, gold saw a huge spike in price appreciation, during September 2018.

Nevertheless, QE added enormous liquidity to these markets. The problem now is that the economy has halted and investors are liquidating assets for cash. While the real impact has not been felt on prices, since consumers are quarantined and not spending much, the trend will eventually shift. This brings us to the main driver of hard-money price appreciation.

As additional money floods the economy, through QE, UBI and other expansive monetary policies, consumer confidence will eventually return and inflation will kick in. From the moment consumers return to buying, prices will most likely increase, given the enormous amounts of dollars trapped in the economy.

This sudden drop in the purchasing power of currency could drive up the prices of hard-money assets. Much like what happened to real estate around the world during the past 10 years, where house prices boomed across North America, Europe and Asia, we could now see a similar pattern emerging in the hard-money market.

Because markets are at a period where liquidity is needed, we will most likely see the U.S. dollar remaining king for a while, at least until there is an avalanche of currency flowing into the pockets of consumers.

Hence, every asset or commodity with limited quantities and strong network effects, for example gold, silver and bitcoin, could suddenly increase in purchasing power.

The advantage Bitcoin has over precious metals is that it is extremely fungible, divisible, portable and easy to acquire and exchange. All those traits make it more attractive than traditional commodities.

To conclude our analysis, we would like to emphasize that Bitcoin has two very unique characteristics that make it a harder asset than any other money form in existence. First, we can quickly verify the authenticity of a bitcoin transaction and secondly, it's fairly straightforward to enforce our right of ownership, by owning our private keys.

Anyone interested in cryptocurrency can open an account with an exchange, purchase bitcoin and withdraw it to a personal wallet or node wallet. Thus, verifying we bought a real bitcoin is fairly straightforward, as a simple transaction will do, and we can quickly enforce our property rights by moving the coins out of the exchange.

This means that the barriers to entry are fewer than in other markets, such as in precious metals, and it's easier to keep our money within our grasp.

Will QE drive up bitcoin's price in the medium to long-term?

At the end of the day, it depends on how traders and investors view the Bitcoin network. If most believe it is a safe haven asset, then QE will eventually push up BTC's price. As currency becomes extremely abundant, assets with strong network effects and limited quantities tend to rise in price.

If the pendulum of monetary policies swings toward hard money during the next few years, BTC could become a monetary reserve, alongside gold and other precious metals.

Safe trades.

This article was written by Pedro Febrero, with primary co-editing done by Mati Greenspan, founder and CEO at Quantum Economics, and Charles Bovaird, senior contributor for Forbes and vice president of content at Quantum Economics.

Spiritual Reflections On The Bitcoin Halving

By Allen Farrington

Posted May 12, 2020

the halving was not a group call. It was a celebration of a nonviolent revolution trolling its way to victory.

photo by Anthony Cantin, via Unsplash

At approximately 8.23 pm GMT yesterday, the 630,000th Bitcoin block was mined, the first to offer the reward to its successful miner of 6.25 bitcoin rather than 12.5, as has been the case for the past four years. You may have caught wind of this, what with #BitcoinHalving briefly trending on Twitter, an uptick in coverage of Bitcoin in the media over the past few days, or for some other reason.

There are good ways and bad ways to describe “the halving”. Or rather, there are ways that are factually true and then there are ways that are spiritually true. Whatever mainstream coverage you read on this — if you found any at all — I would bet took the factually true route. They will have told you something like the following:

Miners secure the network by wasting electricity solving useless mathematical puzzles. Whoever solves the puzzle first gets a reward and all the pending transactions get logged. The reward just halved, meaning the supply to the market will likely contract, leading many to suspect the price will go up, while others disagree. So far markets have done …

Then whatever markets did in the following hours, which I really don't think is important at all. It is factually important, for sure. But it is not spiritually important. And to ignore the spiritual importance is to misunderstand the halving entirely, just as it is to misunderstand Bitcoin. It is only spiritually important what happens to the price of Bitcoin over years, decades, and centuries.

The halving was not _just _the mining of the 630 thousandth block. It was a social event perhaps unlike any other in history, and perhaps even never to be repeated. Previous halvings (this was the third) were celebrated in bars, beaches, and barbecues, as I am sure this one would have been in normal times. But given the lockdown, the celebrations were migrated to Zoom, YouTube, and Twitter, for the most part.

Many thought this a shame, reminisced spending previous halvings — or previous get-togethers of any kind — in person, and looked forward to being able to do so once again whenever normality returns. But I think the circumstances forced their own beauty, their own poignancy. Not everybody can afford to go to New York on a random Monday in May, but everybody can afford to turn on YouTube. The lockdown meant everybody in the world celebrated the halving in the same place: on the Internet. In Bitcoin's home.

And so rather than take planes, trains, and automobiles to the bars, beaches, and barbecues, tens of thousands of individuals tuned in live from all over the world for what — factually — was little more than a countdown. Many likened it to New Year's Eve, but it was different for at least two reasons, one factual and one spiritual.

Factually, the event itself can only be said to exist on the Internet. It was not "in a place", except insofar as it was in every place. Unlike New Year's, therefore, it happened for everybody at the same time.

But spiritually, the importance of this universality really cannot be overstated. The Bitcoin halving happened at the same time for everybody because the Bitcoin protocol is the same thing for everybody. It knows no borders and no nationalities. It knows no time zones. One might say it _is its own reference time. _The halving didn't happen at 8.23 pm GMT — 8.23 pm GMT happened at block 630 000.

Similarly, the halving didn't happen at ~$8,500 BTC:USD, it happened at 1 BTC:BTC. There will be a time when no "exchange rates" matter or are even meaningful. In anticipation of this, I would encourage the adoption of a different, more consistent metric — perhaps Bitcoin's share of the aggregate global capitalisation of currency? Bitcoin is its own reference value.

Bitcoin's reference time is the same for everybody, as is its reference value, as is its reference software, as indeed are its engendered social celebrations. Provided you have an internet connection you can use Bitcoin to tell the time, to transfer value, to inspect its code, and to join the party.

Moreover, these _must be _the same for everybody, because they exist as references in the first place because Bitcoin, the ecosystem, strongly encourages nonviolent agreement. Bitcoin has elevated the importance of

the word “consensus” in the English language, and its translations in every language, for that matter. Bitcoin is written in C++. This is the factual reason that everybody can read it. The spiritual reason is that it is open source, and that it _must _be open source for consensus to form and be maintained.

Every block has a field called ***coinbase***, which the lucky miner may fill with a limited string of text that has no strictly functional purpose in terms of the code, but, due to the open source nature of the blockchain, anybody can read, and hence can be used as a kind of meta-tool for signalling purposes. The very first block ever mined by Satoshi Nakamoto was given the following text as its coinbase:

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

Factually, this served as a timestamp. Spiritually, it served as a statement of purpose: a call to arms that cheekily elucidated why this radical experiment was even being attempted. It was soon discovered after the halving that the coinbase of the 629 999th block, the last to reward 12.5 BTC, was filled by mining pool_ f2pool _with the text:

NYTimes 09/Apr/2020 With $2.3T Injection, Fed’s Plan Far Exceeds 2008 Rescue

I won’t insult this astonishing gesture by explaining its content. I wish merely to draw attention to its beautiful duality; factually, this achieves nothing. It is a throwback: an impressively well-executed meme.

But spiritually, this is a battle cry. Because here we are again, twelve years and goodness knows however many trillions of unbounded dollars later. Bitcoin is no longer an experiment. It is a nonviolent revolution against financial tyranny, led by nobody, fought by anybody and everybody. And it is literally trolling its way to victory.

Happy halving, everybody. See you again in four years.

follow me on Twitter @allenf32

a lightly edited version of this post has since been syndicated on CoinDesk. Huge thanks to Noelle Acheson and Ben Schiller for making that happen! :)

Tweetstorm: Economics has lost its way

By Per Bylund

Posted May 14, 2020

Economics has lost its way and made the study both impotent and of lacking relevance. It is easy to see how and why if we first recognize that proper economic thinking takes place two steps beyond the apparent. Non-economists typically take none of these steps. Modern economics

has lost the ability to go beyond the first step. This can, I think, be explained by its increasing adoption and reliance on mathematical and equilibrium models, which typically disallow the second step. What are the steps? They involve going beyond what is directly observed to

uncover, first, the immediate or atemporal tradeoff and, second, the temporal dimension of the tradeoff in an overall process. Bastiat famously distinguished good and bad economists by their ability (and inability, respectively) to see the 'unseen'. What he meant by this is that

there is always a tradeoff: something else could have taken place were it not for the immediate cause of observed situation. In other words, it focuses on the proper economizing through imagining the counterfactual. Proper social theorizing can get nowhere bastiat.org/en/twisatwins....

without this fundamental insight. For Bastiat, it is illustrated by the shopkeeper's broken window. Since it was broken, the shopkeeper will give the glacier more business. Isn't that a good thing? Yes, considering only what we can see then this obviously means more business for

the glacier, who in turn can, perhaps, invest in his business, buy more inputs, etc. But, notes Bastiat, to be able to assess this situation from an economic point of view, we must also take into account what would otherwise have happened. If we only consider the outcome of the

broken window, then it would appear as though destroying things would be overall a good investment. Or, to put it differently, a war would make us much more prosperous than peace. Similarly, by analogy, you should put your own house on fire. This is a preposterous thought, and it

is preposterous because it does not consider the counterfactual. Bastiat notes that had the shopkeeper's window not been broken, he would have done something else with that money, perhaps bought shoes. So by breaking the window, the glacier gets more business but the shoemaker

gets less. In both cases, there would be beneficial exchange. So we cannot say that breaking stuff is better because it leads to certain actions. In fact, it is worse because the shopkeeper (and 'society') loses the value of the window. Breaking the window sets us back; it does

not take us forward (unless we are the glacier). But while Bastiat's point is important, it is not enough to properly think about the economy. In fact, modern economic models and equilibrium theorizing is based on this fundamental tradeoff. Economists understand and can point to

the real tradeoff, which explains why they are often disliked by those who conceive of quick fixes and present them as solutions because they base their reasoning solely on the 'seen'. Taking the 'unseen' into account changes the analysis, and makes it much harder to improve

things. The difference between modern economics and proper economic thinking lies in taking the next step after having arrived at the 'unseen': to what I refer to as the 'unrealized'. Rather than comparatively simple comparisons (or comparative statics) taking the immediate

tradeoff into account, the 'unrealized' recognizes that the economy is an ever unfolding process of actions that, fundamentally, are economizing using the imaginable tradeoffs. This goes beyond the multiplier effect that is semi-present in Bastiat's story. Even the multiplier,

that an investment spreads through the economy as the money changes hands, only considers (and follows) one change. The rest of the economy is (theoretically) held constant as the money 'ripples' are traced step by step. This is a simplification, and it is an important one to

recognize since it is only a simplification. It can help to uncover a specific process, or the implications of a specific action, but it does not help us understand the overall market process. The 'unrealized' recognizes the historic processes and the tradeoffs in it as well as

the future. In other words, it doesn't simply take our situation as it is and theorizes from it, but asks where this situation comes from. Specifically, the economy is all of our actions and interactions aggregated. But our choices (and our actions) are made in reaction to the

options we are presented with. The shopkeeper in Bastiat's example had the choice between replacing the window and buying shoes. But what else could there have been, and what else *would* there have been were it not for the many specific prior influences on people's choices? This

becomes a necessary tool when assessing the impact of historic regulations and, more importantly, the possible outcome of introducing new regulations.

Perhaps we want certain restrictions on a specific unsavory behavior. But what does this restriction mean in terms of the choices

that can be made by people in the future? It is not as simple as Bastiat's tradeoff between window and shoes. The glacier's won business leads to different behavior than had he not won this business. It, in turn, affects choices made by yet others, whose 'choice set' (the types

and number of choices available to them in any situation) is affected by the glacier's actions. Had Bill Gates not formed a business around MSDOS and Windows, what options for employment would young people of today have? This is important because it traces the 'ripples' of

actions and changes through the economy over time, and recognizes that there is more than one tradeoff, that one choice influences one's and other people's future choices. For example, it can be argued that any forced change can have enormous consequences in seemingly unrelated

situations, as I do in my book, The Seen, the Unseen, and the Unrealized: How Regulations Affect Our Everyday Lives. For instance, the sweatshop is often argued to be much better employment for people in developing countries than any and all options they https://rowman.com/ISBN/9780739194591/

have. This is true, and the argument emphasizes the tradeoff these people are facing: they choose between working in the sweatshop or something much more terrible. But what this analysis fails to recognize is why these are the only options available. Why is it that sweatshops can

be established in poor countries, but other options are not nearly as beneficial? If one sweatshop can function in some location, why are there not many sweatshops there to compete for workers with (even) higher wages and better work conditions? It should be obvious that the

present economy can facilitate the one sweatshop, which means it can also facilitate more sweatshops. So why is this not the case? Why do those other job opportunities remain unrealized? The answer lies in costs and frictions imposed on the economy *somewhere*. But as it is an

integrated system these impositions may not be where the sweatshops are. In fact, the sweatshop phenomenon can be a result of, for example, international trade regulations and trade agreements, and even regulations in other nations entirely. What appears to be a low-cost policy

or regulation in one country can indirectly affect options for distant peoples and thus their conditions. It is thus possible (even likely) that domestic regulations in developing countries are the cause, or at last contribute to, the lack of economic development in other

countries. A restriction on one person generates different choices than otherwise would have been, which changes the choice set of all those affected: those who are 'stripped' of options that otherwise would be available, and those who 'gain' options. These are real distortions

that must be taken into account to properly understand regulations. And proper economic reasoning recognizes these processes, and their vast and important effects. We may not be able to trace them in detail, or measure them empirically, but they must be considered when studying

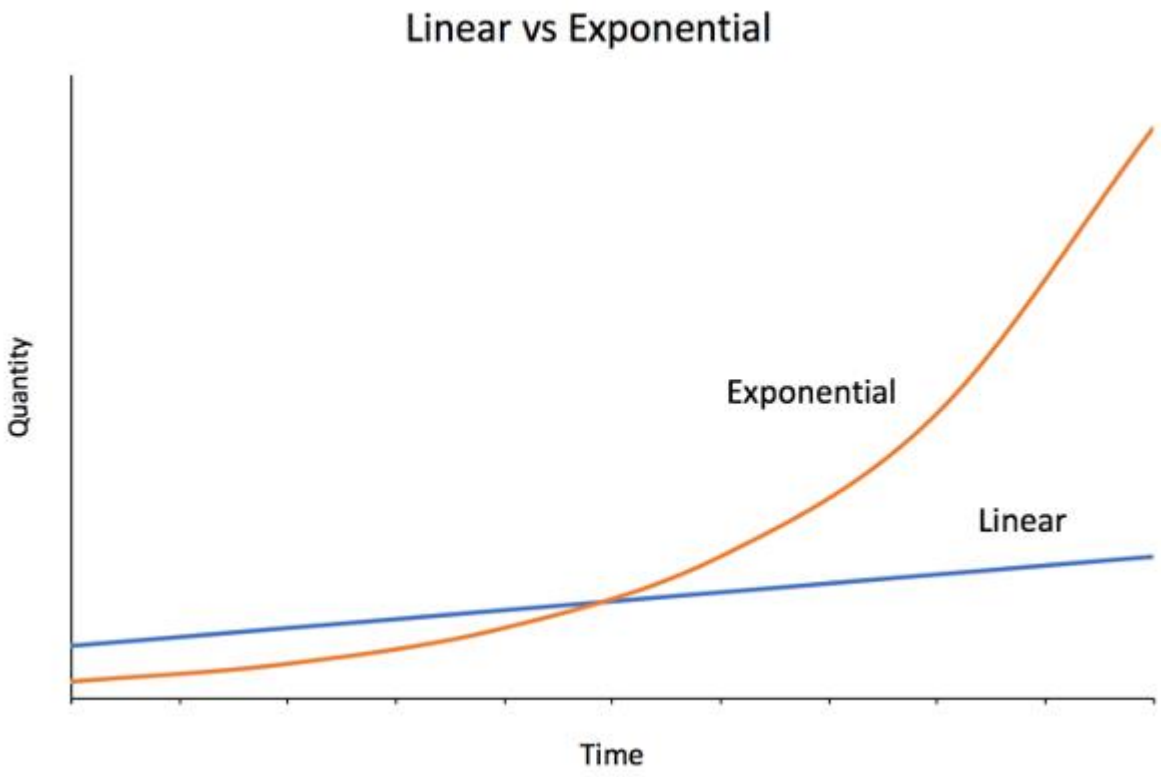
and attempting to understand the economy. Proper economic thinkers take two steps ahead, from the seen through the unseen to the unrealized.

Bitcoin's Resilience to Exponential Change

By Yassine Elmandjra & Dhruv Bansal on Unchained Capital Blog

Posted May 15, 2020

Exponential growth is often grossly underestimated. In technological innovation, exponential trends are masked as linear ones, giving old technologies a false sense of comfort. As a new technology gains momentum, forecasts based on linear thinking turn out to be misleading.



In this world, it becomes hard to predict the winners. As innovation proliferates, old technologies are rapidly displaced by new ones. Competitive market dynamics create little competitive advantage and leave no company or industry immune to disruption. Countless examples show that disruption is often initiated from outside the established market leaders. IBM dismissed the threat of personal computers, allowing competitors to capture the market years before it entered. Digital wallets are disrupting legacy banking. Electric vehicle manufacturers are overtaking the transportation industry.

While new entrants begin dominating a new paradigm, traditional incumbents remain over-committed to a particular conception of a technology. This over-commitment controls decision making processes. When an innovation appears, established industries tend to double down on their allegiance to traditional technologies that once made them market leaders. Falling into a sunk cost fallacy, these leaders prohibit themselves from employing a "rip and replace" strategy. It becomes only a matter of time before they submit to new innovation and survive, or stagnate and die.

Incumbents who ***are*** successful in keeping up with technological innovation create products and compelling narratives about the role these technologies will have in society. Once accepted into the market, these technologies rely on incumbents to maintain their relevance. If not, the "cheaper, better, faster" solution replaces both the technology ***and*** the incumbent.

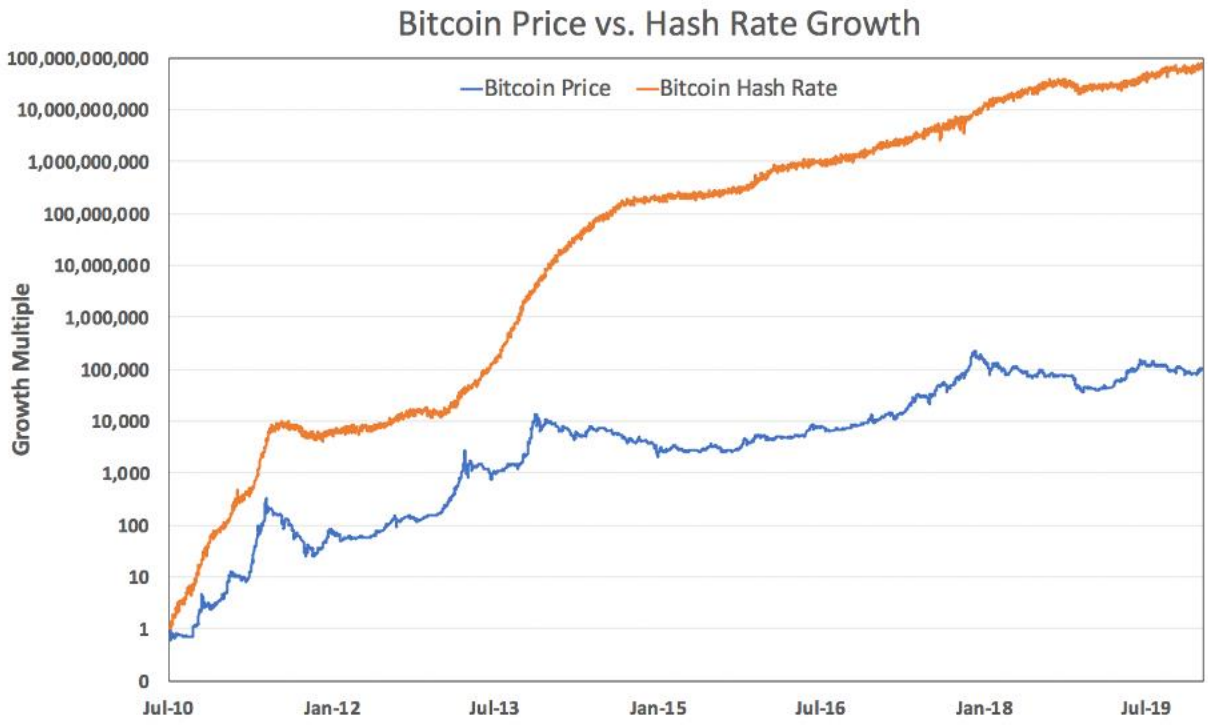
Herein lies the implication of traditional market technologies: in an exponentially growing world, central planners are necessary for their survival. If a technology is to remain relevant, effective central planning is required by the entities adopting that technology. Absent an effective central planner, technologies may fall victim to disruption caused by exponential growth.

But what happens when technologies with _no _central planner, like Bitcoin, are exposed to exponential change? How might decentralized systems adapt? Or are their fates doomed by exponential rates of technological advancement?

Bitcoin's exposure to exponential growth

Once dominated by hobbyists drawing CPU from desktops, mining bitcoin has evolved into a hyper-competitive, multibillion-dollar industry harnessing specialized chip hardware. Through exponential advancements in hardware, mining today is exclusively powered by application specific integrated circuits (ASICs), hardware designed for the sole purpose of mining Bitcoin.

As a result of exponential advancements in hardware and an increased demand to mine, the number of computations dedicated to mining Bitcoin has grown by nearly 11 orders of magnitude, a 1 million times faster rate than Bitcoin's increase in price.



Despite these exponential advancements, Bitcoin's fundamentals remain intact. Specifically, Bitcoin has been able to issue new coins and produce blocks at a constant rate of production, ensuring a predictable monetary policy.

So how does Bitcoin achieve immunity from this exponential growth?

Proof-of-work helps Bitcoin achieve immunity

Bitcoin's resistance to exponential change is best explained by unpacking creator of Bitcoin Satoshi Nakamoto's implementation of proof-of-work.

As suggested in its name, proof-of-work was initially conceived as a way to make certain things harder to create. Spam, denial of service, and other attacks all rely upon an attacker's ability to flood a network with useless traffic at low or no cost to the attacker but at great cost to the network.

In a centrally planned network such as a subway system (or a corporate LAN), a central planner can issue tickets to grant users access, mediate traffic flow, and establish checkpoints to validate these tickets. As a network exponentially grows, it becomes increasingly expensive for a planner to maintain checks and balances. Attackers who obtain a ticket machine (or some private key) can flood the network with valid traffic without paying for the ticket.

Bitcoin's implementation of proof-of-work embeds a system of checks and balances by creating a digital, self-validating ticket that is measurably difficult

to produce. Proof-of-work tickets can't be printed out on a stolen ticket machine because no machine exists that can cheaply make proof-of-work tickets. The only way to produce a ticket is to do work, and anyone who sees the ticket will be able to verify exactly how much work went into producing the ticket.

If transmitting an email or web request required first performing proof-of-work, the rest of the network could easily identify how much work went into messages before they decided to process them. A market-driven computing price would emerge that would be trivial for users to verify and difficult for attackers to exploit. As the network scales, attacks would become more expensive and less common.

A promotion offering subway riders the chance to exercise briefly instead of paying for a ticket. This is a funny example but it's not proof-of-work; possessing the ticket isn't proof you did the exercises. Even a video of you doing the exercises isn't proof as it might be faked. Real proofs-of-work are believed to be unfakeable.
(https://edition.cnn.com/2013/11/15/tech/apparently-this-matters-squats-moscow-subway/index.html)

Proof of work is time

However, making it difficult to mint coins is only one part of creating a distributed currency. Absent a central planner, the various "minters" would also need a ledger to list and record trades of the coins they were creating. This is solved by having every market participant keep its own copy of the

ledger and update it whenever it was made aware of any new transfer of tokens. But what happens if some participants receive conflicting transactions in different orders?

Enter the double-spend problem.

The double-spend problem is solved by answering "which transaction is first?" In other words, all market participants must agree on the order of events. Satoshi's solution was to implement an ***ordered*** sequence of "blocks" each irrevocably cemented to its ancestors using proof-of-work. Combined with the "heaviest chain" rule, this "blockchain" would provide a universal order to all (sufficiently confirmed) transactions.

Even if the integrity of the order of transactions could be guaranteed, however, the rate of block production would be difficult to regulate given changes in the amount of work performed. In Bitcoin's case, an irregular block production would mean irregularity in issuing bitcoin. Irregularity in issuing bitcoin would mean an unpredictable monetary policy. How could blocks be produced at a constant rate if the amount of work performed to produce blocks was constantly changing?

Bitcoin's difficulty rebalancing algorithm

Satoshi realized that proof-of-work could also be used to engineer a distributed market-driven clock. The clock would provide both an ordering to events and tell time by producing new blocks. But in order to keep itself calibrated, the clock would need a ticker that would readjust based on the amount of work performed to produce blocks. This is known as the difficulty rebalancing algorithm.

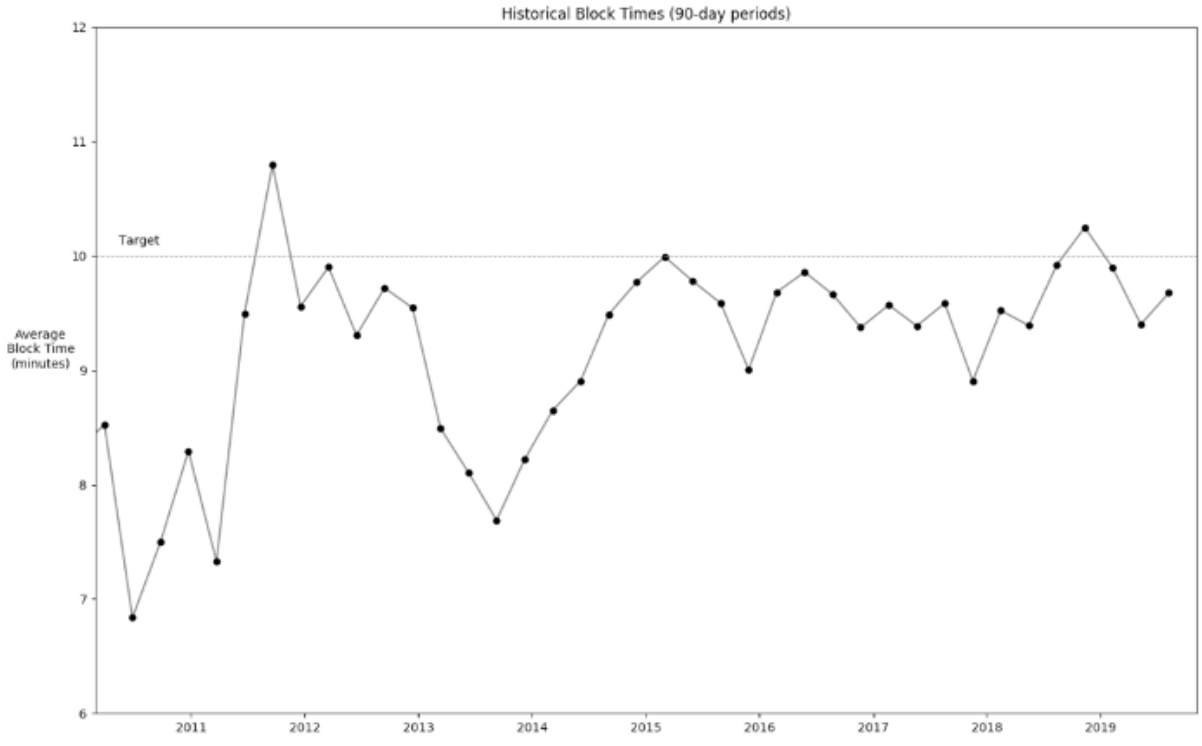
Bitcoin's difficulty rebalancing algorithm is Bitcoin's elegant way of providing this calibration mechanism. The importance of Bitcoin's difficulty rebalancing algorithm is underappreciated and highlights how proof-of-work is used to resist exponential change. The goal of difficulty rebalancing is to ensure that a certain number of blocks (2016) always gets mined in the same real-world time period (2 weeks). Shared time in centrally planned systems is typically "looked up" by asking a central time-keeping server. Bitcoin has no time-keeping server, and instead resorts to this form of crowdsourcing.

During a rebalancing, the Bitcoin software examines submitted timestamps included in each of the prior 2016 blocks. A validation rule is built into the software that ensures valid blocks have timestamps within a small range of each user's own configured time. The block timestamp is thus used as a "crowdsourced timestamp" for the network. During rebalancing, the software uses prior blocks as a sample (N=2016) from which to ***statistically estimate*** the amount of time those blocks took to produce. Through this mechanism, Bitcoin's difficulty readjustment is able to account for any

changes in work and act as a subversion when exponential growth in work is performed.

Regardless of changes in work, the clock serves to measure consistent durations of time. If blocks are produced at a (statistically) constant rate, an issuance schedule can be encoded into block production, establishing a fixed monetary policy. This solves a potential "supply glut" by ensuring that difficulty follows work in such a way that block production remains constant.

How well does Bitcoin's clock work? As shown in the graph below, for more than a decade, Bitcoin has maintained a consistent block time despite exponential increases in work performed, also known as hashrate. Over time, block times have moved closer to the target block time of 10 minutes, suggesting that Bitcoin becomes a more accurate clock as it scales.



Bitcoin turns threat into virtue

Decentralized systems can survive (and even thrive) in the absence of a central planner if they are designed to be resistant to exponential advancements in technology. It is with this implicit realization that Satoshi Nakamoto, the anonymous creator of Bitcoin, pursued creating a distributed, market-driven digital money immune to disruption in an exponentially growing world.

Centrally planned systems are easier to design, construct, and reason about than distributed, market-driven systems. However, the system itself cannot survive without central planners managing adoption and participation. Central planners regulate, coordinate, coerce, and monitor the participants and activity in the system.

In distributed systems, participants can come and go as they please. They can choose to break rules and be adversarial instead of cooperative. They can attempt to subvert, divide, or destroy each other, or the market itself. With the right incentives, however, decentralized systems can sustainably coordinate activity at a larger scale more efficiently, robustly, transparently, and fairly than centrally planned systems.

By implementing proof-of-work, Bitcoin has become the first successful digital money immune to the exponential disruption vector. Proof-of-work in Bitcoin is used to throttle miners, mint new tokens, order transactions, and crowdsource time measurements. With cumulative proof-of-work as a proxy for Bitcoin's security, exponential growth in computing technology has seemingly turned from a potential threat into a virtue. Bitcoin neatly steps around exponential advancements in technology by ensuring a counter-balancing growth of difficulty, suppressing the influence of exponential change on the network and instead elegantly using it to further protect itself.

Thanks to colleagues at ARK Invest and Phil Geiger for reviewing and providing valuable feedback.

What Does Bitcoin Really Represent?

Bitcoin beyond the technical aspect.

By Sylvain Saurel on In Bitcoin We Trust

Posted May 15, 2020

Bitcoin is a true technological revolution. For many, Bitcoin is the most important technological invention since the emergence of the Internet. For others, Bitcoin is simply a new financial investment that offers the potential for much higher returns than traditional investments.

The fact that Bitcoin has made it possible to transform $1 invested at the beginning of 2010 into $90K at the end of 2019 can indeed make people dream.

However, Bitcoin cannot, and especially should not, be reduced to a financial investment.

Bitcoin is much more than that. For me, **Bitcoin is a multifaceted revolution**: technological, industrial, social and ideological.

A lot of people miss the most important thing about Bitcoin, because they only focus on the pursuit of profit. In what follows, I would like to lead you to understand that **Bitcoin represents something much more important for the future of humanity**.

The impacts of Bitcoin's paradigm shift are so broad that I would have to write a whole book to hope to be as exhaustive as possible. So I ask you in advance to forgive me if I miss a few things in this story. If so, please feel free to tell me in comments.

Bitcoin's creation date makes it possible to understand its purpose

If you really want to understand what Bitcoin purpose is, you need to look at when it was conceived. Bitcoin was created by Satoshi Nakamoto in late 2008.

On October 31, 2008, Satoshi Nakamoto published his white paper presenting Bitcoin as "A Peer-to-Peer Electronic Cash System".

Bitcoin was therefore designed following the banking and financial crisis of 2008. As such, **Bitcoin should be seen as a response to the flaws of the**

monetary and financial system. These flaws are exposed in every economic crisis. The crisis of 2020 is no exception.

The message included in Bitcoin Genesis Block clearly confirms Bitcoin purpose:

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

Satoshi Nakamoto inserted in the coinbase transaction of the Bitcoin Genesis Block the title of an article from The Times of January 3, 2009.


THE TIMES

£1.50

Eat Out from £5

More than 900 great restaurants, including four Gordon Ramsay favourites from £15

Israel prepares to send tanks and troops into Gaza

Michael Sheen Frost, Nixon and me

Working mums So that's how she does it

Detox in style The best spas on the planet

Salman Rushdie I won't marry again

Giant killing? Guide to the FA Cup third round

Chancellor on brink of second bailout for banks

Billions may be needed as lending squeeze tightens

99p

The Times of January 3, 2009

The message was very clear: Bitcoin seeks to offer the inhabitants of the Earth an alternative to a fiat system that no longer respects them and has failed in its mission.

Well aware of the importance of his invention, Satoshi Nakamoto made the fundamental choice to remain anonymous and offer it to the world as a gift.

Bitcoin belongs to all its users. It is a true democracy in which every user has potentially equal weight. There is no leader at the head of Bitcoin who could be sued to stop the network. Bitcoin is literally unstoppable.

Bitcoin is a necessity for answering fiat system's flaws

Bitcoin is a solution that emerges from the people. This solution will only succeed if its users make it a success. **All Bitcoin users made Bitcoin what it is today**. A hope for millions of people around the world, but also a reality

with a market capitalization of more than 170 billion dollars at the time of writing.

By giving power back to the people, Bitcoin represents the first step in the separation of money and state.

A famous quote from Satoshi Nakamoto justifies very well the need for the people to regain power by taking it out of the hands of the central banks:

“The root problem with conventional currency is all the trust that’s required to make it work. The central bank must be trusted not to debase the currency, but the history of fiat currencies is full of breaches of that trust. Banks must be trusted to hold our money and transfer it electronically, but they lend it out in waves of credit bubbles with barely a fraction in reserve. We have to trust them with our privacy, trust them not to let identity thieves drain our accounts.” — Satoshi Nakamoto

To function properly, the current monetary and financial system requires absolute confidence in central bankers and banks.

Unfortunately, history has shown us that this is impossible. The Fed’s current unlimited quantitative easing program is a good example of a central bank abusing trust of its citizens.

The Danske Bank money laundering scandal is another example of trust betrayed by a banking institution. One could easily add to this the totally arbitrary confiscation of assets of certain people, or the refusal to carry out certain transactions for totally false reasons.

Since the advent of Bitcoin, more and more banks are blocking transactions to trading platforms.

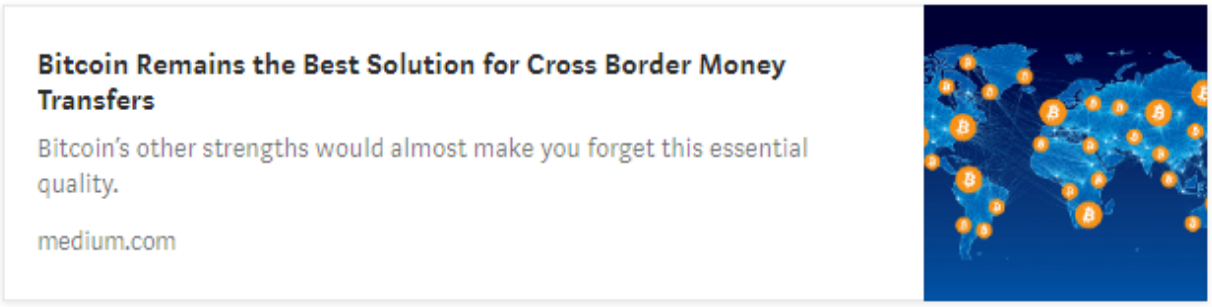
They claim that they are trying to protect their clients, but this is not true. The big question is what do they want to protect their customers from?

Perhaps they want to protect them from finding out the truth if they were to exchange fiat money for Bitcoin…

The need for Bitcoin is therefore essential to regain your sovereignty, but also to no longer have to rely on trust in third parties you cannot really trust.

With Bitcoin, you are able to manage your money as you wish.

You can make all the transactions you want without anyone being able to stop you. Best of all, transactions over the Bitcoin network are ultra-fast, and transaction fees are kept to a minimum.



All this within **a pseudonymous network that protects your identity as long as you don't reveal the addresses you use to others**. Not everything is perfect when it comes to privacy, but the Bitcoin community is working every day to improve this, and make Bitcoin even more protective of your privacy.

The Taproot evolution, or the Lightning Network, will help improve this in the future.

Bitcoin puts you back in control, which means that **Bitcoin allows you to live your life on your own terms**. With Bitcoin, you can choose to save what you own. This is exactly the opposite of what happens with the U.S. dollar, for example.

Indeed, the constant increase in the U.S. dollar money supply arbitrarily decided by the Fed devalues what you have in cash.

The great monetary inflation that we are currently experiencing in 2020 will make those who are already poor poorer. **Choosing to save your fiat money is impossible under the current system**.

With Bitcoin, it's different. Bitcoin increases in value over time, giving you reasons to keep it as long as possible. By keeping your Bitcoins, you will be rewarded in the future.

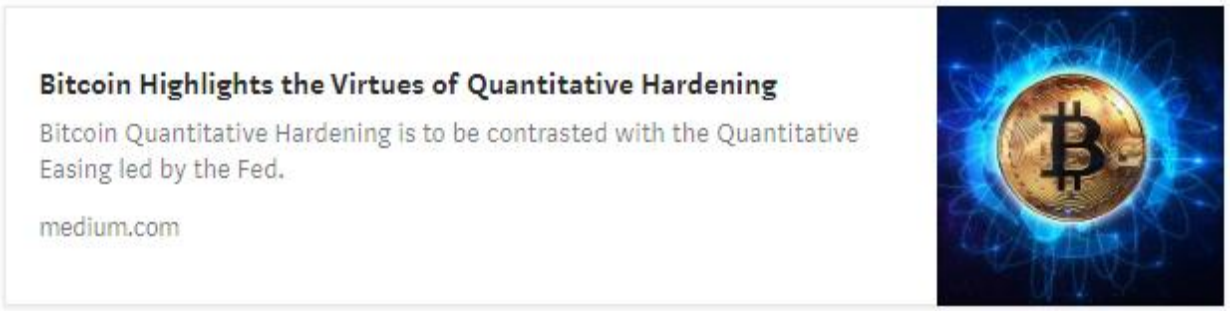
Bitcoin's monetary policy is unique

The power of Bitcoin lies in its unique monetary policy:

- Fully automatic as it is written in the Bitcoin source code.
- Bitcoin supply is finite: a maximum of 21 million Bitcoins will be put into circulation.
- An inflation in the supply of new Bitcoins that decreases over time due to so-called Halving.
- Bitcoin supply inflation will reach zero around 2140.

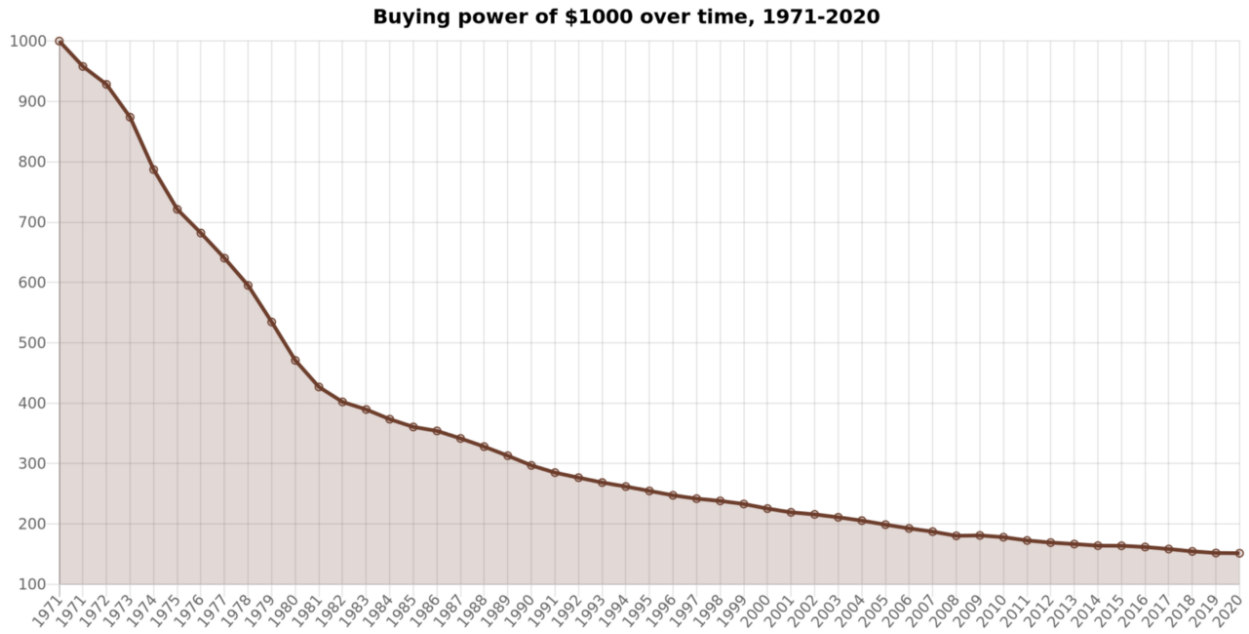
This monetary policy that reduces the supply of new Bitcoins over time is to be contrasted with the policy pursued by central banks around the world.

While central banks use and abuse quantitative easing, which consists of printing more and more units of their respective currencies, Bitcoin highlights the virtues of quantitative hardening.



Quantitative hardening gives more value to existing Bitcoin units.

With Bitcoin, you can therefore accumulate wealth with **the guarantee that 1 BTC of 2020 will always be equal to 1 BTC of 2100**. With the U.S. dollar, this is clearly not the case as shown by the incredible erosion of $1,000 buying power since 1971:



Buying power of $1,000 over time, 1971–2020

Your $1,000 from 1971 has lost 85% of its value by 2020 since it only gives you $150 in purchasing power right now.

Bitcoin is completely transparent

The problem with the fiat system is also its lack of transparency in my opinion. Many opponents of Bitcoin claim that it is primarily used to launder money.

In fact, those who accuse Bitcoin of this are the ones who are laundering the most money.

The Danske Bank money laundering scandal is, in my opinion, just the tip of the iceberg.

When you look at the numbers and the transactions, you come to the conclusion that **Bitcoin is used less than the U.S. dollar for illegal purposes because it is harder**.

The transparency of Bitcoin allows you to have access to all these figures. In today's banking world, this is virtually impossible and huge grey areas still remain. **They allow unscrupulous people to continue to take advantage of a system that is still extremely corrupt**.

If you have any doubts about Bitcoin, just check for yourself. Its Blockchain is totally accessible to everyone. It is immutable which means that all transactions made since the Genesis Block have remained as is and could not be modified.

Bitcoin's slogan is not usurped:

"Don't trust, verify."

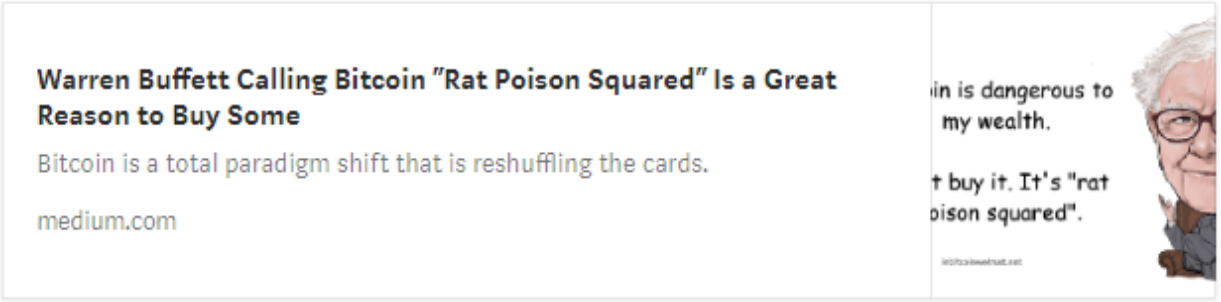
Bitcoin teaches you to be critical. You have to figure things out for yourself. That's how you will discover the flaws in the current system. Then you will probably understand that the powerful people at the head of the system know very well that the system is broken, but they simply don't want to change it.

This system benefits too much to a minority of very wealthy people. They obviously do not want to risk losing their privileges. The Bitcoin revolution is

necessary to bring about a fairer system for everyone that will allow the cards to be reshuffled.

Seeing powerful fiat system guys like Warren Buffett being totally opposed to Bitcoin should alert you.

For me, the fact that Warren Buffett is so afraid of Bitcoin clearly shows that it is a necessity for normal people who are tired of being subjected to a totally unfair system. **The current monetary and financial system has only increased the disparity in wealth since its creation 49 years ago**.



Bitcoin is the best hedge against the Great Monetary Inflation

In the face of the economic crisis we are currently going through, many people are promoting gold as the ultimate hedge against the Great Monetary Inflation.

Recognized for decades, gold is indeed a good store of value. Nevertheless, if we remain objective, **Bitcoin is a superior reserve of value in all respects**:

- Divisible up to 8 digits after the decimal point. You can buy 1 Satoshi, that is 0.00000001 BTC.
- Portability. Your Bitcoins can fit in your head as long as you learn your 24-word recovery phrase.
- Recognizability. It is much easier to verify that your Bitcoins are authentic.
- Harder to counterfeit.
- Scarcer. The amount of gold on Earth is probably limited, but this limit is much greater than the limit for Bitcoin.
- Non-confiscable.

You can easily carry your Bitcoins with you, or send them to a friend halfway around the world in minutes. **With gold, that's impossible**.

Besides, getting into the Bitcoin world requires little effort.

You must just have a smartphone and an Internet connection. From there, you are able to buy your first Bitcoins.

If you want to buy gold in 2020, I doubt you can do it as easily and quickly as you can buy Bitcoin.

Bitcoin is the most secure decentralized network in the world

Bitcoin's decentralized side makes it much more resistant to attack attempts. Since its inception, more than eleven years ago now, **the Bitcoin network has never been hacked**. The few bugs that have made the network unavailable some minutes have been solved at an incredible speed when you consider that Bitcoin is open source and belongs to everyone.

While it is only supported by its users, Bitcoin has an uptime that has nothing to envy those of web giants like Google, Amazon, or Facebook.

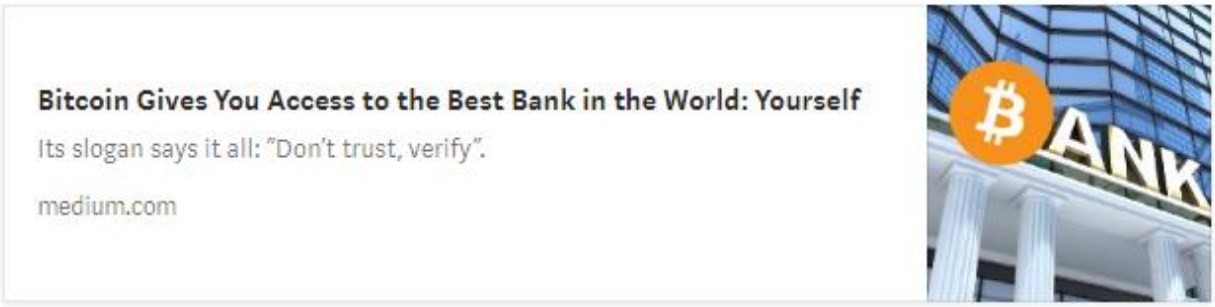
Bitcoin uptime is 99.98% since its creation on January 3rd 2009.

Bitcoin network's Hash Rate is also constantly growing which makes **Bitcoin the most secure decentralized network in the world in 2020**.

By buying Bitcoin, you also have the guarantee that your wealth is safe. Your best guarantee is that you will be responsible for your own security.

It will be up to you to secure your Bitcoins on a hardware wallet. This may scare you initially, but **it's the price you have to pay to take full control of your wealth and your life**. It's a small price to pay in my opinion.

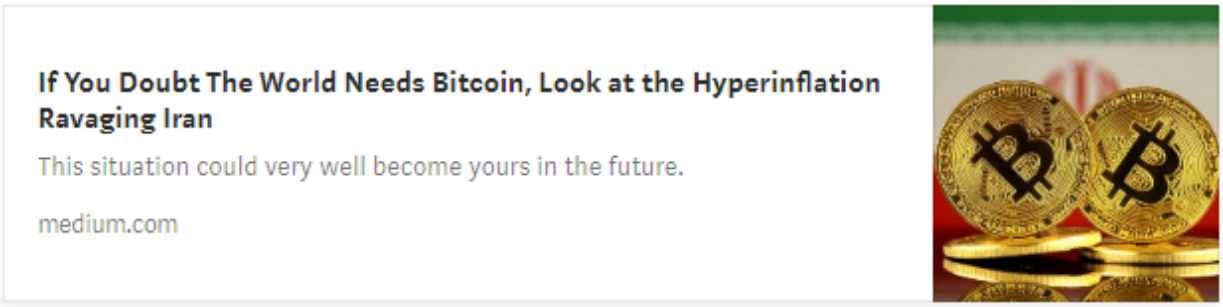
Bitcoin allows anyone who wants to become a network node because its blockchain is permissionless and trustless. Under these conditions, Bitcoin gives you access to the best bank in the world: yourself.



Bitcoin is already a plan A for millions of people

For people living in countries with authoritarian regimes, Bitcoin already plays a vital role. It is an incredible weapon to guard against the inflation that is ravaging Venezuela, Argentina, Iran, and Zimbabwe.

If you still doubt the need for Bitcoin in 2020, I advise you to take a look at the hyperinflation that is currently ravaging Iran.



The situation is the same, or even worse, in Venezuela, or Argentina. For the people in those countries, **Bitcoin is already a plan A**.

It also helps to maintain the right to freedom of speech. Indeed, since no one can confiscate your Bitcoins, you can speak without fear of having your bank assets frozen, for example.

Bitcoin already plays a fundamental role in the protection of human rights. This role is bound to grow in the future.

And even if you live in a Western country, you too may need Bitcoin to protect you from the surveillance society that more and more governments want to impose.

The example of China's social credit system seems to give ideas to the leaders of the major Western democracies, which is not a good thing.

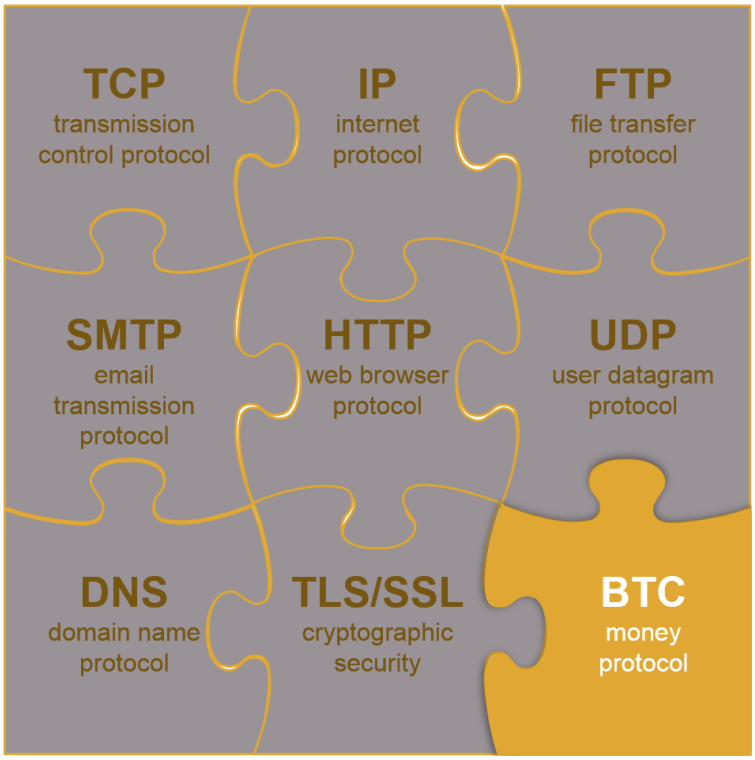
Fortunately, Bitcoin can help you cope. Of course, Bitcoin alone will not be the solution that will fully protect you from mass surveillance. Nevertheless, it will be one of the weapons at your disposal.

Bitcoin is the money protocol of the Internet

Bitcoin is the weapon you will need to use to protect your privacy when it comes to money. More and more people are starting to realize that **Bitcoin cannot be replaced by another cryptocurrency in the future** for the simple reason that Bitcoin goes much further:

Bitcoin is the money protocol of the Internet.

I don't know who is the author of the illustration I will present below, but it helps to understand why Bitcoin is not ready to be replaced by another cryptocurrency in the years to come:



Bitcoin is the money protocol of the Internet

Bitcoin is a protocol in its own right that must be placed on the same level as TCP, IP, HTTP, ...

Once you have understood this, you will understand why with each passing day it becomes impossible to replace Bitcoin for other cryptocurrency projects that claim to outperform Bitcoin. **The Lindy Effect theory fully applies to Bitcoin** which block after block becomes more difficult to replace.

Bitcoin is much more than just a cryptocurrency.

You have to understand this if you want to really get the most out of the Bitcoin revolution. **It would be a real shame to limit yourself simply to the financial side of Bitcoin**.

So I advise you to ask yourself what Bitcoin really is. By looking for the answer to this question, you will discover how much Bitcoin has already brought to the world, and how much it will bring in the future.

After that, I think there is a good chance that you will become a Bitcoiner too.

The Last Word on Bitcoin's Energy Consumption

By Nic Carter on Coindesk

Posted May 19, 2020

CoinDesk columnist Nic Carter is partner at Castle Island Ventures, a public blockchain-focused venture fund based in Cambridge, Mass. He is also the cofounder of Coin Metrics, a blockchain analytics startup.

Much ink has been spilled on the question of Bitcoin's energy footprint. But amid the clarifying details and the energy mix calculations we have lost sight of the most important questions. Anyone who wades into this muddy debate must consider the fundamentals before making a final assessment.

Energy: a local phenomenon

Let's start with the basics. Many people, when decrying Bitcoin's energy footprint, point out its energy consumption and presume that someone, somewhere is being deprived of electricity because of this rapacious asset. Not only is this not the case, but Bitcoin's presence in many jurisdictions doesn't affect the price of energy at all because the energy there isn't actually being used. How could this be?

The first thing to understand is that energy is not globally fungible. Electricity decays as it leaves its point of origin; it's expensive to transport. Globally, about 8 percent of electricity is lost in transit. Even high-voltage transmission lines suffer "line losses," making it impractical to transport electricity over very long distances. This is why we talk about an energy grid — you have to produce it virtually everywhere, especially near to population centers.

When you consider Bitcoin's energy intake, interesting patterns emerge. New data from the Cambridge Center for Alternative Finance has confirmed what we effectively already knew: China is the epicenter of Bitcoin mining, with specific regions like Xinjiang, Sichuan and Inner Mongolia dominating. With the cooperation of mining pools, the Cambridge researchers were able to geolocate the IPs of a sizable fraction of active miners, creating a novel dataset giving us new insight into Bitcoin's energy mix.

And the results are revealing: Sichuan, second only in the hashpower rankings to Xinjiang, is a province characterized by a massive overbuild of hydroelectric power in the last decade. Sichuan's installed hydro capacity is double what its power grid can support, leading to lots of "curtailment" (or waste). Dams can only store so much potential energy in the form of water before they must let it out. It's an open secret that this otherwise-wasted energy has been put to use mining Bitcoin. If your local energy cost is

effectively zero but you cannot sell your energy anywhere, the existence of a global buyer for energy is a godsend.

There is historical precedent for this phenomenon. Other commodities have been employed to export energy, effectively smoothing out ripples in the global energy market. Before Bitcoin, aluminium served this purpose. A huge fraction of aluminum's embodied cost is the cost of electricity involved in smelting bauxite ore. Because Iceland boasts cheap and abundant energy, in particular in the form of hydro and geothermal, smelting bauxite was a natural move. The ore was shipped from Australia or China, smelted in Iceland and shipped back to places like China for construction.

See also: ***Bitcoin Miners, US Energy Producers and Moore's Law***

This led to an Icelandic economist famously stating that Iceland "export[s] energy in the form of aluminum." Today, Iceland is hoping it can replicate this model with the export of energy via data storage. This is why smelters are located in places where electricity is abundant, and where the local consumers may not be able to absorb all that capacity. Today, many of these smelters have been converted into Bitcoin mines – including an old Alcoa plant in upstate New York. The historical parallels are exquisite in their aptness.

ULTIMATELY IT'S JUST A MATTER OF OPINION AS TO WHETHER THE EXISTENCE OF A NON-STATE, SYNTHETIC MONETARY COMMODITY IS A GOOD IDEA.

So to sum up, part of the reason Bitcoin consumes so much electricity is because China lowered the clearing price of energy by overbuilding hydro capacity due to sloppy central planning. In a non-Bitcoin world, this excess energy would either have been used to smelt aluminum or would simply have been wasted.

My favorite way to think about it is as follows. Imagine a topographic map of the world, but with local electricity costs as the variable determining the peaks and troughs. Adding Bitcoin to the mix is like pouring a glass of water over the 3D map – it settles in the troughs, smoothing them out. As Bitcoin is a global buyer of energy at a fixed price, it makes sense for miners with very cheap energy to sell some to the protocol. This is why so many oil miners (whose business results in the production of lots of waste methane) have developed an enthusiasm for mining Bitcoin. From a climate perspective, this is actually a net positive. Bitcoin thrives on the margins, where energy is lost or curtailed.

It's about the energy mix

Another common mistake energy detractors make is to naively extrapolate Bitcoin's energy consumption to the equivalent CO2 emissions. What matters is the type of energy source being used to generate electricity, as they are not homogenous from a carbon footprint perspective. The academic efforts that get breathlessly reported in the press tend to assume either an energy mix which is invariant at the global or country level. Both Mora et al and Krause and Tolaymat generated flashy headlines for their calculations of Bitcoin's footprint, but rely on naive extrapolations of energy consumption to CO2 emissions.

Even though lots of Bitcoin is mined in China, it's not appropriate to map China's generic CO2 footprint to Bitcoin mining. As discussed, Bitcoin seeks out otherwise-curtailed energy, like hydropower in Sichuan, which is relatively green. Any reliable estimate must take this into account.

Silver linings

The prospects look even sunnier when you consider the changing nature of Bitcoin security spend. Eighty-seven percent of Bitcoin's terminal supply has been issued already. Due to the path Bitcoin's price took during the heavy-issuance phase, miners will have been collectively rewarded just over $17 billion in exchange for finding those coins (assuming simply that they sold their coins when they mined them), even though the coins are worth $160 billion today. This is because most of those coins were issued at cheaper price points.

If Bitcoin ends up being worth substantially more in the future than it is worth today (say, by an order of magnitude), then the world will actually have received a discount on its issuance. The energy-externality of pulling those Bitcoins out of the mathematical ether will actually have been very low, due to the historical contingency of when, price-wise, those Bitcoins were actually mined. In other words: Bitcoin's energy expenditure may end up looking rather cheap in the final analysis. Coins only need to be issued once. And it's better for the planet that they be issued when the coin price was low, and the electricity expended to extract them was commensurately low.

See also: ***Bitcoin Halving 2020: How the World's Largest Mining Pool Is Helping Miners 'De-Risk'***

As any Bitcoin observer knows, issuance as a driver of miner revenue will decline with time. Last week's halving cut the issuance side of miner revenue by half. If I had to make a guess, Bitcoin's periodic halvings will at least offset its appreciation long term, making runaway growth in security spend unlikely. Fees will necessarily grow to account for a much larger fraction of

miner income. Fees have a natural ceiling to them, as transactors must actively pay them on a per-transaction basis. If they become too onerous, users will look elsewhere, or economize on fees with other layers that periodically settle to the base chain.

Thus it's unlikely that security spend results in the world-eating feedback loop that has been posited in the popular press. In the long term, Bitcoin's energy consumption is a linear function of its security spend. Like any other utility, the public's willingness to pay for block-space will determine the resources that are allocated to providing the service in question.

Is it worth it?

Now, despite all the caveats listed above, it's undeniable that Bitcoin not only consumes a lot of energy but produces externalities in the form of CO2 emissions. This is not under debate. What Bitcoiners are often confronted about is whether Bitcoin has a legitimate claim on _any _of society's resources. This question relies on a kind of utilitarian logic about which industries should be entitled to consume energy. In practice, no one actually reasons like this. The Bitcoin-energy supplicants are mum when it comes to the energy used to illuminate Christmas lights, to power the data centers behind Netflix or to distribute untold millions of single-serve meal kits. It's clear that because Bitcoin's footprint is so easy to quantify — and an object of revulsion among the chattering classes — it is singled out for special treatment.

Ultimately it's just a matter of opinion as to whether the existence of a non-state, synthetic monetary commodity is a good idea. The truth is that blockspace is a service which is paid for, and that's where its resource cost is derived. Something duly purchased cannot, by definition, be a waste. Its buyer derives benefit from its existence, regardless of anyone else's subjective opinion of the merit of the transaction. These same arguments have been made countless times about perceived "costs" of the gold standard, and rebutted on similar grounds before. Fundamentally, millions of individuals the world over still value physical, bank-independent savings, so it still gets pulled out of the ground with regularity. As long as people value Bitcoin, so, too, will the block-space auction continue in perpetuity.

The Bitcoin-energy worriers need not despair, however. There is a solution. All they must do is persuade Bitcoin fans to use and value an alternative settlement medium. Their best bet will be to devise a system that is even more secure, offers stronger assurances, settles faster, is more privacy preserving and is more censor resistant – all without using Proof-of-Work. Such a system would be miraculous. I'm waiting with bated breath.

Bitcoin's Value Proposition – Is It Truly the Best Currency?

By BTChap on The Bitcoin Reserve Journal

Posted March 22, 2020

Why bitcoin is the king of the hill when it comes to hard money.

Disclaimer: Opinions expressed in this article do not constitute investment advice from Bitcoin Reserve.

How Bitcoin stacks up against traditional currency and possible new competitors

The hype about Bitcoin is sometimes overwhelming and presumably difficult to understand from a conventional investor's point of view. So, let us try to unravel that mysterious "internet money" for the interested reader. Bitcoin's most important difference, in comparison to other currencies that operate within the conventional banking system, is the way in which payments are transferred. Payments by credit card or smartphone are made via banks, which in turn settle with each other via a system operated by a central bank. With Bitcoin, on the other hand, payments are processed via a distributed ledger - a decentralized database in which all transactions are recorded permanently. If a transfer is pending, someone has to check whether the paying party has a sufficient Bitcoin balance and subsequently needs to arrange the transfer of funds to the payee. But who is this "someone"? Bitcoin, for the first time in financial history, relies solely on volunteers running the infrastructure to maintain the network and pays them in newly created Bitcoin.

So how can the hype about Bitcoin be explained?

Bitcoin is new. In order to comprehend its disruptive effects on today's financial industry and banking system, it's important to examine the aspects of Bitcoin's value proposition. During the financial crisis of 2009, an anonymous person or group by the pseudonym of Satoshi Nakamoto published the Bitcoin whitepaper as no less than a counterproject to the traditional financial system. Thus, Bitcoin was born and designed during a financial crisis, and it is the only asset that was built with a particular emphasis on its resilience to wither such a situation.

History has shown that its resilience against continuous attacks is staggering, considering its constant exposure to assaults by individuals, groups of people or even governments within the last ten years of its existence. In fact, it can be viewed as the world's largest honeypot for hackers. In this hostile environment, the Bitcoin protocol has proved its resilience repeatedly as the Bitcoin blockchain itself has never been successfully hacked throughout its entire existence. This is not true for Bitcoin exchanges, however, which are hacked on a regular basis. Thus, it is of utmost importance for the interested investor to invest in an adequate storage method.

Another side effect of those constant attacks was the stoic calm acquired by early investors. Those early adopters believed in Bitcoin's superiority over any other asset, but is this mindset justified, or are those people merely naive idealists?

The two concepts powering Bitcoin's popularity

This steadfast belief in the Bitcoin protocol is based on two simple concepts. They may seem trivial at first glance, but when these two points are understood, it is possible to understand how a currency, which is not backed by any government, could achieve such a meteoric rise. Those two concepts are:

1. There are only 21 million bitcoin.
2. You cannot create a better Bitcoin.

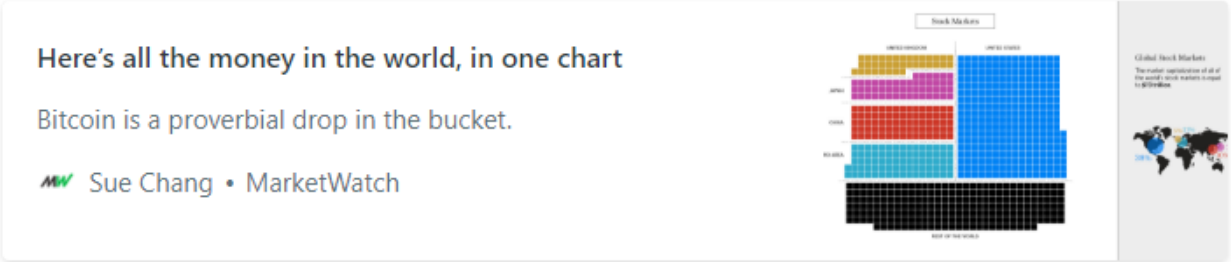
Let us elaborate on both statements since they are anything but trivial.

Concept 1: There are only 21 million bitcoin

There will only be 21 million Bitcoins in existence. This is engraved in Bitcoin's source code and cannot be changed by anyone. This "hard cap", or maximum supply, is one of the main reasons for Bitcoin's price valuation. Bitcoin is thus the most deflationary currency humanity has ever seen. In a centralized economy, the currency is issued by a central bank at a rate that is supposed to match the growth of the number of goods. The monetary base is controlled by a central bank, which can increase the supply by issuing more currency. The resulting distribution of capital is interesting, to say the least.

Here's all the money in the world, in one chart

Bitcoin is a proverbial drop in the bucket.



Bitcoin today just represents the proverbial "drop in the bucket" of the global financial system – albeit with all its advantages (very high risk/reward ratio) and risks (high volatility, possibility to manipulate the price, etc.). Since Bitcoin represents a fully decentralized monetary system, no central authority regulates its monetary base. Instead, the currency is created by the miners at a fixed and predefined rate, and transactions are verified by the nodes of this peer-to-peer network. Everyone can participate without the need to register at a higher level, making the network truly decentralized and democratic. The Bitcoin protocol defines how the currency will be created and at what rate. This boundary condition was established at Bitcoin's creation in 2009 and cannot be changed. Any Bitcoin transaction that is generated by a malicious user and does not follow the rules postulated by Satoshi Nakamoto in 2009 will be rejected by the Bitcoin network. As a result, Bitcoin represents the most deflationary currency known to humankind and enables verifiable, and thus trustless, transactions between two entities without any intermediary. This property makes Bitcoin a serious contender to become the world's reserve currency.

Concept 2: You can't create a better Bitcoin

But how about just creating a new, superior cryptocurrency? Well, that is not possible either. The reason is simple: no government will allow anyone to take away their monetary sovereignty - ever.

In today's market, if a cryptocurrency files to be listed at a currency exchange, the exchange requires the founder of the currency to reveal its identity to comply with Anti-Money Laundering (AML) laws, among other requirements. By doing so, the single point of attack of the digital currency would be revealed to everyone, basically enabling state actors to enforce changes in the project.

Take Facebook's Libra currency project, for example. Of course, legislators will want to protect customers and thus will treat the Libra organization as a bank, which is backed by its shareholders, such as Facebook. Facebook would in turn be regulated like a bank – something the organization will definitely not want. So, the Libra project will hardly be a reality, a view shared

by many powerful leaders such as the Bank of France's Governor Francois Villeroy de Galhau. Bitcoin is a different beast altogether - no government in the world is able to change the rules of the Bitcoin protocol, or ban its use. Thus, Bitcoin is the ultimate store of value.

A possible alternative to Bitcoin? Digital central bank money

Alternatives to privately issued digital currencies are those issued by central banks, which are basically tokenized fiat currencies. Projects like these are under investigation by many central banks and should soon be available (e.g. in China, where the digital currency will be operated by the Chinese central bank). To what extent this concept is supposed to differ from existing fiat currencies - especially in a country where most payments are already being made via smartphones - is unclear. If one wants to protect wealth from devaluation by inflation, it makes no sense to hold fiats - tokenized or not - as was made clear by the PRC Central Bank a few weeks ago. In that instance, the bank injected capital equaling Bitcoin's market cap into the economy to maintain the market's liquidity in the face of the coronavirus outbreak (see link).

Current global currency and policy challenges that Bitcoin overcomes

As the PRC Central Bank example shows, a tokenized fiat currency can and will be manipulated and respectively inflated by the respective governments to react to such situations. Bitcoin is different altogether - no single person is ever able to change the protocol and subsequently inflate supply. This makes it the number one choice if you want to stop inflation from eroding your wealth.

Since inflation is an issue not only in China but also in the US, in the EU, and particularly in many smaller economies, it is just a matter of time until a growing number of people will want to secure their wealth. This will trigger a vicious cycle of monetary devaluation, increasing capital outflow from fiat currencies, higher Bitcoin valuation and so on, which can result in bank runs and eventually the collapse of the conventional banking system. This will not start in the big economies but rather in small ones like Venezuela, Argentina, and Lebanon, where the local currency is already weak and the incentive to adapt Bitcoin is higher than in the EU, China or the US. As soon as this chain reaction is set in motion, however, it will increasingly affect larger economies and intensify itself, which will eventually result in a global bank run. This effect can only be prevented by governments and central banks if the fiscal policy is changed fundamentally, by making moves like reintroducing the gold standard. This global reorientation of central bank policy is considered highly unlikely by the author, since it would render debt repayment almost

impossible at the current state of national debt in even the largest economies.

Now that you understand the unique selling points of Bitcoin, let us focus on the current problems many millennials face today, which make them a group especially well-positioned to invest in and adopt Bitcoin.

The Cantillon Effect and its impact on millennials

Richard Cantillon's original thesis outlines how rising prices affect different sectors at different times and suggests that time difference effectively acts as a taxing mechanism. In other words, the first sectors to receive the newly created money enjoy higher profits as their pay increases, but general costs are still low. On the other hand, the last sectors in which prices rise (where there is more economic friction) face higher costs while still producing at lower prices. As Milton Friedman taught us, because the real economic variables are still the same in the long run, the price of inflation is paid for by a "tax" on the sectors with more friction, which subsidizes more time-responsive sectors.

In our modern economy, the Cantillon Effect is at play with a stratified socioeconomic impact, favoring investors over wage earners. This effect is an ever-growing fuel for increasing global wealth inequality, which particularly affects millennials - the first generation that is likely to be less wealthy than its preceding generation. The results are unrest and protests in several Latin American countries such as Chile and Argentina, as well as in Spain, Italy, and, of course, France.

Negative interest rates

There is another incentive to get exposure to Bitcoin: short and medium turn. The European Central Bank (ECB) will not end the time of asset purchasing programs or negative interest rates, as Christine Lagarde made clear during her introductory statement as head of the ECB.

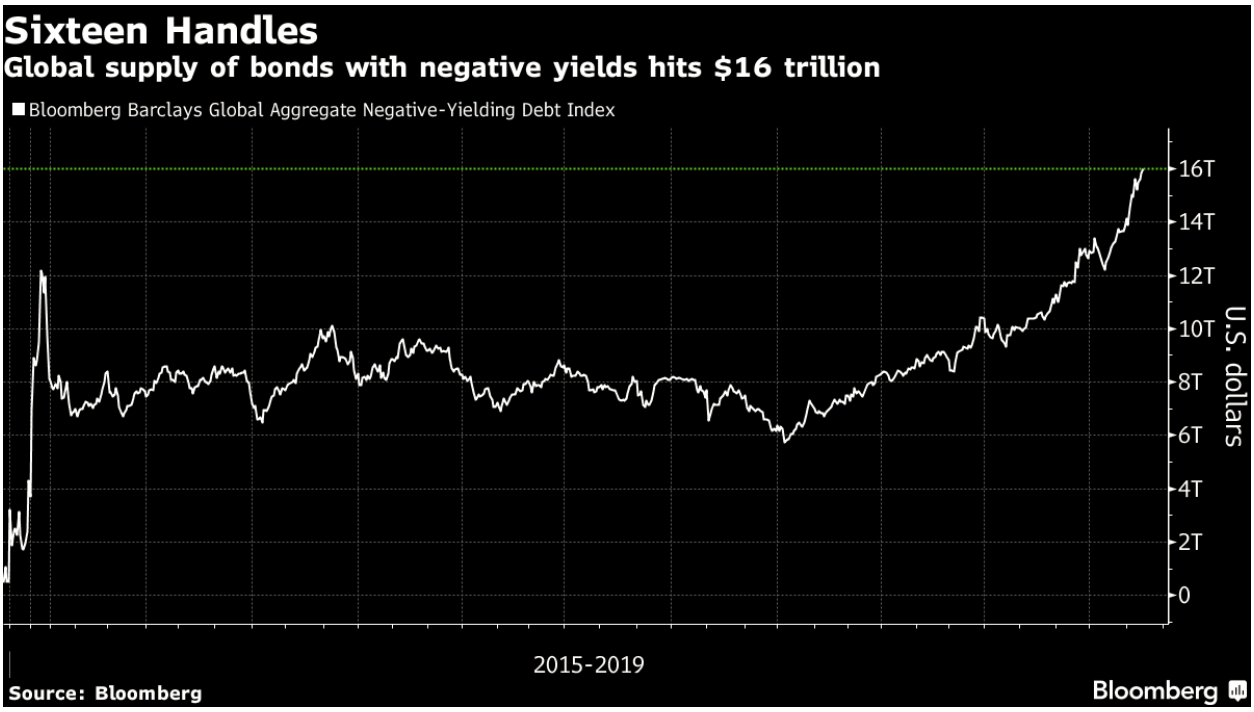
This results in an interesting effect: if investors are facing negative interest rates, the price for scarce goods (real estate, gold, Bitcoin, art, etc.) is in theory infinite as you can earn interest for taking a credit. This is unheard of in the history of humankind.

Within the last 3,000 years, there has never been such a time where you would have been paid to take out a loan. The result of that policy is absurd. A Danish bank, for example, launched the world's first mortgage with negative interest rates. Another development was the introduction of Austria's infamous 100-year bond. Buyers of such bonds are speculating on a century of rock-bottom interest rates, which is interesting considering that

the present Republic of Austria was founded in 1918 and has only existed for 102 years. Whether the described developments are rational or sustainable, it's up to the readers to decide.

Banks also face another challenge – it is becoming increasingly difficult to earn capital in a low interest rate environment, as there is the threat of high penalties for depositing capital with the central banks. These costs are increasingly passed on to the customers, who in turn are confronted with the problem that they are expected to pay increasingly higher fees for depositing savings with the bank. It is unlikely that this can be conveyed to a customer, and the author assumes that this effect alone will lead to an increase in interest in Bitcoin.

Another absurdity of today's financial system, that is likely hard to comprehend for the average person, is the existence of negative yielding bonds. An unimportant niche? Well, we are talking about a total global supply of bonds with negative yields of 16 trillion US dollars. Bitcoin's market cap at the moment is $170.2 billion US dollars, or less than 2% of the global supply of bonds, just for reference.

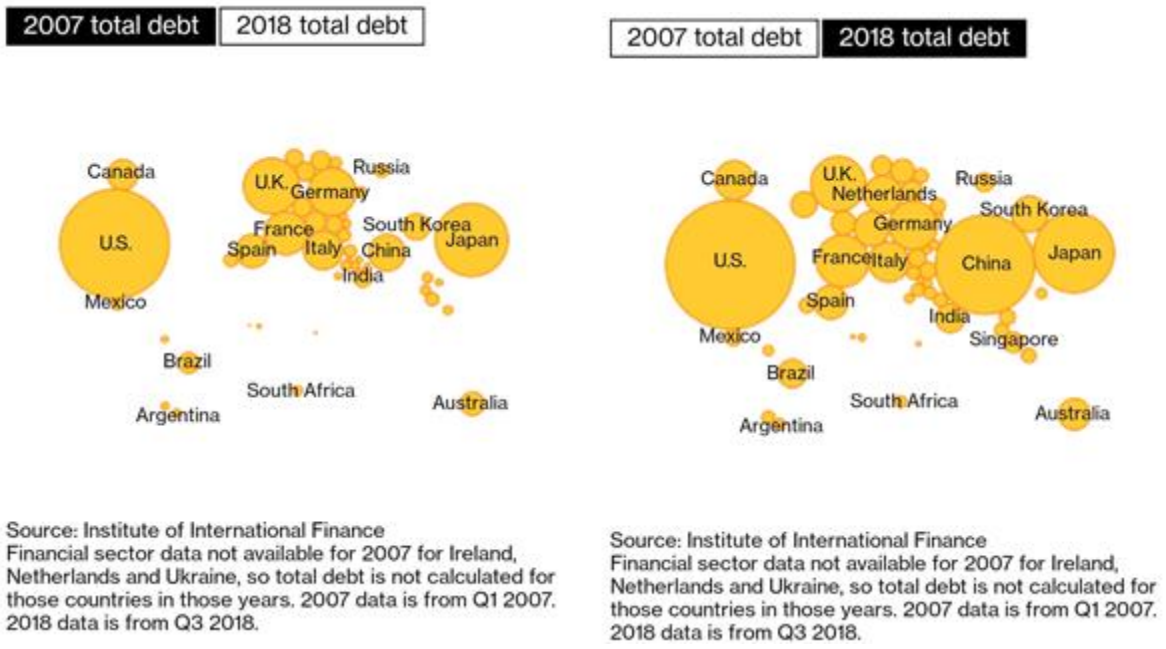


Global supply of bonds with negative interest rates (Source)

Debt

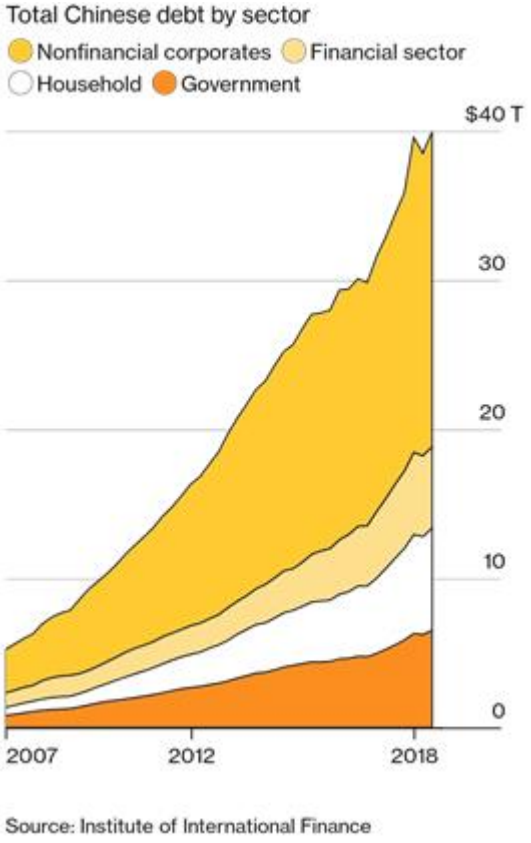
All the world's largest economies are facing an increasing amount of debt. This is a looming catastrophe scenario, which central banks are trying to

counteract by stacking ever-larger amounts of gold. Global debt levels are up 50% since the global financial crisis in 2009.



Global debt development from 2007 to 2018

This fact becomes particularly striking if one looks at companies in China:



Overall, China's total debt has increased sevenfold since the crisis. Due to the constant money infusion by the government and due to its deficit spending, many unprofitable companies are kept in business, which would otherwise be bankrupt. The problem of Chinese "Zombie companies" has been recognized for some time, but the government must keep those companies alive and keep annual GDP growth at a certain level to prevent social unrest. This is the Achilles heel of the Chinese Communist Party and the only threat to its power – a vicious cycle of money printing and amassing debt, which wealthy individuals might want to escape from sooner rather than later.

The downside of Bitcoin: Circumventing sanctions, enabling money laundering and financing terrorism

As of today, the US Dollar, the Renminbi and the Euro all play a far greater role in financing nefarious activities than Bitcoin does. However, there is one thing to keep in mind:

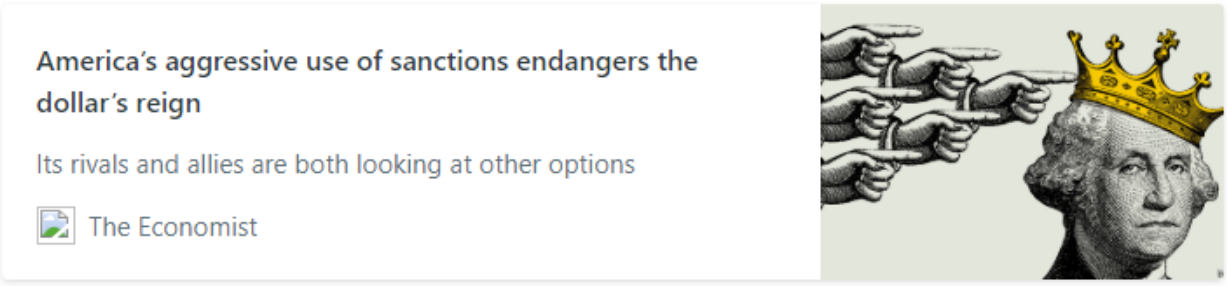
"If only good actors value a currency the currency has no value at all."— Anonymous

This quote puts it nicely. If a global, decentralized currency is to compete against currencies like EUR or USD, it must be immutable and immune to censorship or government interference. This is not a bug of the Bitcoin protocol but a feature. No government on the planet is able to prevent a Bitcoin transaction from happening, which gives the participants in the network total and absolute sovereignty over their capital. This is critical for a currency to become a true global reserve currency.

Today, the US is able to exert a significant amount of economic pressure on any country using the US Dollar for settlements (e.g. by enforcing sanctions on them if they do not agree with some political decisions in those countries). Recent examples include sanctions against Russia, Iran, Pakistan, and the EU because of Nord Stream 2 and an ever-growing list of countries that do not obey to the will of the US President. This excessive sanctioning by the US slowly starts to erode other countries' trust in the dollar as settlement currency.

America's aggressive use of sanctions endangers the dollar's reign

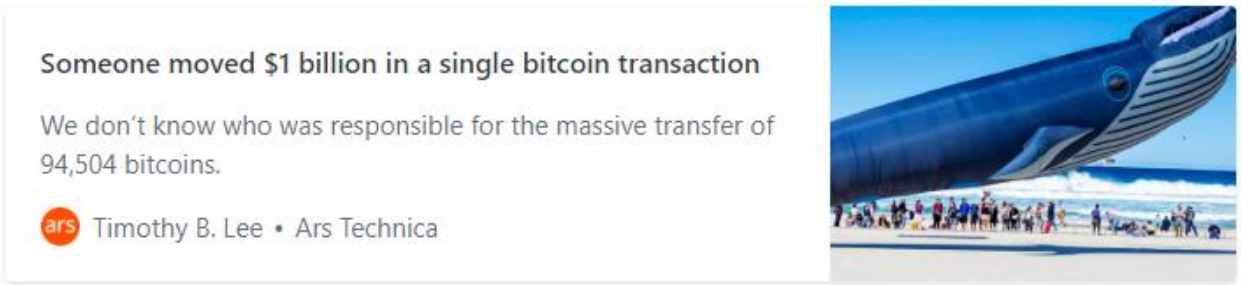
Its rivals and allies are both looking at other options



The affected countries need to look for an alternative currency to settle their trades in. Since the countries in question may not necessarily want to trade in the currency of the respective partner, and since both currencies could be manipulated by the opposite side, it is desirable to have an asset with predetermined issuance by an algorithm that can´t be manipulated at hand. In addition, the transaction can be monitored literally in real time from any

device that has access to the internet. Those properties make Bitcoin a truly neutral settlement layer between parties and even nation states in the future, which represents a big step towards its adoption as a global reserve currency.

In addition, Bitcoin's transaction fees for cross-country settlements are low, as was famously shown by a transaction worth $1 billion which cost the transacting party a fee of 0.065 Bitcoins or $690 at the time of the transaction.



The same transaction in gold would be far more expensive; we are talking about 19.9 metric tons at the current exchange rate (as of 27.1.2020). The logistics of such a transaction would be challenging, to say the least, and certainly impossible to achieve for 700 USD. The cost for safe storage of 20 tons of gold is not included in this calculation but shouldn't be neglected either.

Conclusion: Is Bitcoin the ultimate reserve currency?

Many of the issues addressed here will probably not hold immediate relevance for an institutional investor, but they will have an impact on Bitcoin's price mid- and long term. Mid- to long-term, we will not only see Bitcoin adoption by millennials but also high-net-worth individuals, troubled Third World countries, rogue states, and governments that will want to circumvent sanctions.

Other use cases will be central banks backing their currency with Bitcoin to brace for a "Black Swan Scenario" or pension funds that have the obligation to maintain their depositors' purchasing power. It is important to note that every single reason pointed out above could just be the catalyst for other effects to unravel. Capital will inevitably gravitate towards the hardest money available, depriving people holding onto the weaker currency from their wealth and leaving them vulnerable to the people controlling the harder currency – a situation humans have experienced countless times throughout history. Examples include glass beads, shell money, or rai stones. The Dollar, Renminbi, Euro and Ruble are the glass beads of the 21st century.

But is that true? Let's look at Bitcoin's performance in 2019 alone in comparison to other assets:

- Bitcoin + 96%
- Oil + 36%
- Nasdaq 100 + 16%
- S&P 500 + 13%
- Commodities + 9%
- Bonds + 3%
- Gold + 1%

Bitcoin outperformed any conventional asset, which is interesting considering that the NASDAQ 100 and the S&P 500 benefited significantly from the Fed's money infusion. Actually, that growth is largely attributed to the liquidity provided by the Fed in conjunction with the Cantillon Effect covered above.

An interesting side note is the fact that, by the year 2250, a single Bitcoin will be worth $1 million, based on USD inflation alone if it prevails at current levels. In the not so distant future, central banks might even be forced to add Bitcoin to their assets to protect the Dollar, Euro, or Ruble against devaluation. It is interesting to see the Russian Central Bank increasing its gold holdings since 2005, and it would be naive to think central banks would not know about Bitcoin's potential. However, it would be equally naive to assume they would admit a purchasing program.

Many people tend to forget one thing today: Fiat money is not as stable as it is perceived - Germany alone has had four different currencies in the last 120 years. In contrast, Bitcoin could offer the stability and assurance that other currencies fail to provide.

Author's contact: btchap@aikq.com

Tweetstorm: Elon is Satoshi

By Chris Espley

Posted May 20, 2020

HOLY SHIT I'VE WORKED IT OUT.

@elonmusk INVENTED BITCOIN FOR HIS MARS COLONY.

ELON MUSK IS SATOSHI NAKAMOTO!

A THREAD

I know this sounds crazy but hear me out. In 1999, Elon Musk founded an online financial service called http://X.com, which acquired PayPal shortly there-after.

PayPal's cofounder, Peter Thiel, described their mission like this:

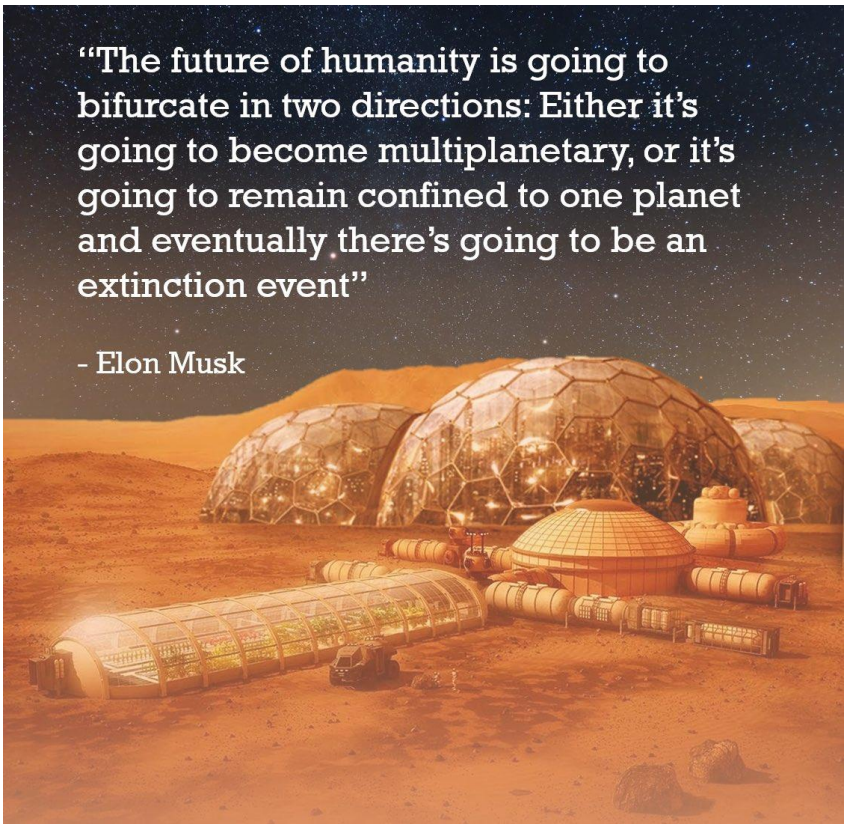
"We're definitely onto something big. The need PayPal answers is monumental. Paper money is an ancient technology and an inconvenient means of payment. In the 21st century, people need a form of money…that can be accessed from anywhere with a PDA or an Internet connection. (Governments) use inflation…to take wealth away from their citizens. Eventually PayPal will change this"

Sound familiar?

But Musk and the PayPal mafia never managed to fulfil this vision, and instead sold PayPal to eBay in 2002 for over $1 billion. But Musk didn't forget. Months after the sale of PayPal, Elon Musk founded SpaceX, with the mission of creating a self-sustaining human colony on Mars.

This has always been his mission.

He is said to evaluate every problem through the lens of whether or not it brings us closer to the day that we have a sustainable human colony on Mars.



After a few false starts, and near bankruptcy, it was the 28th September 2008 that Musk launched the first privately-funded rocket into orbit.

The Falcon 1

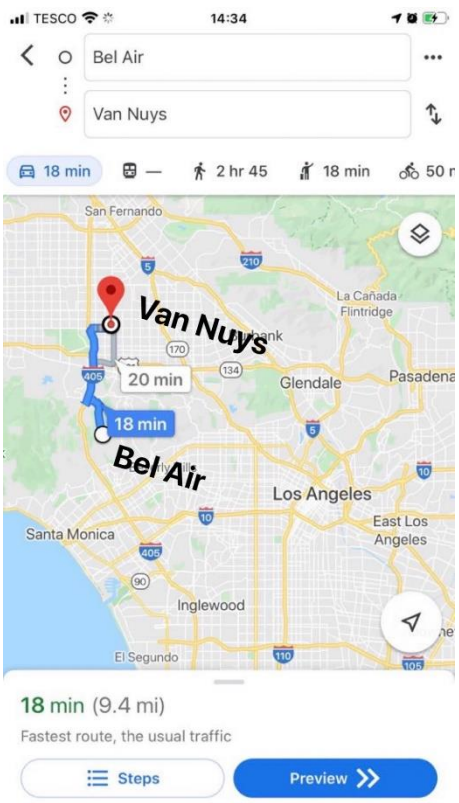
At this very moment, Elon Musk knew that it was only a matter of time before humans reached Mars. So he turned his attention to the next problem. Once humanity reaches Mars, how do we ensure that the civilisation there is sustainable? Once again, Elon was inspired to think about the problem of money.

What would humans use for money on Mars?

He had to solve the problem that PayPal was never able to. The Falcon 1 reached orbit on 28th September, 2008. One month later, on October 31st 2008, the Bitcoin whitepaper was released. Three months after that, the genesis block was mined and the Bitcoin network was live.

Humans on Mars cannot use $, or they'd be reliant on the stability of a nation-state from another planet. They can't use gold, or they'd have to transport it there! They will have to use Bitcoin, a truly scarce digital currency that can be beamed to Mars via satellite. Elon knew it would take time for the Bitcoin network to grow big enough to function properly for a Mars colony. He couldn't wait for SpaceX to put a human on Mars to turn his attention to the problem of money. **He had to solve the problem of money first.**

So Elon had the motivation, experience in thinking about the problem, and the timing works out. What other evidence do we have that Elon is Satoshi? In Bitcoin's early days, bitcoins were sent and received between participants using IP addresses. Bitcoin's debug log reveals the IP address of those users, one of whom is known to be Hal Finney. The other was an address out of Van Nuys, California, a location only 11 miles north of Musk's home in Bel Air.



In one of his early forum posts on http://bitcoin.org, Satoshi Nakamoto responded to a Bitcoin skeptic with:

"If you don't believe me or don't get it, I don't have time to try to convince you, sorry"

No shit he didn't have time, he was busy running SpaceX and Tesla! Satoshi's last post on the Bitcoin forum was 12th December, 2012. Why did he disappear? **SpaceX**. In December 2012, SpaceX announced its first two launch contracts with the United States Department of Defense. Musk's involvement in Bitcoin, now that SpaceX was reliant on the US government, beyond this point could have been detrimental to his long-term mission:

To create a sustainable human colony on Mars.

Besides, Bitcoin didn't need him anymore. Elon Musk invented Bitcoin so that his Mars colony would have a functional currency to transact with.

Elon Musk is Satoshi Nakamoto.

Bitcoin is Mars Money.

Original image credit: Bryan Verstee of spacehabs dot com

Bitcoin and the Conquest of Privacy

By Erik Cason on Citadel21

Posted May 21, 2020

The Personal Decision to Use Cryptography to Protect One's Privacy, Property, and Wealth

"All genuine political theories presuppose man to be evil." - **Carl Schmitt**

Our privacy was never for sale.

We never agreed to be watched, inspected, spied upon, directed, numbered, regulated, enrolled, indoctrinated, preached at, controlled, checked, estimated, valued, censured, commanded, and identified by creatures who have neither the right nor the wisdom nor the virtue to do so.

Through the constant and considerable violations of each and every single one of our constitutional rights, personal dignities, and human liberties; we can see these were to only be taken, never given. In this time of great need, we are seeing that among nation-states around the world, there is no nation to be found where liberties are not threatened, where people are not under the sinister gaze of the digital panopticon with nowhere to hide.

Satoshi Nakamoto was able to understand the total state of emergency that we all live under; as citizens of the modern, technologically advanced state, and how cryptography could help end this emergency. He understood that through cryptography and the protection of privacy it can assure; a new kind of social contract could be created. This social contract would require a new kind of theology, which could offer us protection when no other sovereign power could. Satoshi saw the secret of power that Hobbes always knew to be the true hidden power of sovereigns, and is the only real obligation that any subject has to any sovereign power:

"The obligation of subjects to the sovereign is understood to last as long, and no longer, than the power lasteth by which he is able to protect them. For the right men have by nature to protect themselves, when none else can protect them, can by no covenant be relinquished." - **Hobbes, Leviathan**

What Satoshi Nakamoto created with Bitcoin is a theology of cryptography which guarantees privacy, and the ability to protect one's wealth beyond any physical power. No matter what government rules over you, what state claims you are its citizen, or which currency you are forced to pay taxes with; all may own bitcoin equally without regards to their station of

birth, the laws that claim to command them, or emergencies that are enacted over them.

Bitcoin is a common form of wealth and power that assures privacy beyond any corrupt law. **Bitcoin is an idea whose time has come**, and that nothing can stop. Bitcoin offers itself as a form of economic order that that guarantees privacy through cryptography, and how bitcoin's timechain uses cryptography to verify that all bitcoins are fairly accounted for through its consensus and protocol.

This radical, unstoppable force that is Bitcoin, and the cryptography that empowers it, is not only a new system of wealth and privacy protection; it is the very foundation of a new society.

Bitcoin is an economic order for the internet alone, making banks and fiat money no longer needed, nor desired. It is a new form of digital contract that assures its order through cryptography, and verifies each truth with the work of the timechain. This allows for any person to choose this new system of economic power, to verify the truth of its facts for themselves, and to join the revolution to overcome the old corrupt systems of the dying age of fiat money.

Satoshi understood that in order to restore order once again, he had to find a way to evade the sanction of physical identification. Through the power of cryptography and the personal privacy it guaranteed, Satoshi was able consummate both a new form of wealth and a contract from which order may be restored. **This new order is beyond any sovereign power, as there is no kind of violence, statist or otherwise, that can destroy or change the truth of its timechain.** Bitcoin is a new form of personal sovereign organization that uses cryptography to go beyond the physical power of any nation-state, and the brutishness of their violent powers of law. Bitcoin returns economic power and personal privacy directly to the hands of anyone who chooses to use it. Through choosing bitcoin, anyone can reclaim the rights that are rightfully theirs and become the sovereign owners of their property once again.

Privacy As The Final Banishment of State Law

"If mythic violence is lawmaking, divine violence is law-destroying; if the former sets boundaries, the latter boundlessly destroys them; if mythic violence brings at once guilt and retribution, divine power only expiates; if the former threatens, the latter strikes; if the former is bloody, the latter is lethal without spilling blood." — **Walter Benjamin, Critique of Violence**

This is the power of Bitcoin.

Bitcoin is this divine power that can be lethal to all nation-states without spilling a drop of blood. **It is the non-violent revolution that we have been hoping and praying for.** It is a way for humans to meaningfully reconnect and organize digitally, and anonymously if they choose, against the tyrannies of the modern age. Through using Bitcoin to economically organize ourselves, and the cryptography it contains to protect our personal privacy, we create a new kind of social agreement that is beyond any sovereign power of the modern age.

Bitcoin is a means for anyone to use these memetic techniques of cryptography to protect themselves in a way that no nation-state, no police, no political system can guarantee to its citizens. In every form of state law there is always a chance of a 'state of emergency' in which any person may become an 'enemy of the state' and stripped of their very right to life, liberty, and property for whatever reason the state sees fit.

Through the constant, rampant, and gross violation of all civil liberties by all states to all people; we can clearly see that our personal privacies, rights, and dignity have been totally liquidated by the security state in every form.

We are told these violations are for our own safety and security, and under the pretext of public utility; in the name of the general interest, we are to be fleeced, exploited, monopolized, extorted, robbed; and then, at the slightest resistance, the first word of complaint, the first utterance of 'No!' to be repressed, fined, vilified, harassed, hunted down, disarmed, bound and imprisoned.

That is government today; that is its justice; that is its morality, and that is the crime that they want us to roll over and simply take.

And it is in this very same vein that we should totally and completely reject whatever fiat money our respective government's print, whatever amount they offer to bribe us as common whores. They have no right, nor any claim over the kind of wealth each of us should choose. Through rejecting their disgusting and corrupt money with Bitcoin, and blinding their violating technology with cryptography, we can reject these corrupt monetary, economic, and political systems.

Using the technology of Bitcoin and asymmetric cryptography to organize ourselves, **we WILL win the new territory of freedom that Satoshi spoke of**. A territory where our privacy will truly be preserved, our property protected, and our order guaranteed through the oath that is Bitcoin, and the power of cryptography, but only if we can keep it. There is only one chance to encrypt the internet and preserve it as a bastion of freedom and liberty for all future generations - and **that time is NOW**!But only if we can keep it!

The Coming War Over Privacy

The war for privacy is already here, and they are already spying on you, cataloging your data for the day they choose to use it against you. The question is what are you going to do about it? Do you let them take everything, or do you choose to fight back? Bitcoin offers an answer to this question, and it is the final power which will allow anyone to throw away the yoke of economic slavery and corrupt, violating state powers.

As this conquest of privacy evolves, it will come to the inevitable, dangerous, and insane conclusion that all people, everywhere, should always be monitored and spied upon, 'for the safety and security', of the state. Only the most sinister and evil deeds may be produced through such radical authority.

Good intentions will always be pleaded for every assumption of authority. The Constitution was made to guard the people against the dangers of good intentions. There are men in all ages who mean to govern well, but they mean to govern. They promise to be good masters, but they mean to be masters.

It does not matter if there is good in their heart initially; as the machinery of politics will turn the hearts of men into cold stone; it will make evil become a reasonable thing. **We must remember that we are dealing with men, not gods** - we should not expected godly behavior from them. And as all of history will tell us, rights that are freely given are not won back so easily.

This is why it is so imperative for us, as free people of this earth, to banish such tyrannical and banal authoritarianism from this planet once and for all. To complete the final messianic task where man takes his rightful place as the master of himself, for himself alone. This task is not just to save us from the evil that is the global total surveillance system that all governments are becoming; but to redeem us from the fall of humanity and the grievance that all contemporary forms of politics have become.

We now have the means, the technology and the kind of economic security to create this radical privacy, and the time to act is now! Bitcoin allows for us to create a radical, and totally new form of politics using the internet as its heart, Bitcoin as its mind, and privacy as its soul. As with the production of the medieval commune of the 11th century, and the nation-state that came from the Peace of Westphalia in the 17th century; we are on the cusp of a totally new kind of human organization that can change the course of human history forever.

If we are to live as free people, to have the liberty and dignity to discuss and decide exactly what freedom and liberty means; we must have the power to

protect our privacy and property against state power and any emergency they enact.

Through the power of cryptography, and the dignity that is Bitcoin, we have a chance to stop this psychopathic system of rampant economic corruption that has defiled and debased our system of politics across the globe.

With Bitcoin as our mutual form of money, and foundation for our new social contracts, we can change everything.

Why Bitcoin might not survive a Bitcoin Standard

By Hasu on Deribit Insights

Posted May 25, 2020

Bitcoin allows users to store and transfer value without trusting any third party. However, these assurances are constrained to 4400 transactions per block (more, if you count one-to-many payments). All else equal, Bitcoin's capacity is constrained by the block size. The current block size limit exists for technical and incentive-compatibility reasons that are unlikely to go away soon.

Some people posit you can scale Bitcoin by increasing the blocksize. While that would allow more transactions, the assurances of these transactions would be worse. Consequently, Bitcoin protects its properties by excluding usage beyond the safe capacity limit. Over time, the safe capacity limit can be expanded, for example via additional layers like Lightning.

I'd like to challenge this orthodoxy by saying **Bitcoin's ability to exclude users is smaller than commonly assumed**. While Bitcoin can control the number of users inside the network, it has no control over the number of users accessing the network through custodial banks. The growth of this banking layer is outside of the protocol's control and could grow into a systemic risk for Bitcoin.

Users adopt custodial banks because they offer lower transaction cost over a variety of dimensions. These can include stronger network effect, faster payment clearing, legal recourse, lower transaction fees, or access to financial services like exchange or money markets.

A popular vision today is that the future "Bitcoin stack" will consist of different layers that represent unique points on a trust/cost graph. If higher layers break down, users can retreat to lower layers.

In this article, I will show **how a custodial banking layer creates systemic risk for Bitcoin.** Then, **what drives the growth of the custodial banking layer**, and finally, **how a negative outcome for Bitcoin could be prevented**.

How a custodial banking layer creates systemic risk for Bitcoin

Imagine a future where 200 million people use Bitcoin, most of them via the custodial banking layer. These banks use the base chain as an interbank settlement network. Users trade in Bitcoin IOUs representing bitcoin deposits.

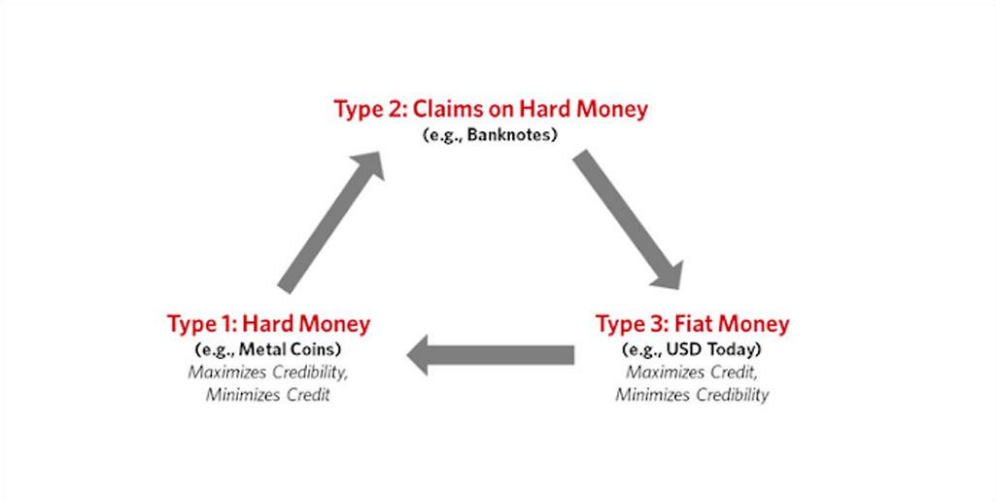
The long-term stability of this arrangement is a matter of who has leverage over whom. If users can leave at any time and go to a competitor (including the trustless layers of the system), the custodial banking system is kept in check. But if users are locked in, then the power resides with the banks (and thereby governments). **Whether users are locked in or not depends on the exit cost from the system**.

Manual exit cost

When governments can come in and cancel the redeemability for bitcoin, this may be seen as jacking the exit cost from the system to infinity. Governments may find it difficult to control the network layer itself, but in this example they don't need to at all. They **already control the banks**.

This is what happened in 1933 to the gold of US citizens and in 1971 to the gold of other nation-states held within the domestic US.

If redeemability is canceled, Bitcoin completes the transition back to fiat money based on Dalio's chart of the long-term debt cycle.



Source: Linkedin

Notably, this is not a scenario where users could "UASF" or respond in any other way at the protocol level since the rules of the Bitcoin standard still abide by the rules of the Bitcoin protocol. Users allowed it to become a political problem that now requires a political solution.

Organic exit cost

In practice, governments may not even have to cancel redeemability for bitcoin, because the exit cost can grow very large organically.

Take a bank run scenario where all 200 million people, or at least a significant part of them, wanted to leave the banking system and move down the stack to a more trustless layer. Some of them can successfully make the transition, but they would be the winners of an auction that jacks transaction fees to the thousands to tens of thousands of dollars. The rest would be left behind on the higher layer.

If a higher layer grows too large relative to the capacity of the lower layer, people **lose the optionality of moving back down the stack**. As users find themselves permanently locked into the higher layer, governments can safely implement a variety of taxes or rule changes in the system.

What drives the growth of the custodial banking layer

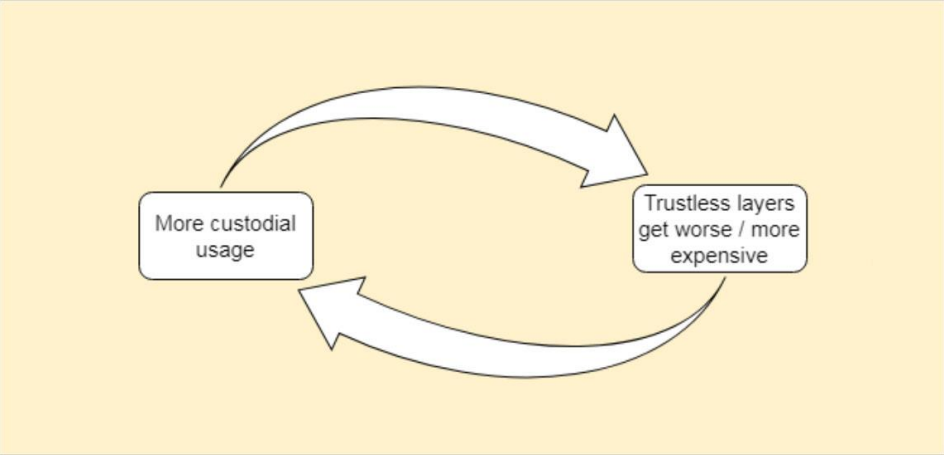
People use higher layers because they offer them more favorable points on the trust/cost spectrum. Remember that "cost" includes many things, not just transaction fees. It also includes network effect, settlement time, reversibility, privacy, etc.

I'm afraid there exists **a feedback loop that makes custodial layers more attractive the larger they become, driving further users to them**.

This can be first shown with an example from the gold standard. Every user of gold competes with other users in the market place. If they can settle debts sooner rather than later, suppliers are more willing to do business with them. If banking can give them lower fees, they can forward this price saving to their trading partners. The result is a feedback loop where users migrate to the cheapest solution over time.

The benefits of using a bank ledger are local and immediate, whereas the downsides are global and often happen with decades of delay.

The same feedback loop exists in Bitcoin, but arguably in an even stronger way. If the custodial banking layer becomes very successful, imagine that all these settlement transactions drive up the transaction fees on the base layer. Suddenly, **more and more people become priced out of using trustless layers at all**. The custodians can afford to pay more for the base layer space because their transactions represent the bundled interest of thousands of users off-chain.



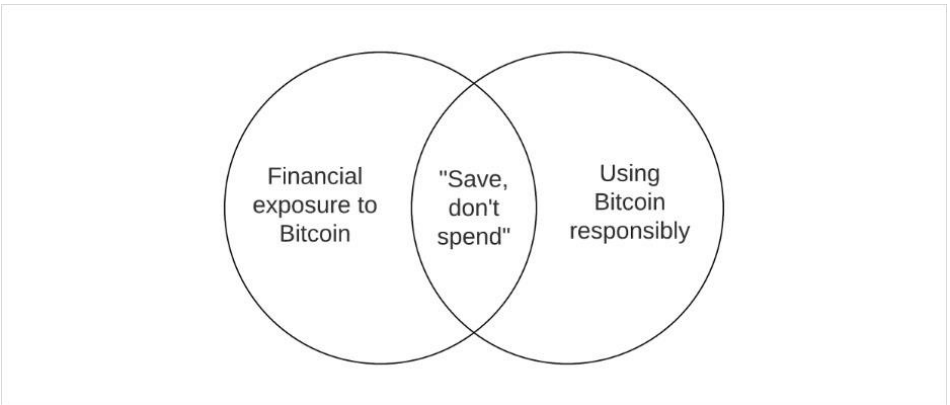
As a result, formerly noncustodial users can find themselves facing the option to use custodial options or stop using Bitcoin altogether. This also holds, for an only slightly lesser degree, for the Lightning Network, where you can't safely route payments smaller than 3.5x the on-chain fee limit.

Interestingly, the feedback loop can still hold if transaction fees are very low. The reason is, again, that fees represent merely one aspect of the overall transaction costs. If the security budget of the main chain is very low, settlement times could become very excessive. This further increases the relative advantage of custodial off-chain solutions like banks.

How a negative outcome for Bitcoin could be prevented

I see two ways to minimize the systemic risk from a custodial banking layer.

First, the community can **discourage users from adopting IOUs on a large scale**. This involves constructing a narrative where new users can still get financial exposure to Bitcoin, but not use it in a way where banks have a leg up on the trustless layers.



Arguably, this has already happened in the last couple of years and shows how well the Bitcoin community instinctively understands that Bitcoin's assurances degrade for everyone if too many people use it in the wrong way.

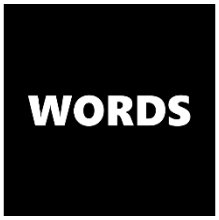
Second, we need to continue to **innovate and expand Bitcoin's trustless capacity to more users**. Specifically, we need to pioneer ways for multiple users to share a single UTXO, so they can also bundle their interest and survive in the on-chain marketplace for blockspace with custodial banks.

There is an implicit assumption in Bitcoin that users will pay more to use the base layer or its trustless extensions like the Lightning network. In practice, Bitcoin doesn't just compete with fiat money or even other cryptocurrencies, but also with custodial Bitcoin banks.

I would still firmly count myself as a "small-blocker", but the analysis raises some doubt whether keeping validation costs low is as effective as commonly assumed. You can have a low validation cost but become forced into custodial layers by high transaction fees, very long settlement times, or other cost factors.

Many in Bitcoin believe there is a big risk in moving too fast, but hardly any risk in moving too slow. This would be true if Bitcoin could grow at its own pace, but it can't. We **must make sure that enough demand from the market can be met with trustless capacity, or risk that the custodial banking system will forever encumber the base layer**.

Disclaimer:



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