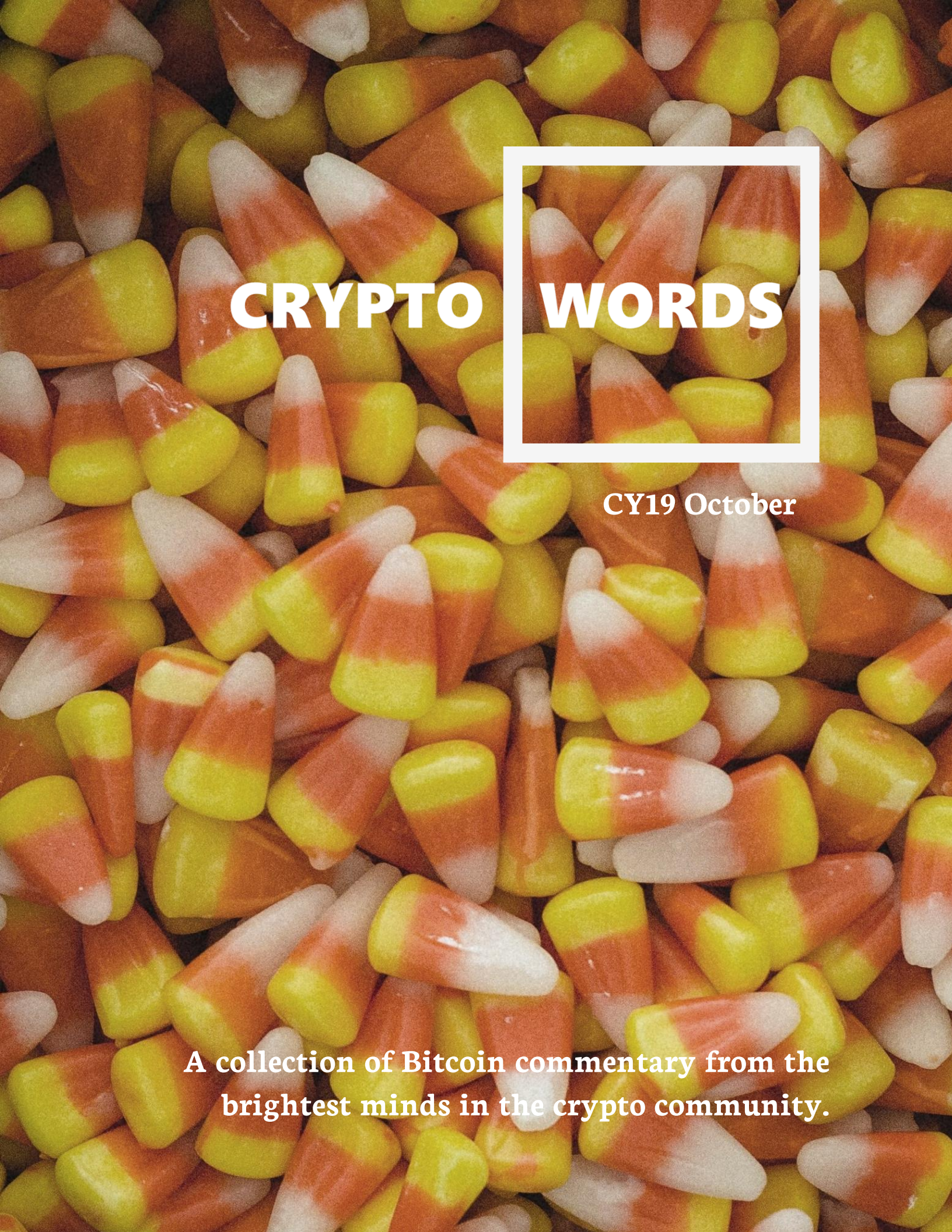


CRYPTO WORDS

CY19 October

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

Contents

Goals and Scope 2
Support Crypto Words 3
Bitcoin Equals Freedom 4
Tweetstorm: On making Bitcoin easier 10
Reddit Response: Question on the Vulnerability of Bitcoin 11
The Monetary Case for Bitcoin 13
Crypto without Criticisms 36
The Startup Government 39
Bitcoin is for Stackers 44
Money and time 45
Bitcoin is Not a Pyramid Scheme 48
Tweetstorm: 5 Insanely Bullish Charts for Bitcoin 65
A Fossil Fuel Future for Bitcoin Mining 68
The Legend of Satoshi Nakamoto 82
All 21 Million Bitcoin Already Exist 85
Tweetstorm: The Matrix 93
Tweetstorm: Plot Twist 102
Disclaimer: 103

Goals and Scope

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

History

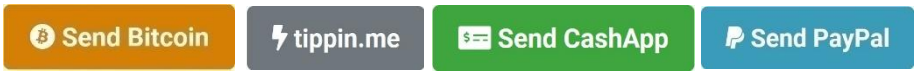
There exists a gap in Bitcoin publishing. For authors with commentary and scholarly papers on topic, the choice of publication outlets is relatively limited. The number of journals that serve as outlets for crypto research is in any event too small, as the number of crypto thinkers continues to grow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

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

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

Support Crypto Words

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



Spread the word

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

Follow us on social media

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

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

Subscribe to our newsletter

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

Our pledge

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

Bitcoin Equals Freedom

By Ross Ulbricht

Posted September 25, 2019

Something special happened in the first year or so after Satoshi gave us Bitcoin, something no one expected and many thought was impossible. Try to imagine Bitcoin back then, before you could buy things with it, before there was an exchange rate, before anyone really knew what, if anything, would happen with it. Bitcoin didn't start out as money. It became money, but it did so unlike any money that came before it. For all the things Bitcoin has made possible, for all the ways it is changing our world, we don't fully appreciate or even understand what happened in those early days, when it was just a play thing for geeks.

Every other money that predates Bitcoin — in the long history of human civilization — was valued for reasons other than its use as money. Cattle in Africa, postage stamps in prison, sea shells and precious metals all have been used as money and fit this pattern. The only exception is fiat money — something declared to be money by an authority — but even national fiat currencies were once backed by something with prior value, like gold.

Bitcoin changed all that. Bitcoin had no prior value, and no one was forced to use it, yet somehow it came to be a medium of exchange. People who don't understand and care little for Bitcoin can nevertheless accept it as payment because they know it can be used to pay for something else or be exchanged into conventional money.

People often mention the pizzas that were bought for ten thousand bitcoins and, in hindsight, poke fun at the guy who ate what would become a multi-million dollar lunch. I'm more interested in the person who gave up two perfectly good pizzas for mere bitcoins. What did he see in those bits and bytes, that digital signature on something people were calling a blockchain? Whatever motivated the pizza seller may have also called to the early miners who could not liquidate but happily hoarded. It may have inspired the ones who simply gave bitcoins away by the thousands. Whatever it was, it was something new.

Classical economics says exchange won't happen unless both parties value what they are getting more than what they are giving up. So where did the value come from? Bitcoin should never have gotten off the ground, but it did. Even a new product has some kind of value to it, and early adopters are taking a risk that they won't get their money's worth, but they still expect to gain from the exchange.

The early adopters of Bitcoin, on the other hand, had no way of knowing that we do now. All they had was a dream, a conviction and enough infectious enthusiasm to bootstrap a digital contrivance into a multi-billion dollar phenomenon we are only beginning to see the effects of.

I'll tell you what I think happened, but the truth is no one knows. It is like magic that Bitcoin could somehow come from nothing, and without prior value or authoritative decree, become money. But Bitcoin did not appear in a vacuum. It was a solution to a problem cryptographers had been struggling with for many years: How to create digital money with no central authority that couldn't be forged and could be trusted.

This problem persisted for so long that some left the solution to others and dreamed instead of what our future would be like if decentralized digital money did somehow come to be. They dreamed of a future where the economic power of the world is accessible to everyone, where value can be transferred anywhere with a key stroke. They dreamed of prosperity and freedom, dependent only on the mathematics of strong encryption.

Bitcoin was therefore birthed onto fertile ground and was recognized by those that had been waiting for it. This was an historic moment for them, far more important than pizzas or electric bills run up from mining. The promise of freedom and the allure of destiny energized the early community. Bitcoin was consciously, yet spontaneously taken up as money while no one was watching, and our world will never be the same.

Bitcoin Equals Freedom
by Ross Ulbricht

Something special happened in the first year or so after Satoshi gave us Bitcoin, something no one expected and many thought was impossible. Try to imagine Bitcoin back then, before you could buy things with it, before there was an exchange rate, before anyone really knew what, if anything, would happen with it. Bitcoin didn't start out as money. It became money, but it did so unlike any money that came before it. For all the things Bitcoin has made possible, for all the ways it is changing our world, we don't fully appreciate or even understand what happened in those early days, when it was just a play thing for geeks.

Every other money that predates Bitcoin—in the long history of human civilization—was valued for reasons other than its use as money. Cattle in Africa, postage stamps in prison, sea shells and precious metals all have been used as money and fit this pattern. The only exception is fiat money—something declared to be money by an authority—but even national fiat currencies were

once backed by something with prior value, like gold.

Bitcoin changed all that. Bitcoin had no prior value, and no one was forced to use it, yet somehow it came to be a medium of exchange. People who don't understand and care little for Bitcoin can nevertheless accept it as payment because they know it can be used to pay for something else or be exchanged into conventional money.

People often mention the pizzas that were bought for ten thousand bitcoins and, in hindsight, poke fun at the guy who ate what would become a multi-million dollar lunch. I'm more interested in the person who gave up two perfectly good pizzas for mere bitcoins. What did he see in those bits and bytes, that digital signature or something people were calling a blockchain? Whatever motivated the pizza seller may have also called to the early miners who could not liquidate but happily hoarded. It may have inspired the ones who simply gave bitcoins away by the thousands. Whatever it was, it was something new.

Classical economics says exchange won't happen unless both parties value what they are getting more than what they are giving up. So where did the value come from? Bitcoin should never have gotten off the ground, but it did. Even a new product has some kind of value to it, and early adopters are taking a risk that they won't get their money's worth, but they still expect to gain from the exchange.

The early adopters of Bitcoin, on the other hand, had no way of knowing what we do now. All they had was a dream, a conviction and enough infectious enthusiasm to bootstrap a digital contrivance into a multi-billion dollar phenomenon we are only beginning to see the effects of.

I'll tell you what I think happened, but the truth is no one knows. It is like magic that Bitcoin could somehow come from nothing, and without prior value or authoritative decree, become money. But Bitcoin did not appear in a vacuum. It was a solution to a problem cryptographers had been struggling with for many

years: How to create digital money with no central authority that couldn't be forged and could be trusted.

This problem persisted for so long that some left the solution to others and dreamed instead of what our future would be like if decentralized digital money did somehow come to be. They dreamed of a future where the economic power of the world is accessible to everyone, where value can be transferred anywhere with a key stroke. They dreamed of prosperity and freedom, dependent only on the mathematics of strong encryption.

Bitcoin was therefore birthed onto fertile ground and was recognized by those that had been waiting for it. This was an historic moment for them, far more important than pizzas or electric bills run up from mining. The promise of freedom and the allure of destiny energized the early community. Bitcoin was consciously, yet spontaneously taken up as money while no one was watching, and our world will never be the same.

Tweetstorm: On making Bitcoin easier

By Beautyon

Posted October 1, 2019

You can use your iPhone or Droid to do many wonderful things without knowing anything about how they work or who built the software. Billions of people do this trillions of times a day. Why does anyone think billions of people are going to read a book to know how to use Bitcoin?

The idea that people need to know the theories behind Bitcoin or who wrote it is absurd. This artificial requirement and recommendation is only for the extreme stratospheric reaches of the global elite (Bitcoin Twitter) but not for the public, who shouldn't be required to think.

All consumer electronics are similarly layered with generations of innovation and super complex concepts and techniques. The "Smart TV" is a perfect example. https://youtube.com/watch?v=yZV46Q_yTs0 what this represents is incomprehensible to all but a tiny handful of experts yet millions use it.

For Bitcoin to succeed, it too must packaged in a way that removes the need for anyone to understand how it works. There is nothing wrong with this, and it will be a difficult task to achieve. Rest assured it will get done, because the need for Bitcoin is greater than you think.

Once people experience just how simple it is to send money with Bitcoin, they'll never EVER return to the horrific experience of dealing with banks and their terrible, horrible, invasive, insulting, broken tools and services. And you don't need to have read Hayek to know that!

Reddit Response: Question on the Vulnerability of Bitcoin

By Greg Maxwell

Posted October 5, 2019

I think questions like this are ultimately the result of a fundamental lack of understanding about what Bitcoin is doing.

The problem Bitcoin is attempting to solve is getting everyone everywhere to agree on the same stable history of transactions. This is necessary because in order to prevent users from printing money from nothing the system must have a rule that you can't spend a given coin more than once– like I have a dollar then pay both alice and bob that dollar, creating a dollar out of nothing.

The intuitive way to prevent that excessive spending is to decide that first transaction that spends a coin is valid and any additional spends are invalid. However, in a truly decentralized system "first" is actually logically meaningless! As an inescapable result of relativity the order which different parties will perceive events depends on their relative positions, no matter how good or fast your communication system is.

So any system that needs to prevent duplication has to have a way to artificially assign "firstness". Centralized systems like ripple, eos, iota, blockstream liquid, etc. just have a single party (or a virtual single party) use its idea of whatever came first and everyone else just has to accept its decision.

A decentralized system like Bitcoin uses a public election. But you can't just have a vote of 'people' in a decentralized system because that would require a centralized party to authorize people to vote. Instead, Bitcoin uses a vote of computing power because it's possible to verify computing power without the help of any centralized third party.

If we didn't have the constraint that this system needed to work online, then you could imagine an alternative where consensus could be determined by people presenting large amounts of some rare element. … but you can't prove you control osmium online, it appears that computing power is the only thing that can work for this purpose online.

When people talk about "51%" all they're really talking about is people rigging that election, so that they can override what everyone previously thought was the accepted order of transactions with a new order that changes some of their payments from one party to another.

With this understanding maybe you can see that the concern doesn't even depend on a single person having too much of the hash-power. The attack would work just as well if there were 100 people each with an equal amount and a majority of them colluded to dishonestly override the result.

Also, any mechanism that would let you prevent one party (much less a secret collusion) from having too much authority would almost certainly let you just replace mining entirely. The only known way to do that is to introduce centralization and if you're willing to do that it's trivial, if you're not it appears impossible. People have cooked up 1001 complicated schemes that claim to do it without introducing centralization, but careful analysis finds again and again that these fixes centralize the system but just hide the centralization.

I think people obsess far too much about "51%"– it has some kind of attractive mystery to it that distracts people. If you're worried that someone might reorder history using a high hash-power collusion– just wait longer before you consider your transactions final.

A far bigger risk to Bitcoin is that the public using it won't understand, won't care, and won't protect the decentralization properties that make it valuable over centralized alternatives in the first place. … a risk we can see playing out constantly in the billion dollar market caps of totally centralized systems. The ability demonstrated by system with fake decentralization to arbitrarily change the rules out from under users is far more concerning than the risk that an expensive attack could allow some theft in the case of over-eagerly finalized transactions.

The Monetary Case for Bitcoin

By Ben Kaufman

Posted October 5, 2019

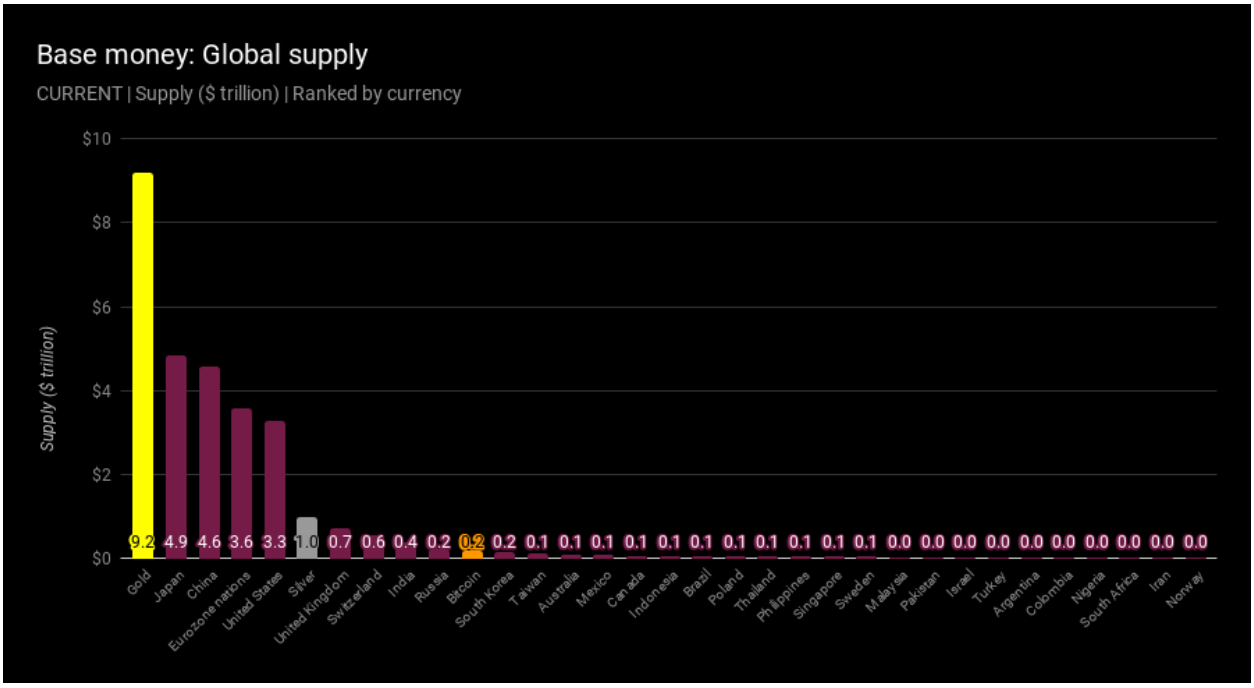
The introduction of Bitcoin to the world ten years ago as a new monetary system sparked new interest in the field of monetary economics. After a century of fully nationalized money production systems, and about five decades of an irredeemable national paper money standard, the battle for sound money seemed to be long lost. A return to gold, even within the circles of Austrian and free-market thinkers, became an increasingly less practical approach, and it seemed there was little left to do but wait for the inevitable collapse of the contemporary system, to which we arguably came close several times.[1] The fight in the intellectual arena was seemingly over as well, both from the academic view and the general public acceptance. With very few exceptions, such as with the case of Friedrich Hayek, most prominent economists acknowledged by public endorsement were followers of the Keynesian monetary approach. Thus endorsing monetary nationalism[2], and the enactment of legal tender paper money, as both a cost-efficient alternative to gold and as a device for government financing and "fine-tuning" of the national economy.

At the same time, while the public and academic fights for sound money could be declared lost, the rise of new technology has opened up a new frontier, and the search for a digital monetary alternative began. A small unorganized group, composed mainly of individual computer scientists and cryptographers, called Cypherpunks, started looking into the new possibilities computer networks and cryptography could provide for liberating people, which included the effort of creating open digital money. With the pioneering works of David Chaum (DigiCash) with digital payments, and with such various later research and practical initiatives, most notably of Adam Back (HashCash), Wei Dai (b-money), Nick Szabo (BitGold) and Hal Finney (RPOW), the attempts at introducing digital cash started piling up. These efforts, though nonetheless

interesting for their merit, all failed to either deliver a working system or gain sufficient traction to have any considerable impact on monetary affairs.

The introduction of Bitcoin, around late 2008, can arguably be marked as the most important turning point in monetary affairs since 1971, when the collapse of the Bretton Woods system occurred and led us to the irredeemable paper standard of today. Though not at all immediate, the growth of Bitcoin as a new form of money started to accelerate. Now, about ten years after its inception, it regularly makes it to the news headlines and has even reached US Congressional discussions. The wild success of Bitcoin consequently drew a lot of attention to the area of monetary economics and reignited the lost battle for sound money.

At first, Bitcoin received but insignificant attention and skeptical reactions from both sides, which considered it to be no more than a bubble or a passing trend. However, as time passed, and with Bitcoin growth accelerating with each passing year, it started receiving some attention, making its intellectual allies and rivals. From all economic schools, the phenomenon of Bitcoin seemed to be compatible only with the theory of the Austrian school. There, it is currently still debated with strong enthusiasm between its many supporters and skeptics. On the other hand, within all other economic schools, Bitcoin is still considered mostly as a bubble, a “market irrationality” or a trend about to collapse. The incompatibility of Bitcoin, as money not backed by the authority of the government, with their economic theories in general and their ideas on monetary economics in particular, blinded them to the mere possibility of new money like Bitcoin emerging. Despite the rather small (but growing) support, and strong opposition from the academic circles, Bitcoin has continuously progressed and established its monetary status as more economically significant than many national currencies.[3]



The market cap of Bitcoin compared to other national currencies and precious metals. Source: https://cryptovoices.com/basemoney

At this point, it has become clear that Bitcoin can no longer be ignored, but should rather be studied and investigated thoroughly. It seems that understanding its nature may expose both the reasons for its success, and a rough expectation for what its future holds. Throughout the previous two articles[4], I outlined some of the foundations for understanding the economics of money, its nature and substance, from the perspective of the Austrian school. We started by looking into the nature of money as the most saleable commodity, that which imposes the least economic costs on its holders for future exchange. We then continued by exploring the various factors influencing the saleability of commodities, and therefore their likelihood to emerge as money on the market.[5] In this article, we shall utilize this understanding and apply it to the case of Bitcoin, exploring the case for Bitcoin from the view of monetary economics.

Bitcoin's Monetary Properties

The common monetary properties influencing the suitability of a commodity to be money, such as its divisibility, portability, and durability, are usually inherent to the physical composition of the commodity itself. The physical limitations resulting from this have affected the specific substance of money to a large extent throughout the years. For example, the physical limitation of dividing gold into small enough denominations as to be used for low-value transactions prevented its (physical) use in many exchanges, forcing people to

resort to such less valuable metals as silver and copper, and later also to money certificates.

The emergence of Bitcoin as the first digital form of money allowed us to bypass those "physical" limits of money, and scale them to the almost non-existing limits of the digital realm. Understanding how Bitcoin allows us this improvement of monetary properties requires a basic understanding of how it works, and how Bitcoin is digitally represented. Bitcoin, in its "rawest" form, is a piece of software which automates the achievement of consensus over the ownership of (the conditions under which one is allowed to spend) units of Bitcoin. In other words, Bitcoin in this raw form is a list of spendable amounts and the conditions for spending them.

Since Bitcoin, unlike previous monetary assets, is not based on physical ownership, but on the consensus on its spending conditions, we should separate our discussion of its limitations into two consensus layers. The first, which is commonly termed the "on-chain" layer, is the global consensus layer which we just described, and we may think of it as the ultimate source of truth for determining ownership over Bitcoin units. From its nature as a global consensus layer, binding for all its participants, it is relatively rigid and restrictive. Thus it provides us with a somewhat moderate degree of improvement in terms of the monetary properties. For example, the divisibility of Bitcoin here is limited up to a single "satoshi," which is equivalent to a hundred millionth of a Bitcoin. The process of division itself requires changing the spending conditions assigned to the associated units, meaning they need to be "spent" to divide them. We may notice that, despite the unit size limitation, it is possible to scale it, if necessary, through a change in the global consensus mechanism. Such changes, though extremely hard and costly to perform, are nonetheless feasible, and provide us with a certain level of improvement to the asset itself as new needs arise over time.[6] The ability to change those technical monetary properties of the asset is an unprecedented capability which Bitcoin introduced, and already gives it a significant advantage over its predecessors.

The second, called the "off-chain" layer, utilizes the nature of Bitcoin both as a consensus-based digital asset, and as programmable software, allowing cooperating individuals to create a "subset" of the consensus of Bitcoin, and to transact within that subset using various mechanisms. If we look at the portability of Bitcoin as an example, while it is unarguably cheap and easy to move between physical locations, the transfer of actual ownership (change in spending conditions) of Bitcoin on the on-chain layer is somewhat constrained, allowing roughly about 600,000 final settlements (ownership transfers) per day. However, as transactions are usually made between cooperating entities wishing to make the transaction go through, the off-chain layer allows them to use various constructions for achieving consensus. Thereby, it enables them to

scale the transaction capacity to the nearly infinite limits of the physical movement of electronic data. There are many options for such constructions, a lot of which are currently under research and development, with each of them offering widely different tradeoffs for the transacting entities. Prominent examples are the "Lightning Network,"[7] which offers trustless and instant transactions, with mostly some liquidity limitations, and "sidechains" such as "Liquid," which provide benefits like high-speed and confidential transactions, and asset issuance with the tradeoff of introducing trust in a federation of trusted entities which manage the consensus subset for their clients.

In conclusion of the analysis of the monetary attributes of Bitcoin, we see how the transition of the monetary asset from the physical into the digital realm allows us not only for unprecedented improvements but also a high level of flexibility in the monetary properties of the asset. Therefore, we may conclude here that Bitcoin, from the perspective of its "inherent" properties, is unprecedentedly superior to all its predecessors. With this in mind, it seems that Bitcoin deserves a further investigation of its suitability as money. We will thus continue with what is probably the most controversial and innovative aspect of Bitcoin, its production and supply.

Bitcoin Production

Before Bitcoin, the challenge of producing digital money on the market seemed almost impossible from the view of monetary economics writers. Prof. Jörg Guido Hülsmann, an Austrian economist focusing on monetary economics expressed this widespread belief in one of his books. He states that "an economic good that is defined entirely in terms of bits and bytes is unlikely ever to be produced spontaneously on a free market."[8] Coincidentally, he published this on October 2008, two months after the whitepaper of Bitcoin was first published, and about three months before the first bitcoins came into existence.

The invention of Bitcoin indeed required finding a solution to what was up to that point an unsolved problem, the ability to produce digital scarcity with controllable supply (solving the "double spending problem"), without depending on a trusted entity. The creator of Bitcoin solved this by introducing the mechanism now commonly referred to as "Nakamoto Consensus,"[9] which is the solution for the discussed problem. The basic idea is to have an open competition between computers over finding a solution to a mathematical challenge. This challenge is similar to a random lottery in the sense that the only known way to find a solution is through random guessing, and the chance for discovering a solution remains the same for every guess. This process requires the expenditure of computation power, which is mostly limited by the availability of energy for the computing machines. Adam Back has initially proposed a similar process as part of the HashCash system in 1997. Bitcoin

works similarly to that proposed mechanism, but a critical point where Bitcoin improves over this proposal is with the ability to set a strict schedule for the production of new units. Bitcoin achieves this by using a peer to peer consensus network (which we discussed above) to enforce and validate the monetary rules and schedule, and an automatic periodical adjustment to the computational work needed for producing new units which adjusts the difficulty of the challenges, and thus the speed of production as to match the schedule.

Unlike previous monetary assets, such as gold, silver and seashells, which relied on particular physical limitation and scarcity for their production, and also unlike the current fiat paper monetary system, which relies on a trusted issuer (the central bank) for the production of money, Bitcoin relies on a purely mathematical system for its production. This characteristic allows for an objective and universal way for auditing the validity of a unit of Bitcoin and enables a fair and open competition on its production. Anyone is free to participate (and stop participating) in this competition by expending computation power, having a probabilistic chance to produce Bitcoin directly proportional to the computation they spent.

Money Production and Externalities

Historically, the production of the substance of money was always costly, both from a direct and indirect perspective. Cattle for example, which were used as money in lots of nomadic societies, were expensive to raise ("produce") and resulted in some entirely unexpected externalities, mainly due to the great need for graze-lands required for growing them.[10] Gold, as another example, is also very costly to produce, as its mining process requires filtering out many tons of dirt just to obtain a small quantity of it. Its externalities are quite unpleasant as well, as the military seizure of gold mines and the dangerous and sometimes forced labor it involves present us with multiple economic and ethical issues.

Marco Polo was perhaps the first to introduce the seemingly impressive concept of paper money, which he observed in China, to the western world.[11] Since he made that discovery, the appetite of rulers, bankers and intellectuals for easy money has been continuously growing. The first European experiment with easy paper money was when in 1661 the Swedish central bank, Stockholms Banco, started issuing banknotes. The practice then led to the bankruptcy of the bank just three years later, but this failure seems to have only increased the desire for more such experimentations on the part of rulers and bankers. As for intellectuals, the desire to make the production of money more "efficient" was evident from the very beginning of the field of political economy. The idea indeed finds support with such early economists as Adam Smith and John Law, which saw the use of precious metals as an inefficient

process.[12] They, along with many other economists, especially from our current time, sought to make money production cheaper, thus more efficient, by replacing its substance with such cheap alternatives as paper. They believed that such an alternative monetary system could function just as well as that of precious metals, only with a fraction of the production costs. This difference between the production costs and the "face-value" of the money is what we may term as "easy" money, which we should distinct from "hard" money. Thus from this superficial point of view, the difference is that easy money has seemingly insignificant costs for its production, while hard money is expensive to produce.

The problem with easy money, and the reason which such theoretical supporters of it as David Ricardo opposed its implementation[13], is its externalities, the hidden costs and risks which it involves. It is well known and agreed that truly easy money could never emerge on the free market. That is because, for any commodity, market participants will be willing to increase their production and its costs up to the point where it is no longer profitable to increase production. This means that if we were to attempt and install an easy monetary system on the free market, the market participants would start producing it in such quantities as to make the value of each money unit roughly equal to its production costs, canceling the intended "efficiency" of the easy money. Thus, all attempts to introduce an easy money system required the state to assign a monopoly privilege over money production to a specific entity, commonly known as the central bank. With the market participants legally prevented from participating in money production, supporters of easy money believed they could successfully reduce the costs of money production to the mere printing costs of paper notes.

However, this almost obsessive look on the direct and highly visible costs for money production has blinded those economists to the many non-obvious costs easy money imposes. First, and probably the most obvious concern, which was expressed by Ricardo, was the risk for the abuse of the system. From the many hyperinflation scenarios to the less notable moral hazards,[14] the trap of easy money introduced various risks and was abused many times by those in a position to do so. This issue alone should make the trap of easy money clear. It gains small efficiency while introducing fatal risks and many points of moral hazard. However, there are two more aspects where the fallacy of cheap money is exposed.

The second aspect we may look at is the actual costs of operating such a system. With the large bureaucracies typical to all public institutions, and with hundreds of thousands of central bank workers, it is hardly disputed that the supposedly "cheap" and efficient paper money system of today is really more efficient compared to hard money.[15] Along with this consideration, we should also note that the production of gold for monetary purposes still continues to a

large extent. Therefore, these extra costs of the cheap money system come mostly in addition to, not instead of, the costs of the previous hard money one. The issue gets even worse when we understand the important fact that while regulations excluded market participants from direct money production per se, those will still expend as many resources as is still profitable on forecasting and influencing the policies of the central banks. The supporters of easy money have evidently failed to take into account the willingness of market participants to still make the most out of money production, and the jobs of many analysts, economic forecasters and lobbyists are the results of this indirect inefficiency of easy money.

The third and most critical issue that easy money causes is the manipulation of the market process. The market uses money as a tool for resource allocation, with money holders directing the market according to their needs and demands. However, when using easy money, its producer (the central bank) has the power to disproportionately influence the allocation of resources. In fact, we can say it practically takes control over the market, as it can cheaply create money for itself to direct resources as it wishes. Thus, in an easy money economy, the power to allocate resources shifts from the market to those who control the central bank. This distortion of the market gradually shifts the entire economy into indirect central planning. Combined with the moral hazards involved with cheap money production, this process accelerates even further, with the ensuing destructive consequences of economic central planning, disguised under the pretense of a market phenomena.

Easy money, as we see, does not reduce the costs of money production, neither does it make it more efficient in any other sense. The only function it fulfills is to reduce the directly visible costs of money production, while disproportionately increasing the hidden, non-obvious ones. We can draw two main conclusions from this analysis. The first and more obvious one, is that easy money is not only inefficient but may even be destructive due to its risks and externalities. Second, we can notice here that we should aspire to have the process of money production be obvious and transparent, as to minimize such risks and unexpected externalities.

When looking at Bitcoin, one of its remarkable features is its process of production. The most significant and costly part of producing Bitcoin, as discussed above, is the process of turning energy into electricity, and converting this into computational power. While all types of production require the use of energy, most other processes require applying it in very indirect methods, and more importantly, at highly specific locations. The production of gold, for example, requires both extensive human labor and many complicated types of machinery, but more importantly, it requires miners to apply them at particular locations (gold mines). Thus, gold not only requires many complications for its production process, but it also limits the

ability of people to produce it to specific locations. The production of Bitcoin, on the other hand, allows anyone, anywhere in the world[16], where there is an untapped energy source, to use it to produce Bitcoin. This unique production process of Bitcoin has three main advantages we shall discuss here.

First, it makes the competition for money production more fair and open than ever, removing many spatial constraints and allowing for a truly efficient process of market competition. Second, by making the process of production so simple and straightforward, Bitcoin reduces the hidden costs and externalities involved in the process of money production. This reduction of externalities makes the system much more robust overall and allows us to understand its consequences better. Third, the production of Bitcoin, by removing spatial limitations, allows the utilization of energy sources which were previously unusable due to such spatial considerations. The ruthless competition in Bitcoin production forces its producers (often called miners), to minimize their costs as to be more efficient than their competitors. This competition requires them to constantly seek for the most efficient energy production process, which will minimize their successive production cost, and it appears, both theoretically and in practice, that this most efficient source is to be found in renewables. The energy naturally available from these sources, such as sunlight, water, wind, and many others, is much cheaper than traditional sources as it is both so plentiful and mostly unused. While transportation costs of such energy limit its viability for many daily purposes, the production of Bitcoin has no such spatial limitations. Thus, the production of Bitcoin promotes the profitable funding and development of renewable energy and incentivizes progress in the field of energy production.[17] It is thus no surprise to find out that most of the energy used for Bitcoin production likely comes from renewable energy sources[18], making Bitcoin production probably one of the cleanest sectors of the economy.

We may summarize here that, as for the reasons discussed above, the production of Bitcoin seems to be the most desirable process for money production we may have. The fact that it is hard money, combined with its simple and transparent production process, open and direct competition, and seemingly positive externalities makes it largely superior to any of its predecessors. The second important consideration, which is typically linked to the production process of money, is the issue of its supply and is our next point of discussion.

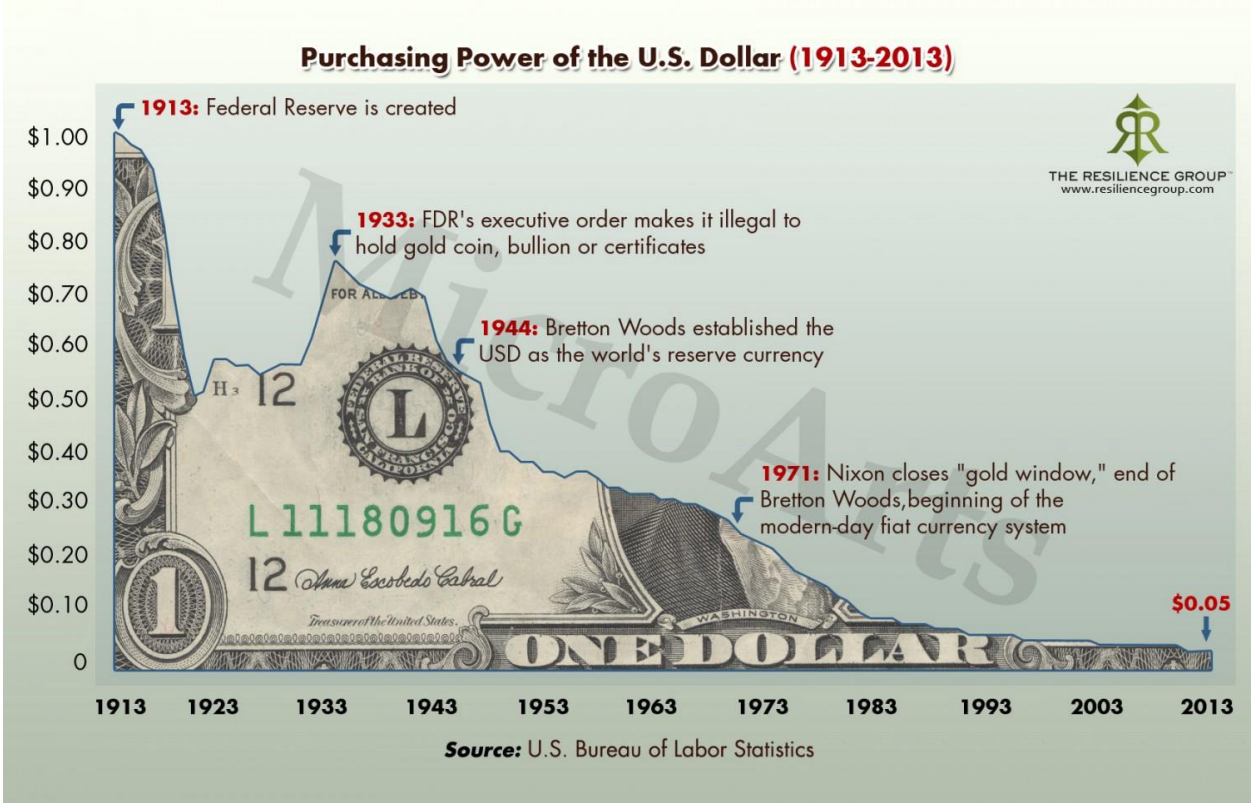
The Supply of Bitcoin

The nature of Bitcoin as a software-based asset means that its supply, unlike previous natural monies[19], is under the ultimate control of its users. It is, in fact, a critical part of its consensus rules, and is capped at roughly 21 million Bitcoin units. This is usually termed as the “monetary policy” of Bitcoin and is enforced

by the economic activity of each participant of the Bitcoin network. The decentralized nature of Bitcoin as a peer to peer network means there is no central entity authorized to dictate the monetary policy of Bitcoin. So while it is theoretically possible to change this policy, such a change in practice does not seem to be likely or even possible, thus it is not considered within this article.

This policy of Bitcoin is in sharp contrast with the prevailing policies enacted by the central banks of today. These institutions, from their very inception, have been pursuing policies of constant expansion of the money supply. These expansionary policies tend to be justified as necessary for the "common good" as they supposedly allow the government, and its "highly qualified" economists, to promote economic growth, reduce unemployment, and combat the business cycle. A task at which they have failed quite miserably for the last hundred years, during which those problems seems to have only further aggravated.[20] Within the present discussions, the monetary policy of Bitcoin is usually deemed to be quite radical in the eyes of most. Many critics of Bitcoin have claimed that this lack of an "elastic" monetary policy, that is a policy which may be modified according to the alleged needs of arising circumstances, prevent Bitcoin from ever seeing any meaningful adoption.

However, the notion of a need or even a necessity of an elastic policy has started to gain notable support only around the last hundred years. It is, therefore, a relatively new one compared to the thousands, or arguably tens of thousands, of years where money existed.[21] Furthermore, when inspected more closely, the modern experiment with an elastic monetary policy, enacted and managed by central banks, have failed to achieve any objectives it has set to itself.[22] The list of those broken promises from our central bankers includes the inability to tame the business cycle, a failure to maintain consistently low unemployment rates, and a complete failure to preserve the value of the money and the general price level.[23]



Purchasing Power of the U.S. Dollar (1913–2013). During this period, the USD lost at least 95% of its purchasing power.

The case for an elastic monetary policy, which many take for granted today as a necessity of money, is quite unconvincing in view of its actual merits and results. This goes without even mentioning its utterly indisputable failures before this modern attempt.[24] Moreover, this claim gets even weaker when we take into account the more than 50 economic collapses caused by hyperinflation just in the last century, which could not occur if not to the presence of elastic monetary policy.[25] [26]

A full critique of the ills of modern central banking, and the errors on which their theories lie upon is out of scope for this article. The interested reader can find references to such works in the footnotes.[27] For our present purposes, we shall focus on the most notable arguments for why an elastic monetary policy is undesirable, and why Bitcoin's limited supply serves for its advantage over its predecessors. Let us start by first exploring the idea of a "need" for an elastic monetary policy. As mentioned above, in light of its empirical failures, and when considering the impressive success of the gold standard which prevailed during La Belle Époque, and ended around the time of the establishment of the Federal Reserve System, there seem to be no empirical grounds for an actual "necessity" of elastic monetary policy. However, despite the lack of evidence for such necessity, one may still argue that such a policy would

generally be desirable. Thus, we shall now turn to investigate this question further.

With our prior discussion of easy money, which in principle is money with such elastic monetary policy, we have already articulated some of its ills. Those include severe moral hazard and the potential risk of abuse and ruin of the system. We shall now skip these stated issues and focus on an additional, more general argument against this policy type, which deals with the epistemic errors of such central planning of the supply of money and credit.[28]

Let us suppose that those in charge of the monetary policy have managed to resist all temptations for abusing it and are doing their best to help the economy. They may have at their disposal insurmountable amounts of data and information of supposedly relevant metrics. Their task is then to use all this knowledge and insights to adjust prices as to induce people to make economic decisions according to what they (the central planners) believe will have the most positive effect on the economy. In other words, they use their influence over the supply of money and credit in the economy to regulate such behaviors as prices and unemployment rates. The task of these central planners is then to predict the influence possible monetary policies might have on the parameters they wish to adjust (CPI, unemployment, etc.), and pursue the most "optimal" option of them.

However, this means they need not just predict the consequences of their actions, but also any reactions to these, and therefore any further reactions to those consequences as well. All attempts at predicting and modeling the most optimal monetary policy, even under the assumption that there exists such an optimal one, will fail from the very nature of the economy, which is a complex of individuals acting, and most importantly *reacting*, at an attempt to provide for themselves. The actions and reactions of humans are by themselves mostly unpredictable, but attempting to predict the repercussions of such reactions to changes, and the consequent reactions to the changes caused by those prior reactions must be considered ludicrous.[29]

The inability of central bankers to make predictions of the economy is even more visible when we consider the limitations of the data which they can possess. Within the realm of social phenomena in general, and economic phenomena in particular, the outcome is dependent to a large extent on all human actions involved in forming them. While we know how to measure certain parameters with high precision, we have no ability to measure many other facts relevant to the economic actions of individuals. Hayek explained this limitation of knowledge with the example of prices and wages, saying: "Into the determination of these prices and wages there will enter the effects of particular information possessed by every one of the participants in the market process — a sum of facts which in their totality cannot be known to the scientific observer, or to any other single brain."[30] This lack of access to such

many important facts caused most economists to completely ignore their significance, in Hayek's words again: "they [economists] thereupon happily proceed on the fiction that the factors which they can measure are the only ones that are relevant."[31] Central bankers, as we see, necessarily start their task with a highly incomplete picture of the past and present. Thus, their efforts to predict economic results are doomed to fail from the beginning, as even if they had proper methods to derive predictions from data, it is impossible for them to account for all data influencing human actions, and as we saw, every single action may potentially have a disruptive effect on the entire process.

The only prediction I can confidently make is that central bankers, as they continue to meddle with the supply of money and credit, will continue to produce unexpected behaviors, and as a result will miserably fool themselves with their efforts to predict — Bitcoin is a financial bet on this exact prediction. As long as the monetary policy is elastic, we are guaranteed to suffer from such epistemic errors and prediction failures, and economic crises will inevitably ensue. The economy is an interdependent system, and any artificial intervention will cause unexpected byproduct results, whose influence will get further aggravated with further interventions. For more than a hundred years, economists have tried to plan the supply of money, and with every intervention, another crisis ensued. It might then be the most appropriate time to face this failure, admit that the economy is too complicated for a central planner to predict, and let individuals make their own decisions as to form the complete picture from their actions.[32]

We have by now cleared the concerns regarding the inelastic monetary policy of Bitcoin, and proved it to be superior to an elastic policy. However, one could argue that a static inflation schedule, for example of 2% per year, could still be a viable option instead of a capped limit.[33] While it is probably true that Bitcoin could still work well even without a strictly limited supply, such inflation seems to be undesirable and even harmful. Monetary inflation, while not necessarily harmful per se, has highly non-linear and complex effects, with influence that which, as we saw, we cannot fully predict. The urge of some to tinker with such a complex system which they do not understand, or worse, believe themselves to understand, is at most not harmful, but may easily become destructive. Furthermore, if we investigate deeper, there seems to be no justification for expansionary policy in the first place.

When we understand the nature of money, and its emergence on the market, such inflation seems to be very undesirable. Money emerges based on its ability to reduce the costs of exchange, and an important factor for that is its ability to maintain its value over time. It is well known that an increase in the supply of money dilutes the value of each unit, its purchasing power, and thus imposes higher costs for using it in delayed transactions. An inflationary policy could thus hamper the adoption of Bitcoin, by making it less useful for

transacting, and would not give us any benefit.[34] To the contrary, an inflationary policy could reduce the accuracy of economic calculations, and would also reduce cash savings and encourage spending, which in a previous article, we already proved undesirable.

Throughout this part, we looked at the basics of the production process of Bitcoin and into its monetary policy. We discussed the idea of money production and its externalities, and how Bitcoin as hard money has the preferable production process out of all. We explored the trap of easy money, and more specifically, that of having an elastic monetary policy, and showed how Bitcoin managed to avoid getting into such issues. Finally, we have also seen how the actual hard policy taken as the rule of Bitcoin, a finite, limited supply, serves to its advantage and promotes proper economic incentives for savings and capital accumulation, while also serving as a reliable measurement for economic calculations.

Up to now, we have explored the "inherent" characteristics of Bitcoin, and as we have so far reached very positive conclusions. We shall continue going deeper into the monetary case for Bitcoin by moving to explore the external factors influencing the substance of money, and how Bitcoin deals with them.

Legislating Bitcoin

In a previous article, we have singled out three prominent external factors affecting the adoption of a monetary substance: legislation, societal structure, and epistemic considerations. We will now turn to inspect each of those factors and attempt to understand how they affect Bitcoin as money, starting here from the legislative aspect.

Even a shallow inquiry into the demise of the use of precious metals as the common monetary substance will reveal to us that it was the influence of legislative authorities which brought upon this demise. With the initial monopoly status granted to gold over other precious metals in most countries, and its further centralization under the control of central banks, the legislative authorities have influenced the specific choice of metallic money. With this centralization of power, they were later able to effectively confiscate gold holdings (Executive Order 6102)[35], preventing any everyday use of them. The last link of our money to gold was then finally broken with Executive Order 11615, issued by President Nixon in 1971.[36] This order ended the long transition process from metallic money into an irredeemable paper standard. This most recent example exposes us just how strong can the influence of the legal authorities be over our choice of money, and with the contemporary system of sovereign currencies, those authorities do not seem to like the idea of being challenged by Bitcoin.

Though the legal challenges Bitcoin is up to seem incredibly hard indeed, this is precisely what it was designed for. Bitcoin, from its very beginning, was created with the Cypherpunk ethos of liberty and freedom, and the use of cryptography in achieving liberation from oppression. Those challenges for Bitcoin are precisely the reason for its creation in the first place. For more than half a century we have been living under an oppressive fiat paper monetary system, and any attempt to implement a competing system was shut down.[37] In contrast, Bitcoin was built with all those past failures in mind and was designed to survive such threats. As its creator explained:

"A lot of people automatically dismiss e-currency as a lost cause because of all the companies that failed since the 1990's. I hope it's obvious it was only the centrally controlled nature of those systems that doomed them. I think this is the first time we're trying a decentralized, non-trust-based system."[38]

The production and maintenance process of Bitcoin is highly open and provides financial incentives for participants matching the actual demand for using Bitcoin, through the payment of transaction fees.[39] The mechanism of storing Bitcoin with private key cryptography makes it resilient to confiscation attempts. Along with the insistence on keeping verification costs extremely low, we can see how these are all design choices aimed at making Bitcoin survive, and even thrive, wherever economic and financial oppression is present.

This "legislation-resilient" nature of Bitcoin is so strong and robust that one US Congressman, Patrick McHenry, even went as far as to call Bitcoin an 'Unstoppable Force.' Continuing that "We [the government] should not attempt to deter this innovation; governments cannot stop this innovation, and those that have tried have already failed."[40] While there are many other legislators, who do not share this view, this bold statement emphasizes the idea of Bitcoin, and the mission of those it gathered behind it. We may not know yet whether Bitcoin will truly be capable of standing up to the legal challenges and governmental pressures it is likely to face, but if one thing is clear, it is that Bitcoin is our best shot at it. This legal resistance of Bitcoin is probably its most significant improvement over previous sound monies and is where its real advantage lies.[41]

Now assuming that governments understand the difficulty in stopping Bitcoin, there is the possibility of them choosing to use it, because of the financial incentives it provides them. Even though they removed the use of gold as money from our daily lives, governments, mainly through their central banks, are still massively accumulating it in increasing quantities, with roughly 17% of the total above-ground gold stocks under their possession.[42] When Bitcoin becomes significant enough, there is a chance that governments will purchase it as a gold alternative, monetizing it for their international monetary affairs, or as a hedging tool to "store value".[43] Another option for governments to

monetize the success of Bitcoin is through participation, whether direct or indirect, in its mining operations, as they control many of the most plentiful sources for energy production. Such mining operations would benefit both the states as another source of income and also help Bitcoin, which utilizes the higher energy invested in its mining for securing its network. While such acts on behalf of governments do not seem likely in the short or medium terms, the option remains very plausible for the long run.

Social Globalization and Bitcoin

The second significant external factor we have identified is that of the prevailing social structure, with the contemporary one being a trend towards globalization and international cooperation. Understanding the needs such transition of society brings with it is highly important to understand what is the proper money to serve such a society. Society today is shifting into urbanization at a high pace, with most of the world's population living in urban cities.[44] The role that the Internet plays in our daily lives becomes increasingly more significant as well. With more than 4 billion Internet users[45], the effect that this technology has on society seems to surpass most previous inventions in the extent of its reach and impact.

Though society is more connected than ever, the world is in a severe state of monetary disintegration on a level unseen in hundreds of years. While in the past most currencies were simply different weights of precious metals, thus accepted almost universally in commerce, today we have hundreds of incompatible paper currencies, disintegrating the world's market and hurting the global division of labor. Any social cooperation over most state borders

now requires monetary exchange between multiple currencies. This imposes additional costs while complicating and distorting economic calculations, and requires trusting more financial institutions. To this issue, we may add the problem of transactions settlements. Due to the costs and regulations of moving currencies across national borders, such settlement is highly expensive and requires the centralized process of going through multiple intermediaries.

With the shift of society into a globally interconnected one, and with ever-increasing amounts of electronic transactions done worldwide, the need for money native to the digital environment grows ever stronger and larger. Settling payments with strangers, without trusting financial intermediaries or the central banks which issue the currencies, is currently an impractical process. Furthermore, such a process simply cannot be implemented with any monetary system we have ever had, up to Bitcoin. As a completely electronic commodity, Bitcoin allows for settlements anywhere in the world, without the need for trusted clearance of payments. It does not require expensive international physical shipments and is easy to store and use from anywhere with minimal costs. Looking at the modern structure of society, there seems to be a genuine need for trustless, natively digital money, and this is likely to promote Bitcoin's adoption as "the decentralized alternative to central banking".[46]

Understanding Bitcoin — The Epistemic Barrier to Bitcoin Adoption

Our final consideration to discuss before we can conclude our investigation is of the third notable external factor influencing the substance of money, the epistemic one. Unlike previous monies, like gold, furs or cattle, Bitcoin has no "practical" use beyond its monetary use. In this regard, it is similar to collectible monies, such as wampums and various seashells, and in this specific regard also to the present fiat paper money. In a more conventional, though not economically accurate term, it has no "intrinsic value." Debating whether such intrinsic value is necessary, or more accurately if it exists at all, is out of scope and irrelevant here.[47]

What is essential for us, for understanding the epistemic barriers for Bitcoin, is that because of the lack of such widespread practical use, and unlike the (arguably) natural beauty of seashells[48], or the legislative promotion of paper fiat money, there is nothing which promotes the use of Bitcoin, thus its initial accumulation, beyond its monetary use. Thus, we may say that there are only two forces promoting the adoption of Bitcoin, the "economic" and the "epistemic", without any "indirect utility" playing a role. What I call here the economic force of Bitcoin is what we have discussed thus far, and is concerned with the economic incentives for using Bitcoin, and the benefits which it provides over legacy systems.

The second, "epistemic" force, deals with our understanding of money in general, and Bitcoin in particular, and with the use of our knowledge in guiding our economic decisions. That is, the more we understand money, its origins, and nature, the better our decisions will be in this regard. The epistemic force I discuss here is thus the motivation of using Bitcoin which does not come from a direct and immediate (or expected to be immediately available) benefit of Bitcoin, but from that which is expected to eventually come from understanding Bitcoin and its advantages. While in the very beginning of Bitcoin I believe most of its holders have participated purely due to the epistemic motive, I think that, as for today, the economic force is what tempts most people to come, but the epistemic is what motivates them to stay. This process is mostly evident during the "supply shocks" (halvings) of Bitcoin, after which we have so far witnessed Bitcoin's price drastically increasing. This increase in price (economic force) draws masive attention towards Bitcoin, but after the hype fades away, what keeps many still interested is the understanding of Bitcoin and its vision (epistemic force). However, a true adoption of Bitcoin is likely to happen only when the economic force of Bitcoin is so strong as to make the epistemic one (of understanding Bitcoin) unnecessary for making people use it as part of their daily lives.

This last subject I find the most important in the article, as unlike the others, this is the only one where I see Bitcoin at a significant disadvantage. While for gold, its established history of thousands of years of monetary use tends to be a sufficient substitute for understanding why it works so well, Bitcoin enjoys no such luxury. On the other hand, fiat paper money, whose "established history" is flooded with failures and economic collapses manage to pass this epistemic issue by providing direct funding for the academic economics department and also serving as their most significant employment option. Fiat money then provided such academics with highly respected, influential, and well-paying jobs, and they, in turn, produced the epistemic base for such a monetary system and certify it with their "credentials." In contrast, Bitcoin, being hard money, has no budget for producing such "scientific base" for itself, and does not provide economists with such influential jobs, but mostly replace their current workings. It is no surprise, therefore, to find out that very little has been written in favor of Bitcoin, especially in academic circles, as mentioned in the opening here.

Without sufficient resources for understanding money and Bitcoin, the only force promoting its adoption would be the economic one. Even if it could be sufficient alone, it will certainly not work well enough, and a transition into Bitcoin would seem unlikely before the contemporary system collapses upon itself, making a transition highly unpleasant, and unnecessarily so. However, the more resources for understanding Bitcoin that exist, and the better people

understand the reasons for Bitcoin, the faster they will act to adopt it, and thus the sooner and smoother the transition into using it may be.

Today, with more than a century of central banking, the general understanding of money is entirely flawed, and even more so in most academic discussions, where they still believe they can "fine-tune" the economy with their complex mathematical models and inflation targets. The last crisis of 2008 has shaken the trust in the current system, and rightly so, but most alternatives offered to the public for understanding money have only aggravated the errors of the contemporary system. Statements like "money is whatever the state decrees as such," or "money is just a shared illusion" are now very common, even among many Bitcoin supporters, and this only shows how extensive the work of explaining Bitcoin and money is. The point here and the purpose of this article is to show just how important it is to explain money in general, and Bitcoin in particular, to others in order to make it succeed as a truly peaceful revolution.[49]

Conclusions — The Emergence of Bitcoin

The last ten years have been some of the most interesting to observe from the perspective of monetary economics. During this period, we got to witness the first monetary good which was invented, rather than discovered, by the free market, and the astonishingly fast process of its monetization. What started as seemingly just another ill-fated proposal on the Cypherpunks' mailing list[50] has grown into a fully functioning monetary system actively serving millions of people worldwide. Throughout this article, we went through the common factors which influence the saleability of money, therefore its adoption on the market, and examined how Bitcoin fares compared to its predecessors. Now, to come full circle with our analysis of Bitcoin, we shall briefly take an overall look at Bitcoin's process of emergence, from its early beginning to how it how it may proceed in the future.

When Bitcoin just launched, and for the first few months of its existence, it had no price, and was transacted mostly for testing the software. The "zero to one" moment of Bitcoin was when in October 2009, its first exchange rate was published and it first became valuable in exchange. Soon after, its few early adopters started exchanging it, breathing life into the system by giving Bitcoin its initial price. As they were willing to spend money to bring Bitcoin to life, while almost no one knew what Bitcoin was going to become, they must have been motivated enough just from the vision of Bitcoin's potential. Thus Bitcoin started circulating not from another "useful" utility, nor by authoritative decree, but from the voluntary actions of its early adopters which valued the opportunity of creating a new monetary system — more than the money they had to spend to facilitate a reality of Bitcoin's visionary potential.[51]

Going a bit forward, while Bitcoin had some exchange value, the number of exchange opportunities which were available for it was quite small, as the

demand for it as a medium of exchange had only just began to coalesce. This means that people initially had to wait a substantial amount of time, compared to the established paper money, to exchange it. That is, they had to hold it to adopt it. Here lies the main reason why the hardness of Bitcoin and its limited supply was, and still is, crucial for its success. Without a hard inelastic policy, the uncertainty which would accompany holding Bitcoin, due to the risk of monetary inflation and consequent depreciation, would be too high and would prevent it from seeing any meaningful adoption.

The monetary hardness of Bitcoin is what allows people to confidently hold it, knowing their wealth will not be diluted. In addition, its limited supply means that as its adoption grows, Bitcoin will necessarily become more valuable, without suffering the negative effect of inflation which would reduce its value. Therefore, the limited supply of Bitcoin, by itself, provides a strong economic incentive to adopt and hold it for those who understand its superiority as a monetary asset, and thus expect the demand for it to increase with time. Satoshi himself understood this very well, writing:

“Instead of the supply changing to keep the value the same, the supply is predetermined and the value changes. As the number of users grows, the value per coin increases. It has the potential for a positive feedback loop; as users increase, the value goes up.”[52]

As for today, Bitcoin is circulating at a much higher velocity than in the past, with many more exchange opportunities for it. However, there is still a very long way for Bitcoin if it is to become a widely used monetary system. The process of monetization, like all other phenomena of social cooperation, is a non-linear process accelerating and benefiting from each additional use. Thus, the velocity of Bitcoin and its use in day to day manner shall not be expected to become substantial in the very near future but should accelerate when inspected in the long term. Looking at the progress it made so far, there seems to be a good reason to believe Bitcoin will succeed to achieve such “critical mass” needed for reaching sufficient acceleration of growth and becoming common money throughout the world.

Currently, the two domains where Bitcoin grows most significantly are within the realm of the Internet, where it has “home advantage,” and in countries that lack minimal economic freedom. In the latter domain, within countries such as Turkey, Iran, and Argentina, we can see how Bitcoin provides some degree of immediate relief from the economic oppression imposed on those who live there. The tighter capital controls get, and the higher the inflation rate goes, the more significant becomes the benefit of using Bitcoin as a government-resistant alternative. Therefore, while we cannot know with certainty how Bitcoin will grow, it seems likely that the emergence of Bitcoin as money will continue largely within economically oppressed countries, whose citizens need Bitcoin to protect their wealth the most, and will continue to increase most

substantially where economic crises arise. It appears that, at this stage, Bitcoin is a free market good, which demonstrates its value proposition most effectively in the absence of free markets. Authoritarian attempts to restrict it only promote its use, and thus it seems that Bitcoin truly deserves to be called an antifragile money.

---

[1]: The crises of the 1980s and 2008 are notable examples of such collapses which seem like they could easily turn catastrophic to the system. [2]: Friedrich A. Hayek: “By Monetary Nationalism I mean the doctrine that a country’s share in the world’s supply of money should not be left to be determined by the same principles and the same mechanism as those which determine the relative amounts of money in its different regions or localities.” — “Monetary Nationalism and International Stability” (1937), page 4. [3]: See both the chart below and further relevant metrics produced by Crypto-Voices here. [4]: The Nature of Money and The Substance of Money. [5]: The principles for our analysis of money here are rooted in the works of Carl Menger. Most notably, his “Principles of Economics” (1871), chapter VIII, and “On the Origins of Money” (1892). [6]: Such changes, though hard to coordinate and perform, have been previously made to the Bitcoin protocol after sufficient consensus was reached. See BIP16 (P2SH) and BIP141 (Segregated Witness) as prominent examples of such changes, which improved the monetary properties of Bitcoin by adding consensus rules to the protocol, a method known as “soft-fork”. [7]: See the following website for an extensive list of resources for learning more about the Lightning Network: https://www.lopp.net/lightning-information.html [8]: Jörg Guido Hülsmann, “The Ethics of Money Production” (2008). [9]: For a more thorough definition of the problem and the solution, the Nakamoto Consensus, see the Bitcoin whitepaper. [10]: See the following article, by Bezant Denier, for a historical examination of these externalities: https://www.bdratings.org/l/war-externalities-of-livestock-money/ [11]: Thomas Wright, “The Travels of Marco Polo, the Venetian” (1854), especially page 168. See also this short thread for a brief lookout over Polo’s recordings of paper money, and this blog post for a more elaborate treatment. [12]: For some historical record on the thought of paper by from those writers see Jörg Guido Hülsmann, “The Ethics of Money Production” (2008), pages 79–81, Robert Minton, “John Law: The Father of Paper Money” (1975). [13]: David Ricardo, “The High Price of Bullion, a Proof of the Depreciation of Bank Notes” (1810) [14]: For an economic view on moral hazard see Jörg Guido Hülsmann, “The Political Economy of Moral Hazard” (2006). [15]: See Milton Friedman, “The Resource Cost of Irredeemable Paper Money” (1986). [16]: With the existence of various data transmission mechanisms, with a notable example being the Bitcoin satellite launched by Blockstream, there is a virtually no barrier for participating in the Bitcoin mining process from anywhere in the world. [17]: See this article by Daniel Wingen on the production process of Bitcoin and how it may positively affect the environment

and sustainable energy production. [18]: See CoinShares mining analysis for more information: https://coinshares.co.uk/bitcoin-mining-cost/ See also this 2 part series of posts on their blog: https://medium.com/coinshares/an-honest-explanation-of-price-hashrate-bitcoin-mining-network-dynamics-f820d6218bdf https://medium.com/coinshares/beware-of-lazy-research-c828c900b7d5 [19]: Jörg Guido Hülsmann: "We may call any kind of money that comes into use by the voluntary cooperation of acting persons 'natural money.'" — "The Ethics of Money Production" (2008), page 24. [20]: A good example for this miserable incompetence can be seen with these two quotes from former U.S. Federal Reserve Chair Janet Yellen, which in 2017 stated that: "I hope that it [financial crisis] will not be in our lifetimes and I don't believe it will be," and less than a year later, she expressed quite a different sentiment, saying that: "I'm not sure we're working on those things in the way we should, and then there remain holes, and then there's regulatory pushback. So I do worry that we could have another financial crisis." [21]: On the history of money see Nick Szabo, "Shelling Out" (2002) [22]: See this article by Mark Hendrickson on the 100 years long failure of the Federal Reserve at achieving any of its goals. [23]: During the time of existence of the Federal Reserve, the USD has lost at least 95% percent of its purchasing power. [24]: See for example the Yuan of 13th century China, the Assignat in France, and the Continental currency in America. [25]: Here you can find a list of 58 hyperinflation collapses of the last century. [26]: Though there was a recorded case of hyperinflation during the Roman empire, which used metallic money, this is still compatible with what is said here as the fault in such cases is still attributed to the severe debasement of the money by governments of that time, an action which equates to their "monetary policy" in present terms. [27]: For such criticism see: Jesús Huerta de Soto — "Money, Bank Credit, and Economic Cycles" (2006), Jörg Guido Hülsmann — "The Ethics of Money Production" (2008), Friedrich A. Hayek — "Denationalisation of Money: The Argument Refined" (1990), Murray N. Rothbard — "What Has Government Done to Our Money?" (1963). [28]: For a brilliant critique on this grounds see Friedrich A. Hayek, "The Pretence of Knowledge" (1974). [29]: An appropriate treatment of the errors of the use of predictions and models in complex domains in general and in economics in particular can be found in the works of Nassim N. Taleb. [30]: Friedrich A. Hayek, "The Pretence of Knowledge" (1974). [31]: Friedrich A. Hayek, "The Pretence of Knowledge" (1974). [32]: In relation, see Friedrich A. Hayek, "The Use of Knowledge in Society" (1945). [33]: Though as for today, Bitcoin do have monetary inflation, this is merely a temporary phase which distributes the initial ownership over bitcoins, and as we saw, is done in accordance to a strictly defined schedule. We may therefore ignore this initial inflation and discuss the long term, permanent policy of Bitcoin, which is a constant supply. [34]: For a full critique on inflationary monetary policy see Ludwig von Mises, "The Theory of Money and Credit" (1912), chapter VII part 3 — Inflationism. [35]: Executive Order 6102 issued by President Franklin D. Roosevelt on April 5, 1933,

prohibited the "hoarding" of gold, and effectively ordered the confiscation of most private gold reserves. [36]: Executive Order 11615 issued by President Richard Nixon on August 15, 1971, as part of what is called the "Nixon shock", cancelled the convertibility of the USD to gold. [37]: Notable examples are e-gold, shut down in 2008, and Liberty Reserve shut down in 2013. [38]: Satoshi Nakamoto in response to a comment on the P2P Foundation Forum. [39]: On how transaction fees help Bitcoin defend itself against the state, see this post by Eric Voskuil. [40]: https://cointelegraph.com/news/bitcoin-an-unstoppable-force-us-congressman-tells-crypto-hearing [41]: This legal resistance also had to be accompanied with a sufficient improvement in the monetary properties in order to be effective, as to prevent centralization risks of holding it. See the following article by The Bitcoin Observer for further explanation on that. [42]: https://www.gold.org/about-gold/gold-supply/gold-mining/how-much-gold [43]: The following article, "The Bullish Case for Bitcoin" by Vijay Boyapati, articulates the possibility of such scenario in more details. [44]: https://ourworldindata.org/how-urban-is-the-world [45]: https://wearesocial.com/blog/2019/01/digital-2019-global-internet-use-accelerates [46]: Saifedean Ammous, "The Bitcoin Standard: The Decentralized Alternative to Central Banking" (2018) [47]: On that subject in relation to Bitcoin, see Conner Brown, "Bitcoin Has No Intrinsic Value — and That's Great." [48]: In his article "Shelling Out: The Origins of Money", Nick Szabo propose the possibility that our natural attraction to such collectibles, which we attribute to their "beauty", is not merely "accidental", but is an instinct developed from their usefulness as primitive money. [49]: See Nic Carter, "A Most Peaceful Revolution". [50]: Besides Hal Finney, most reactions Satoshi initially received were very skeptical, see the original discussion on The Cryptography Mailing List. [51]: See this beautiful short piece by Ross Ulbricht called "Bitcoin Equals Freedom". [52]: Satoshi Nakamoto in response to a comment on the P2P Foundation Forum.

Special thanks to Ben Prentice (mrcoolbp), The Bitcoin Observer (festina_lente_2), Bezant Denier (bezantdenier), Thib (thibm_) and Daniel Wingen (danielwingen) for all the feedback I received from their reviews, comments, and suggestions which helped me shape this article.

Crypto without Criticisms

How Anarchism Without Adjectives Can Point Towards a Method of Unifying Crypto

By Erik Cason

Posted October 7, 2019

Anarchism without adjectives was a form of anarchism developed in the late 19th century a few decades after anarchism split with communism in 1872 over authoritarianism and the use of the state in creating a stateless society. While anarchist were unified in their idea of a stateless society and the need to create it without the state, there was no consensus on how this was to be done, so a number schisms developed within anarchist movement itself. From individualist anarchist, to anarcho-syndicalist and anarcho-communist, there were many different flavors of what a stateless society could look like under the banners of anarchism. In response to the petty narcissism of small differences between various anarchists, anarchism without adjectives rejected specific forms of anarchism for a synthesis of operable praxis. It wanted to focus on what worked, rather than the ideology of what they thought would work.

The great advantage of this strategy is it creates a revolutionary front through the praxis of revolutionism first. It synthesizes all revolutionary tendencies, solidifying them into a primacy of solidarity around the organization of the revolutionary struggle itself. This is how the I.W.W. one of the largest and most revolutionary unions to ever be created functioned was through a synthesis of many revolutionary traditions under the umbrella of 'one big union.'

Drawing from the history that allowed for anarchist to create such a revolutionary movement that was able to threaten the very foundation of the state, we can again create such an organization through unify crypto under a similar banner. Through the creation of one big union people realized that rights were not something that were meant to be protected by the state, but were something that people must defend for themselves together. Through the tradition of 'An injury to one is a concern of all,' crypto renews this same revolutionary struggle into the digital age, with concern to the digital rights of all.

Satoshi Nakamoto gave us a form of money that the state can never control. We need to take this seriously if we are to use this form of money, and everything that has come after it as part of our arsenal in the secret war that is taking place to free humanity from the shackles of fiat money and the state's

totalitarian economic control. We need allies if we are going to win in our various struggles against whatever masters may have claimed us for themselves. Through taking this idea of anarchism without adjectives and applying it to crypto, we can find a new form of synthesis; or syndicalism, that can help weave our revolutionary movement together.

Crypto without Criticism, but Critiques

Now I want to be clear, crypto without criticism **should not mean crypto without critiques**, nor should it mean that we accept fungable tokens, stablecoins, or other shitcoins that are really panoptic statist ledgers, and not crypto at all. What this strategy acknowledges is that bitcoin, while being revolutionary in its own right, and containing the messianic potential to end law and destroy the Westphalian state as we know it; there is still a great possibility that it could fail, or even worse, be seditiously compromised. Every one of us must be vigilant, thoughtful, and apply adversarial thinking to each step of our process in order to ensure that the revolutionary nature at the center of what is being done is never compromised. By very nature of what crypto is, we cannot have any single point of failure, which is why we must be open to other projects and the potential merits (or failings) they may offer.

Bitcoin unequivocally is one of the greatest invention of humanity. There is no question that what Satoshi Nakamoto created has radically changing the world, and has opened a new horizon for human freedom and action. It is even quite possible that bitcoin is messianic, and that Satoshi is the prophet of a novus ordo seclorum that will liberate us from the old law, and allow for us to enable something totally new in its place–but only time will tell. While I zealously have given myself to the cause, and believe Bitcoin to be the most revolutionary vehicle that we have, I still cannot call myself a maximalist (majoritist maybe).

We must be open to the possible that Satoshi is a statist, that a deep reorg 51% attack will happen, the core devs are all somehow compromised, or there is something fundamentally broken in the bitcoin code. We must be open to the worst possibilities in order to create redundancy, to build our ranks, and educate people about the possibility of freedom from fiat, however that may come. Only through creating a robust collective movement that is focused on building and using the revolutionary technology of crypto without anyone's permission for whatever purpose it may be, will be able to create the revolutionary movement that can finally win the freedom and liberty to which we are entitled.

The political objective of what crypto is, how it functions, and why it creates power is of the utmost importance and we must ensure that the technologies of the future really are 'crypto' and not something else. As I warned in the poverty of tokens, there is a real risk of creation a panoptic nightmare of

unparalleled proportions if we run the risk of deploying broken ‘crypto’ that isn’t crypto at all.

Through the tradition of anarchism without adjectives, we can create a movement for crypto without criticism. A movement which can be ideologically committed to the values that represent crypto, while also offering valid critiques of each crypto projects and their weaknesses. It is only though such intellectual exchange, inquiry, and explanation will we be able to understand one another, and create a space in which we can work together.

The Startup Government

By Tim Draper

Posted October 10, 2019

Preface. Tribalism to globalism.

The Startup Religion. We have a particularly diverse student body at Draper University, and in the program, the students are asked to do challenging projects in teams. As a result, they build extraordinarily tight bonds with each other. Most of them overcome biases that they may have held before entering the school.

One particularly powerful and illustrative moment of this took place in the spring of 2019.

I was starting to give my 20th Draper University graduation speech, when I noticed that about 10 Arab students were missing. I asked where they were, and a fellow student said that they were out praying.

I said, “Go get them. We will all pray.” So, the praying Arab students were rounded up, and proceeded to lead the class of about 80 students in a Muslim prayer.

Then I asked, “Would anyone else like to lead a prayer,” and the magic began. Doron Segev, our one Israeli female student said, “I will lead a Jewish prayer.” We all followed along with her.

Then I said, “Anyone else?” And three Indians got up and led us in a Hindu prayer.

Finally, two Catholics led us in a Catholic prayer.

It was such a strong emotional event, I got chills. The spirits were loving this.

“Only at Draper University,” I claimed, but deep down, I hoped that this was the beginning of a series of magical moments that might open the hearts of the people of the world. If it could happen here, maybe it could start to spread. The various religions, the various people, and the various countries could find a spiritual love for each other, we might all start to understand each other better, and barriers, whether they be religious, geographic, or political, would start to fall.

The Startup Currency. In a seemingly unrelated event, about 10 years earlier, Bitcoin was created. Bitcoin is a currency that is global, open, transparent, and decentralized. With it, people everywhere can send money frictionlessly,

without the need to pay banks and credit card companies (2.5–4%), Western Union (8–16%), or central government authorities (whatever they take).

With Bitcoin, and the decentralization that comes with Bitcoin, geographic borders have become less relevant. No longer are we at the mercy of dictators and toll trolls to grow the world economy. Venezuelans, Nigerians, and Venezuelans now have a currency that can get them out of the clutches of failing government currencies. And while in the short-term we may have some governments with (control freak, fear spreading) leaders trying to turn this technology into their own power center, in the long-term I believe with regard to business and economics, we are, more than ever, one world.

The Startup Government. So now given this “one world”, what is a political leader to do?

Before we can answer that question, we need to think about what is the purpose of government.

Tribal to global

Thousands of years ago, people organized into tribes because they afforded security and protection. They wanted to feel secure that if they worked to create something (be it: food, clothing, shelter, or a business) they wouldn’t have to fight off others to keep it. That security afforded by tribes was primarily built around the defense of geographic territory. Each territory had its own set of rules that people needed to follow to be accepted into the tribe or else they would be banished as outlaws. This system worked well for the people of the world. People generally kept to their own tribe as long as everyone was fed, clothed and housed. When there were times of scarcity, however, there were cross-tribal battles for survival.

Over time, tribes found that they could trade goods and services in a way that benefited everyone. The goods, services and eventually the currencies that each tribe offered would often need translation so that the dealings would seem fair to both sides. Banks served to make the fair translations as a trusted third party.

Banking grew trade inside tribes and among tribes. As this web of trade grew and became more intertwined, the world began to open up and prosper in an unprecedented way. The world became much wealthier as the banks created more and more liquidity. People prospered.

Tribes with similar rules even started to band together (eg. The United States from 1776, the Chinese over the centuries, and the European Union more recently). These larger alliances between tribes thrived both economically and politically, and while there were still rivalries between allied tribes, they were

generally not violent and instead were more strategic. Scarcity became abundance, as people could trade across tribes and around the world.

People married across borders and across religions, and this blending brought with it bonds that made all people more worldly, more safe, more wealthy and more powerful. Soon people started to understand that their tribe was really no different from the tribe next door or the tribe around the world from them. In fact, they found that their tribalism was actually curtailing their success. Businesses and trade were limited when tribe governing bodies were building barriers to free trade in the form of customs, tariffs, and regulations. People realized that they are a part of a big world and more interconnected than their own (relic) tribalism allowed.

Today, people are discovering that they are all a part of something bigger than their tribes. People are discovering they are part of one big open world.

The change in thinking from tribal to global is exciting for some of us, but scary and difficult for many of those of us who cling to the security of our tribes and might have remnant xenophobia. To shield ourselves from the scary change, some of us are lashing out, trying to cling to the past tribal world. As a psychological defense mechanism, we deflect our discomfort and call others “racist” or “nationalist” or “anti-semetic” or “fascist” or whatever because we are dealing with these feelings inside ourselves as we struggle to leave our tribal world and enter this new global one.

But the change is happening.

In our impromptu prayer exercise at Draper University, my students discovered that their religions are not incompatible; instead, they are more sides of the same house, the same church.

Bitcoin made it clear to us all that we can all share in the same global economy with the same basic values using a unifying global currency. Those that resist this global currency cling to tribalism by saying things like, “I don’t understand bitcoin.” Or “Bitcoin was just a means to an end. The blockchain is the thing.” or “bitcoin is not money because it is not backed by any (tribe).”

But for many of us, Bitcoin was our bright light, our “a-ha!” moment, our spiritual awakening. Tribalism is dying. And like the dying roar of the king of the jungle, we are hearing political leaders beat their chests as they try to cling to the power they once wielded when the world was still only tribal.

It is ironic when governments try to distinguish themselves from one another. All the tribes look remarkably similar now. The rules are pretty close to the same wherever you go with subtle differences created by governments with more or less desire for control over their constituents.

There are Starbucks and McDonalds wherever you go. There are search engines and Uber drivers and AirBnBs in almost every tribe. You can communicate across any tribe with Skype and email and text. You can buy and sell products and services across tribal borders with relative ease.

It does seem that the dying lions are roaring to try to make this global opening more difficult with trade wars and walls, but I believe that those that encourage free trade will win out in the end.

So, going back to my original question, what is a government to do about our becoming “one world”?

I believe that governments, like any business that is challenged by a new environment, must adapt to the new marketplace. And this is the marketplace of accountable, transparent, and competitive governance. In addition to those services that a government provides that are local and tied to geographic territory (tribe), today’s government must determine what they can provide across border to the cloud (virtual) economy. So, what does a government sell that can be provided virtually?

I would argue that most of what a government sells is safety and security for their people. The virtual portion of security is insurance. Insurance is about to take a great leap forward as smart contracts and artificial intelligence are combined to create a completely transparent, fair and consistent insurance company. The virtual portion of security includes identity security, where individuals can distinguish each other with certainty. Identity is also about to take a great leap forward as data is established as a number of proof points. Those proof points are about who is asking, at what time, from what location, and are these consistent proof points. An identity system like this will build more probabilistic confidence in anyone’s unique identity as the data knowledge base compounds.

The Startup Government Pioneer.

In 2013, The Prime Minister of Estonia came to Draper University to speak. He explained his and his President’s vision of creating a virtual government. The Estonian e-Government is a breakthrough in tribal to global thinking. The idea of an e-Government is that governance, the services of government, can now be provided across geographic borders. Estonia’s e-governance doesn’t offer a lot yet, just the ability to easily do business in the EU through a virtual residency identity program, but down the road they promise a plethora of services. But the game is afoot. Malaysia has a virtual residency program now, and Kazakhstan is working on a virtual citizenship program. Governments are going to compete for us virtually.

What else could a government potentially provide? I have a few ideas.

How about a global health care insurance package that is more efficient and effective (and works globally) than Medicare where the premiums are in bitcoin and the claims are settled to the letter with smart contracts and monitored by artificial intelligence.

Or a comprehensive global camera security service that protects people from intrusion wherever they are. At Hero City, we had several computers stolen, and when we went to the police with a find my computer blinking in a specific house in San Mateo, the police were hamstrung and could not enter the house. So we just put up a network of cameras as a deterrent, and crime went to almost zero.

Or a pension that is not at the mercy of political forces like social security or public pensions, but one that is simply a form of fixed smart contract with the pensioner.

Today, governments, global governments that are willing to eschew tribal tendencies, can provide services across borders the way businesses always have, providing “choice” to global citizens. And we, citizens of the world can potentially pick and choose the services we want from each provider. We can potentially participate as customers in a governance marketplace. As citizens, we could potentially allocate our money to those governments that provide us the best services. In turn, the enlightened governments could be incentivized to more efficiently and effectively meet the needs of the various global citizens. These governments will begin to look at constituents as potential customers.

— -

Bitcoin brought with it a few fundamental technologies that can accelerate our transformation from a tribal planet to a global one. In this, my second book, I will explain why I think these technologies, when combined with artificial intelligence, will transform not only industries like banking, finance, health care, real estate and insurance, but also the biggest of them all: government.

I look forward to sending a few more chapters via Medium, and then publishing “The Startup Government,” my second book.

Best, Tim Draper

Bitcoin is for Stackers

By Elaine Ou

Posted October 17, 2019

There's a common myth that Bitcoin allows anyone to spend money anywhere. That's incorrect — Very few merchants accept bitcoin. Bitcoin is useful because anyone can receive money, anywhere.

As consumers, we don't often think about what it takes to receive payments from strangers on the internet. Wanna sell firearms, fireworks, pharmaceuticals, tobacco, vapes, or any other target of Operation Choke Point? Good luck finding a payment processor. That's where Bitcoin comes in.

The distinction between spenders and receivers may seem trivial, but it's literally how the protocol gets decided (see also: Economic Nodes). Bitcoin's value comes from those willing to offer things in exchange for bitcoin. That's true of any money: The US dollar is valuable because the government accepts it in exchange for a promise not to imprison you this fiscal year. Value comes from **acceptance for value**.

Americans sometimes have trouble with the idea of acceptance value. As the world's biggest consumers, we believe that others value whatever we have to spend.

Nope, it took a lot of work for the USD to become the world's reserve currency. After Bretton Woods, nobody wanted our unbacked dollars. With his brilliant negotiation skills, Henry Kissinger convinced Saudi Arabia to accept dollars for oil, and in return we would grant them billions worth of arms deals, our undying military support, and the souls of our children. Iraq tried to sell their oil for euros, but we set them straight with a good ol' fashioned dose of Freedom and Democracy. They're back to taking dollars only now.

Under ordinary circumstances, Gresham's Law dictates that bad money drives out good — spenders always dump their most worthless asset. Americans don't spend their bitcoins, or even their actual dollars. We pay for everything with credit, most often the credit card that gives us airline miles while sticking it to the merchant. Or maybe we spend that Starbucks gift card we got for filling out surveys on the internet. That's why spenders don't determine the value of money.

The lack of Bitcoin-Only services is perhaps the biggest obstacle to broader adoption. No one voluntarily spends bitcoin. As long as services still accept credit cards, bad money will always drive out good.

Money and time

By acrual

Posted October 17, 2019

Ever since I got the Bitcoin bug, I have been thinking about money like crazy, sometimes coming up with really stupid ideas, sometimes hopefully being more right than others, reading many of the Austrians, but always trying to figure out what is the theory that best could explain Bitcoin's existence. The stock2flow ratio always made a lot of sense to me, but I've always wondered why scarcity meant value in the first place and I think I have finally figured out why.

Everything has to do in one way or another with the most scarce resource we have: the time of a human life. I argue that all economic calculations are done taking into consideration the time needed to carry something out because time is present in every single good and every other resource present is also a function of time too.

Time is therefore the universal currency and everything can be obtained or manufactured with the sufficient amount of time. But time has a problem: you can't exchange it.

Throughout history we have needed a way to represent the time that both sides of a transaction could exchange and with which we can reach an agreement about the "time valuation" of a good. That's what I'm reaching the conclusion money is all about, i.e. time valuation, and it is more demanded the more scarce it is, as scarcity represents a longer time needed to obtain it. Scarcity is therefore a measurement of time, and time a measurement of value.

In fact, the article by Nick Szabo "A measure of sacrifice" rang a bell to me when I realized all the work people have been doing throughout centuries in order to coordinate and synchronize around time. Money is therefore, another way to coordinate around time and being able to exchange it.

Actually we look for a exchange in utility first. If for example I have my lamborghini but I am so thirsty that I am about to die, and someone is interested in my lambo and offers me either $1m or 1 litre bottle of fresh water, I'm very likely to choose the latter.

But if there is no coincidence of wants, we will look after a good that allows us to measure time.

In order to work properly as a measurement of time, a good has to be a **STANDARD** measurement of time. This means that it has to be universally

equally scarce for everyone. If someone can develop some understanding or knowledge that allows them to really manufacture or obtain more of that good in the same time, then it won't be as easily accepted as money. In other words, what technology is all about is time saving, and if more of a good can be obtained through technology, then it is not useful as money.

Let me explain in a very simple example how an exchange would take place according to this theory:

- Alice sells a couple of shoes to Bob that take her 2 months to manufacture because she has developed a special knowledge and skill about this process.
- Bob has no idea how to manufacture shoes and estimates it would take him beyond 10 months to get them done himself.
- A 1 gram piece of gold takes both Alice and Bob approximately 5 months to find. Both know the time it takes each other to find that 1 gram piece of gold, because they know that gold is equally scarce for everyone. Being standard, gold transmits information of the time needed to obtain it as a result. You could be lucky and find that piece of gold in 4 months instead, but as an estimation of the time needed to get it, gold transmits the information "that piece of gold represents a length of time longer than the time it took me to manufacture my shoes, it is a proof of more work than what my shoes are for me". Should he pay with any good other than gold, Alice would have no way to know how much work Bob put into obtaining it. It would be difficult to know if the exchange is therefore fair. With gold, she knows with a high degree of certainty. Error in the economic calculation is therefore minimized with a standard measurement of time.
- So Bob pays Alice 1 gram of gold, and he is happy because he obtains something that would take him more than 10 months to manufacture, paying in exchange something that would typically take him 5 months to find.
- And Alice gets 1 gram of gold worth 5 months of work, in exchange for two pair of shoes that would typically take her 2 months to manufacture. She is also happy as a result.

This is exchange, and it is beneficial for both sides despite not existing any coincidence of wants, as both sides "save time" compared to what they had before the exchange, and progress is created as a result. Both benefit from the difference in the knowledge and skills of each other. We end up being able to do more in a lifetime that we would otherwise, had we not had any money to exchange with, and therefore progress is actually about saving time. In other words, money allows us to benefit from the knowledge acquired by others.

Money allows us to transmit the benefits of knowledge and skill development so that the entire society can progress as a result.

If “The selfish gene” theory is right, we don’t look for utility in a transaction, but fairness, justice or rather reciprocity.

It’s almost like using a meter to measure the size of a good before exchanging it. Instead of a fixed length, it needs to have a standard universal scarcity everyone knows about. If it also has other properties that make exchange easier such as divisibility, transportability, etc… then it will be even more demanded as a result.

While with gold you could develop some particular knowledge about the location of pieces of gold and keep it in secret for a while, **Bitcoin is the only good that is universally scarce for everyone.**

Nobody can develop some special understanding about that could lead them to get more bitcoin units per unit of time. It is simply impossible for as long as the current algorithms keep working flawlessly. The only way is having saved time before (saved money) and investing huge amounts into mining facilities, or otherwise borrowing it at an interest rate (you could argue this interest rate is the cost of saving time).

This turns Bitcoin into the best standard and exchangeable measurement of time there is and as such, as the best form of money ever.

The driver of adoption is therefore according to this theory, not as much the fact it is scarce, but the fact it is universally scarce for everyone. That and the other properties we all know and love, are what is going to inevitably turn Bitcoin in to a moneyness black hole.

Bitcoin is Not a Pyramid Scheme

By Parker Lewis

Posted October 18, 2019

A few years ago, I received an email from a friend asking for my opinion about an investment opportunity that a mutual contact of ours was considering. After a quick search on the internet and after having watched a few videos, I explained that it looked like a pyramid scheme. This was my shorthand for "avoid at all cost." The information was forwarded along to our mutual contact and the reply back was not what I was expecting: "Are all pyramid schemes bad?" Some pyramid schemes are harder to identify than others, but even those that are easy to identify find prey in unassuming victims. A good rule of thumb is to run, not walk, away from anything that even hints of being a pyramid scheme. Thankfully, bitcoin is not one of them. While it may seem obvious, not everyone understands what a pyramid scheme actually is, what the warning signs may be, or why such schemes always fail.

Definition of a Pyramid Scheme – Securities & Exchange Commission

> *In the classic "pyramid" scheme, participants attempt to make money solely by recruiting new participants into the program. The hallmark of these schemes is the promise of sky-high returns in a short period of time for doing nothing other than handing over your money and getting others to do the same. The fraudsters behind a pyramid scheme may go to great lengths to make the program look like a legitimate multi-level marketing (MLM) program. But despite their claims to have legitimate products or services to sell, these fraudsters simply use money coming in from new recruits to pay off early stage investors. – US Securities & Exchange Commission (SEC)*

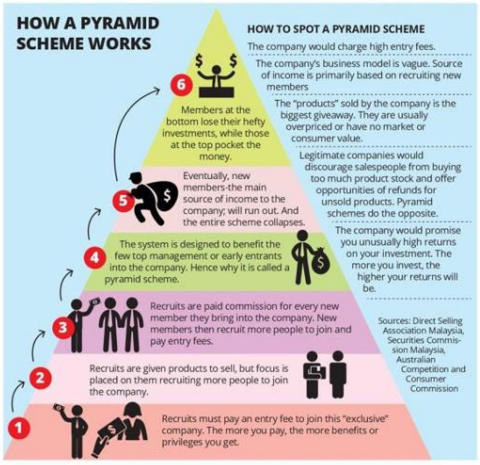
Warning Signs of a Pyramid Scheme – Federal Trade Commission

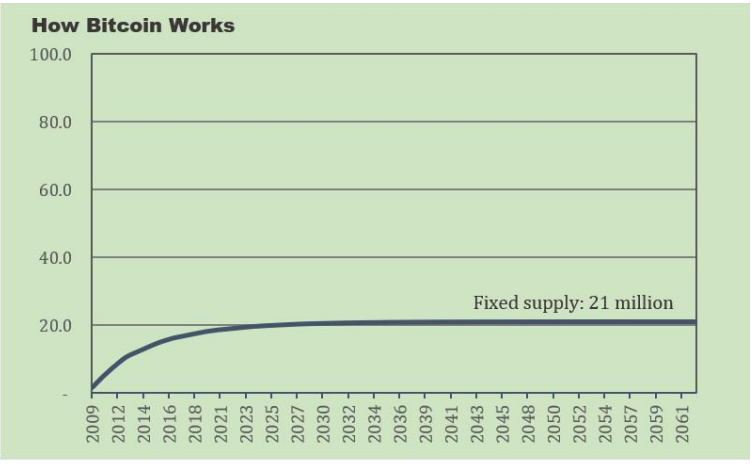
> - *Promoters make extravagant promises about your earning potential. Stop. Such promises are false.*
> - *Promoters emphasize recruiting new distributors for your sales network as the real way to make money. Walk away. In a legitimate MLM program, you should be able to make money just by selling the product.*
> - *Promoters play on your emotions or use high-pressure sales tactics, maybe saying you'll lose the opportunity if you don't act now and discouraging you from taking time to study the company. Leave by the nearest exit. Any company that tries to pressure you to join is one to avoid.*
> - *Distributors buy more products than they want to use or can resell, just to stay active in the company or to qualify for bonuses or other rewards. If you see this happening, keep your money.*

Not all multi-level marketing programs are pyramid schemes, but all pyramid schemes are in some fashion a multi-level marketing program. With pyramid schemes, there is always some company and it is selling a product for which the end demand falls far short of the available supply. The company recruits participants to purchase inventory and to recruit new participants. The participants are all sales people, and compensation is tied mostly to recruiting,

rather than selling the actual product. Often the sale of product is purposefully woven into the recruitment process.

In a normal sales-driven business, the company takes on the inventory risk and pays commissions based on sales to end users. In a pyramid scheme, the sales people take on the inventory risk, rather than the company, and compensation is paid for recruiting more sales people and selling product through to new participants. It all falls apart because sufficient end demand for the product does not actually exist. Everyone up the chain can make money at the expense of the new recruits at the end of the line. This is a pyramid scheme. Bitcoin is not. Bitcoin is not a company. It has no employees and its supply is finitely scarce. No matter how many people adopt it, there will only ever be 21 million bitcoin.





The distinctions should be glaringly obvious, but because bitcoin is complex and the very idea of money is not well understood, it can easily be confused. Bitcoin will only become a global reserve currency if hundreds of millions (if not billions) more adopt it. And seemingly everyone that goes down the bitcoin rabbit hole ends up on the other side explaining it to their family and friends, pitching it as a better form of money. Sounds kind of like a pyramid scheme, right? Wrong. When Dell started selling PCs on its website in 1996 and everyone told their friends to get a Dell, was it a pyramid scheme? When Apple released the first iPhone in 2007 and everyone told their friends to drop the Blackberry for its superior successor, was it a pyramid scheme?

Technological shifts often happen fast. Ten and twenty years later, smartphones and PCs are ubiquitous. It is all about the quality of the product and the incentive structure. If someone owned Apple stock or Dell stock, did it change the fact that the product itself provided a real value proposition? Was there a direct benefit for telling people about a new technological innovation? The value proposition of an innovation trumps all else. It does not matter how you learn about it; all that matters is whether the innovation provides utility. If

it does, people will want to use it; if it doesn't, they won't. That is what makes a market.

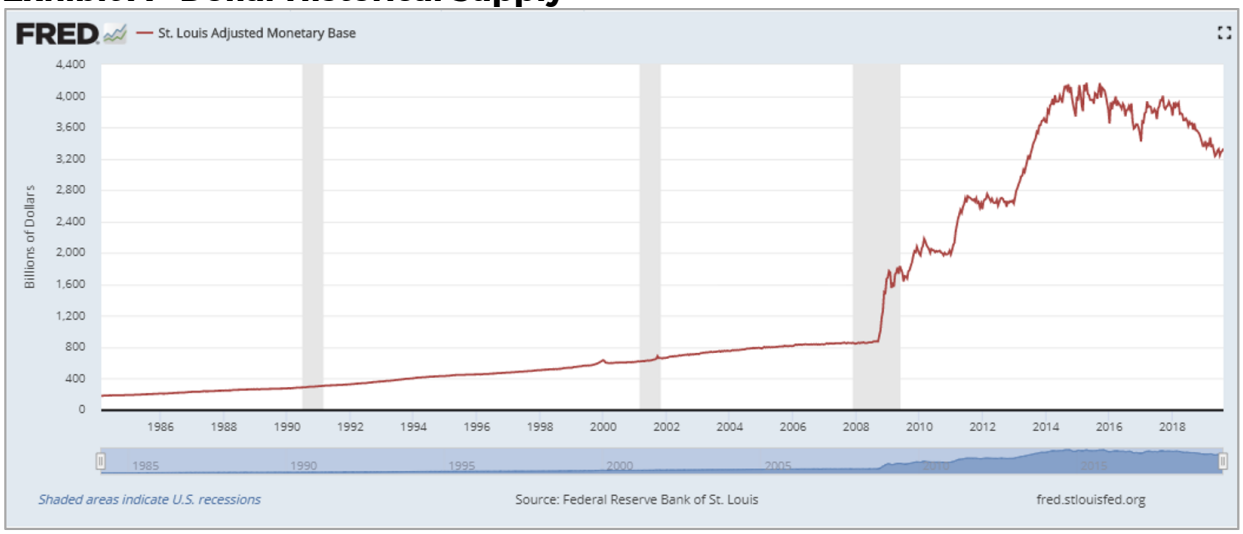
The Utility & Innovation of Bitcoin

Bitcoin's utility is as money. It has a market because it solves a problem inherent in modern money. Not only is bitcoin not a pyramid scheme; it is fundamentally distinct from the class of innovation that could be offered by any individual company. Bitcoin is not Dell and it is not Apple. It is not a tech stock. There is no company that exists behind bitcoin. Bitcoin is not a company selling a product and there is no income stream to pay future dividends. Bitcoin is not about making money; instead, bitcoin is money, or at least it has become money to those choosing to store a portion of their wealth in it. And it's not a get-rich-quick scheme; it is fundamentally about storing the value you have already created. Bitcoin is a bearer asset; however, unlike a bearer bond, there is no income stream.

Bitcoin's innovation is that it represents a superior form of money, but there are no future promises beyond being in possession of a digital bearer instrument. The only utility of bitcoin is in holding it as a currency and transacting with it in the future, whether that be in exchange for legacy currencies or other goods and services. Bitcoin is only useful as a form of money, and it will only maintain value if others demand it in the future. But this is true of any form of money (not just bitcoin). Money is not a collective hallucination or merely a belief system; monetary goods have distinct properties which make them more or less effective in facilitating exchange. However, monetary properties are not absolute; the relative strength of monetary properties is the fundamental basis of demand. When the market evaluates bitcoin, it does so relative to other monetary mediums (the dollar, euro, yen, gold, etc.).

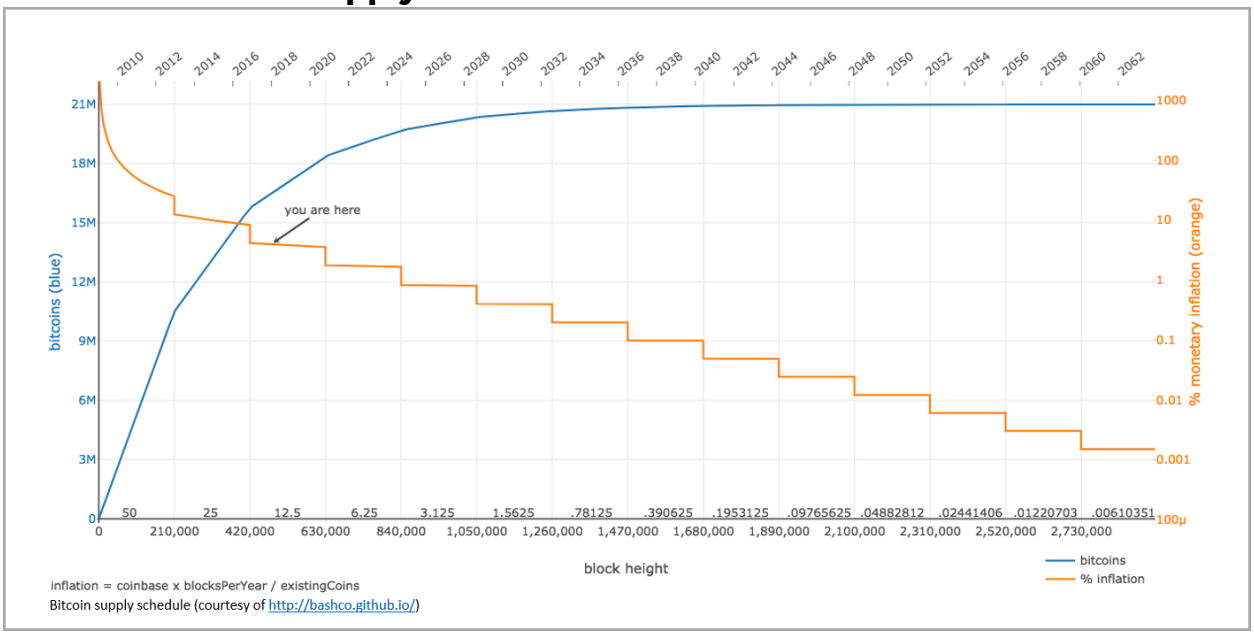
The supply of bitcoin, and its rigid supply constraint, is the foundation of bitcoin's utility and fundamental demand; it is also why bitcoin is not a pyramid scheme. There will only ever be 21 million bitcoin. That is bitcoin's schelling point. Everyone knows it; everyone remembers it. Everyone can also verify it at any point in time. For discussion of how and why bitcoin has a credibly fixed supply, see *Bitcoin, Not Blockchain* and *Bitcoin is Not Backed by Nothing*. But for now, just work on the assumption that the supply of bitcoin is capped at 21 million. In contrast, no one knows the supply of dollars. The Fed estimates the current supply of dollars, but no one knows how many dollars will exist in the future. There is no constraint on the supply of the dollar, other than the Federal Reserve, and all we know for sure is that many more dollars will exist in the future; it is a limitless function. In the end, there is fundamental demand for bitcoin because its monetary policy is i) optimally engineered and ii) credibly enforced. Relative to its competition, bitcoin is a vastly superior monetary medium.

Exhibit A – Dollar Historical Supply



Note: The Adjusted Monetary Base is the sum of currency (including coin) in circulation outside Federal Reserve Banks and the U.S. Treasury, plus deposits held by depository institutions at Federal Reserve Banks. These data are adjusted for the effects of changes in statutory reserve requirements on the quantity of base money held by depositories.

Exhibit B – Bitcoin Supply Schedule

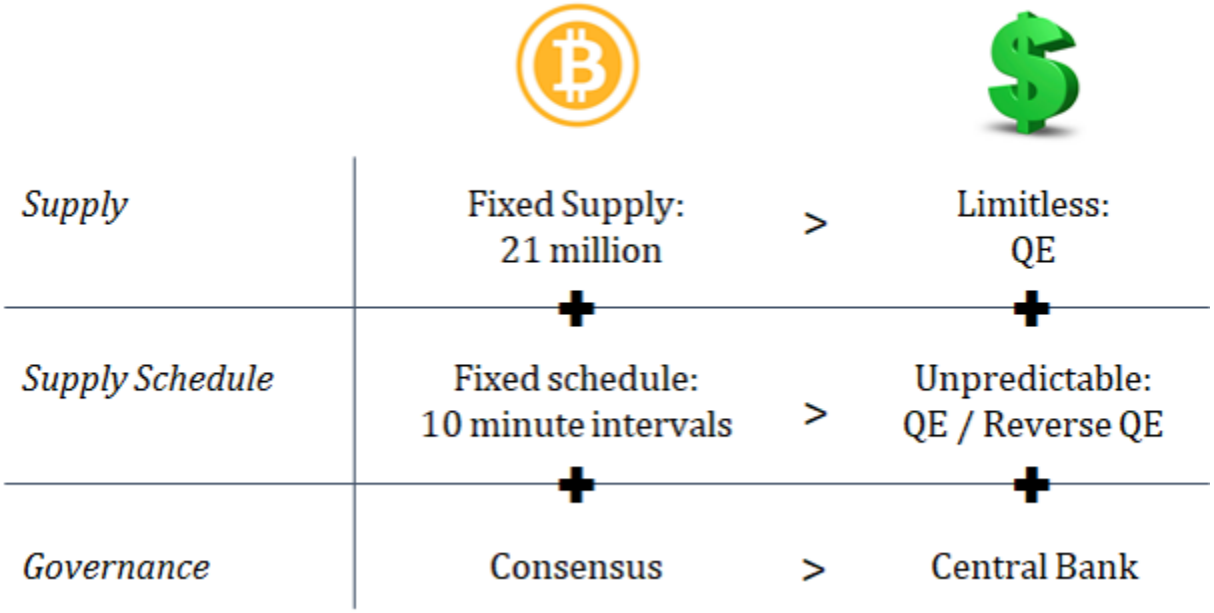


The monetary base in fiat systems changes unpredictably whereas the monetary base in bitcoin is governed by a well-defined supply schedule. Think about the monetary base as setting the foundation of a global economic system. The unpredictable changes in the supply of dollars is not merely akin to shifting the proverbial goal posts. Instead, it is more similar to building the field on a 1980s-style water bed, and then shifting the goal posts. The whole game is distorted, not just the end points. Bitcoin, on the other hand, is a bedrock as a function of its fixed supply, and over time, the foundation becomes stronger and stronger. The credibility of its supply schedule is reinforced with each passing bitcoin block. As it becomes more evident that

bitcoin's supply schedule is credibly enforced, more people adopt bitcoin as a form of money, and those that already have increasingly use it as a store of wealth. Fixed supply + increasing adoption = increased value. As adoption increases and as value rises, bitcoin becomes further decentralized. And as bitcoin decentralizes over time, it becomes harder to change, reinforcing the credibility of its foundation: its fixed supply.

You are the Scammer

In a pyramid scheme, the people selling the scheme are the scammers. These scammers are selling the promise of future monetary gains through high-pressure sales tactics and by recruiting new members to the scheme as the primary compensation mechanism. In bitcoin, the people buying bitcoin are the scammers, as described in Michael Goldstein's timeless piece, Everyone's a Scammer. If this is you, you are the scammer. In most cases today, whenever someone buys bitcoin, they are directly trading a fractionally reserved form of currency (with the promise of future debasement) in return for a bearer asset with a finite supply and a vastly superior monetary policy. The person on the other end of the line is getting the raw deal. It is not to say that literally everyone that sells a bitcoin does so without good reason. It is money after all, and its utility is in exchange; by definition, market participants have a wide variety of present needs for liquidity and real value is transferred every time a bitcoin is transacted, whether for dollars or for goods and services. However, on average and over the longer-term, it is information asymmetry in full effect. Bitcoin's monetary policy is optimally engineered and credibly enforced, though few understand it, which is why it represents the greatest asymmetry in the world today.



Monetary First Principles

A monetary medium with the lowest rate of change is most effective in communicating economic signals, and a fixed supply (zero rate of change) is the optimal monetary policy end game. While the monoculture that is modern mainstream academia disagrees with this view, a fixed supply currency is superior to a currency that increases in supply over time (and at unpredictable rates). In any economy, supply and demand for goods and services relative to the supply and demand of money dictates prices. Price is what ultimately coordinates economic activity, and money is the foundation of the pricing mechanism within an economy. A currency with a fixed supply would remove the noise created by changes to the money supply in the price system, thus creating more reliable market signals. Because a monetary good facilitates the exchange between goods used for the purpose of either consumption or production, the form of money with the lowest rate of change will most accurately reflect changes in supply and demand of all other goods. Essentially, money is used to communicate the relative value of other goods and services, and changes in the money supply distort the communication of this information by introducing an extraneous variable to the equation.

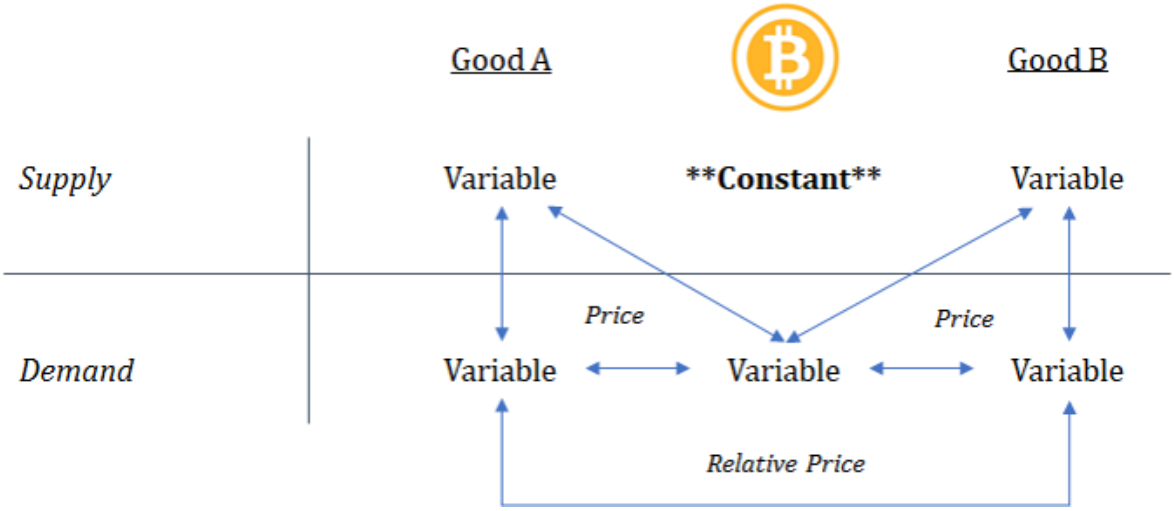
For example, an iPhone costs approximately $1,000, whereas a barrel of oil costs approximately $50. The information communicated through a monetary medium is that an iPhone costs approximately 20 times more than a barrel of oil. Money communicates opportunity cost (economic trade-offs) through its price system, and the more constant the quantity of money (lower rate of change), the more reliable the communication of information and economic trade-offs. If the money supply increased by 10% and prices adjusted equally, an iPhone would cost $1,100 and a barrel oil would cost $55. An iPhone would still cost 20 times more than a barrel of oil, and that is the relevant information which all market participants rely upon. In the real world, the problem is that prices do not adjust equally as the money supply changes. Instead, price signals become distorted. In a world with a constant money supply, changes in price would more accurately reflect changes in supply and demand in underlying markets for goods and services rather than also reflecting the unequal impact of a changing money supply. Changes in the money supply create noise extraneous to the underlying economic activity. Price coordinates economic trade-offs, and the reliability of a pricing system is dependent on the stability of the form of money used to communicate information.

> *Hayek, The Use of Knowledge in Society*
>
> We must look at the price system as such a mechanism for communicating information if we want to understand its real function—a function which, of course, it fulfils less perfectly as prices grow more rigid. (Even when quoted prices have become quite rigid, however, the forces which would operate through changes in price still operate to a considerable extent through changes in the other terms of the contract.) The most significant fact about this system is the economy of knowledge with which it operates, or how little the individual participants need to know in order to be able to take the right action. In abbreviated form, by a kind of symbol, only the most essential information is passed on and passed on only to those concerned. It is more than a metaphor to describe the price system as a kind of machinery for registering change, or a system of telecommunications which enables individual producers to watch merely the movement of a few pointers, as an engineer might watch the hands of a few dials, in order to adjust their activities to changes of which they may never know more than is reflected in the price movement.

In that regard, monetary goods are differentiated (at least those that emerge on the free market); it is why money is an effective communication tool. The market structure for money is different than that of all other goods. A consumption good is consumed and a production good is ultimately consumed in the production of other consumption goods. Whereas, the utility of money is in exchange; it is functional in the coordination of trade by and between consumption and production goods, rather than being consumed itself. Because the utility of money is in exchange, scarcity is more important than the nominal amount of money in an economy. As demand for money increases and as its price rises, there is not a commensurate supply response because of natural supply constraints. The same is not true for any individual good or service. The relative supply constraint of money is what allows it to communicate relative value between other goods and services. Consumption goods and production goods can be substituted for each other, but money facilitates virtually all exchange between all other goods. The value of a money may fluctuate relative to goods and services but relative scarcity of a money supply allows price to be communicated in terms of the money itself.

Prior to bitcoin, no form of money was finitely scarce. Bitcoin has a fixed supply, capped at 21 million. Finite scarcity creates a constant where none existed previously. Imagine the supply of one good being perfectly constant while the supply of all other goods fluctuates. Demand for all goods changes, but only one constant exists: the supply of bitcoin. In this world, everything would be measured against the constant. The purchasing power of money would communicate far more perfect information through this pricing mechanism than if the supply of the money itself were changing. By creating one constant, everything else can be more reliably measured. And the desired

information is not the absolute value of any one good. All value is subjective. Instead, the critical information communicated through a pricing mechanism is the relative value (or relative price) of many goods to each other. While price levels are ever changing due to constantly shifting supply and demand, the stability of the pricing mechanism itself allows for economic coordination via the communication of opportunity cost (i.e. how we know, or learn, that an iPhone costs approximately 20 times more than a barrel of oil).



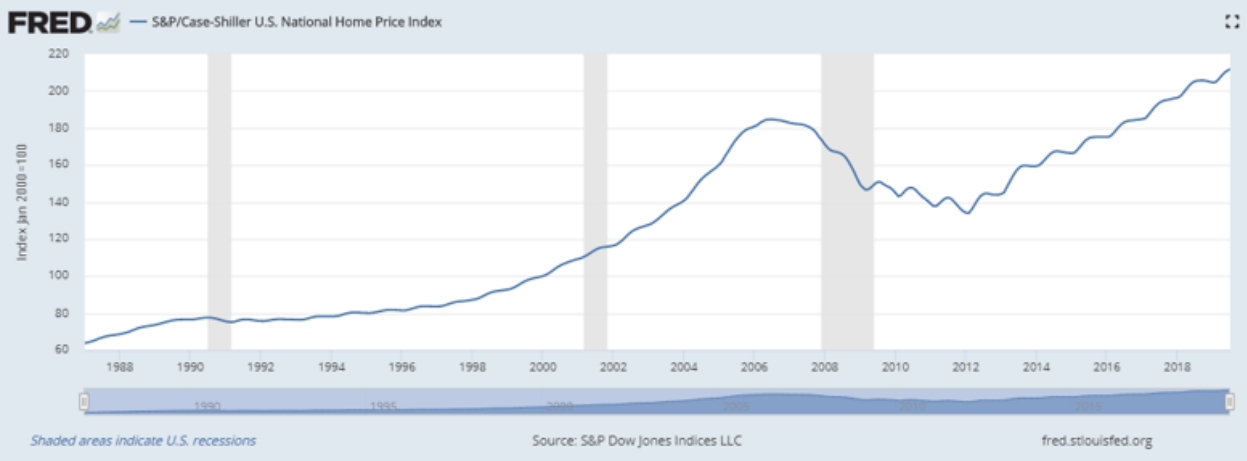
Distortion of the Price System

In our current system, the supply of money changes unpredictably and increases over time. This is core to the central banking monetary model, and it derives from monetarist economic theory which argues that an active management of the money supply stimulates *aggregate demand* and ultimately promotes full employment. What it technically does is manipulate interest rates downward by increasing the supply of money. Lower interest rates increase the willingness and incentive to borrow; however, all else being equal, a lower interest would otherwise decrease the willingness to lend. Essentially, by inflating the money supply, the central bank artificially manipulates the function of credit, creating a sustained imbalance between the incentive to borrow and the willingness to lend. The more pervasive consequence is the distortion of the pricing mechanism that coordinates economic activity. By manipulating the supply of money and the supply of credit, central banks distort all prices throughout the market. False signals (and bad information) are distributed to all market participants.

The entire supply and demand structure of the economy becomes distorted as hundreds of millions of people respond to manipulated price signals and when resources within the economy are re-allocated based on those signals. When the money supply is increased, new money (and credit) enters the system through various channels and at unpredictable times. The quantity and rate of

change is unknown to most market participants. Instead, market participants react to price signals; that is how information is communicated. A price signal may be the cost of a good at the supermarket or it may be a salary an employer is willing to pay for a certain job. The change in the money supply creates a distortion of prices such that market participants cannot effectively understand whether changes in price are driven by changes in underlying supply and demand structures, or to what extent changes in price are merely a function of more or less money in the system. Regardless, everyone reacts to distorted signals.

For a more tangible example, the Fed purchased $1.7 trillion of mortgage-backed securities (~17% of all mortgages) following the financial crisis as part of its quantitative easing program, which ultimately increased the base money supply by $3.6 trillion. Most people recall that prior to the financial crisis there was a housing bubble. By directly purchasing mortgages and by inflating the money supply, the Fed manipulated interest rates lower. Housing relies heavily on the supply of credit and ultimately on the cost of interest. With lower interest rates and more money available to lend, housing prices were manipulated higher. As a result, distorted price signals were sent to both buyers and sellers. Developers of housing respond by building more homes (increasing supply) and buyers of homes believe they can take on more debt at lower rates to purchase homes. More resources in the economy are devoted to the function of housing because of higher price levels. However, any increase in demand can only be sustained so long as the cost of credit is continually manipulated downward as a function of an increasing money supply.



Despite wide recognition of the unsustainable housing bubble in 2007, the national home price index is now 15% higher than it was at the prior peak. This is the manipulation of price levels on full display, and it happens as an intended function of central bank monetary policy. The Fed increases the money supply, lowers interest rates, and inflates asset prices such that the amount of existing debt in the credit system can be sustained. Credit

expansion is the Fed's objective in stimulating growth, and net new credit cannot be created unless existing debt levels can be sustained, which is why the Fed must inflate asset prices to achieve its objectives. Asset prices support existing debt levels. When everyone figures out the price signals are unsustainable and unreliable, it causes a shock to the system. This is what happened in 2007 and it is likely to happen again as the market signals have become even further distorted. But it is not some evil scheme; the Fed is not a purposively malicious actor. The Fed ultimately intends to promote "full employment" through its policies, but what it actually does is manipulate relative price signals which creates imbalances in the underlying supply and demand structures of the economy, creating sudden and more chronic unemployment.

Hayek spoke on this subject in his 1974 Nobel Prize winning speech, the Pretense of Knowledge. As a function of manipulated prices, more resources are devoted to a segment of the economy than could otherwise be sustained naturally; when the central bank changes the course of its monetary policy, prices begin to respond and the market corrects. Because price levels have been manipulated on a sustained basis, a demand shock becomes inevitable and everyone figures out imbalances exist. In the case of the housing example, supply (both of goods and labor) significantly exceeds sustainable demand at current price levels. More broadly, imbalances are everywhere. It becomes apparent that supply and demand are significantly out of balance and unemployment increases rapidly. The market cannot find an equilibrium because all markets have been manipulated on a sustained basis for extended periods of time.

Hayek, The Pretense of Knowledge

In fact, in the case discussed, the very measures which the dominant "macroeconomic" theory has recommended as a remedy for unemployment — namely, the increase of aggregate demand — have become a cause of a very extensive misallocation of resources which is likely to make later large-scale unemployment inevitable. The continuous injection of additional amounts of money at points of the economic system where it creates a temporary demand which must cease when the increase of the quantity of money stops or slows down, together with the expectation of a continuing rise of prices, draws labor and other resources into which can last only so long as the increase of the quantity of money continues at the same rate — or perhaps even only so long as it continues to accelerate at a given rate. What this policy has produced is not so much a level of employment that could not have been brought about in other ways, as a distribution of employment which cannot be indefinitely maintained and which after some time can be maintained only by a rate of inflation which would rapidly lead to a disorganization of all economic activity. The fact is that by a mistaken theoretical view we have been led into a precarious position in which we cannot prevent substantial unemployment from reappearing; not because, as this view is sometimes misrepresented, this unemployment is deliberately brought about as a means to combat inflation, but because it is now bound to occur as a deeply regrettable but inescapable consequence of the mistaken policies of the past as soon as inflation ceases to accelerate.

This is what occurred during, and in the aftermath of, the financial crisis. It was the boiling over point after the Fed had manipulated the supply of money and the supply of credit for decades. As portrayed in the Big Short, the financial crisis often gets blamed on the subprime crisis, but the not-often-discussed 800-pound gorilla in the room is central bank monetary policy. Following the crisis, the Fed responded by pursuing the same policy action it had pursued for decades but on a much greater scale; it massively increased the money supply, further manipulating price signals. When the money supply is manipulated, recognize that not all price levels respond ratably. Money enters the system through different channels and the expansion of credit impacts certain segment of the economy more than others. All prices are manipulated, but not equally. It is fundamentally the distortion of relative prices which disrupt the underlying supply and demand function of a market. Price communicates information. It is how market participants communicate what they value on a relative basis. And, it is how all market participants then respond to those preferences on the supply side: what skills people train themselves with, what businesses people choose to build, what employment opportunities people seek. The Fed may not intend to do harm by manipulating the money supply, but ultimately, it is the unavoidable consequence of distorting the price mechanism within an economy.

Predictability of the Money Supply

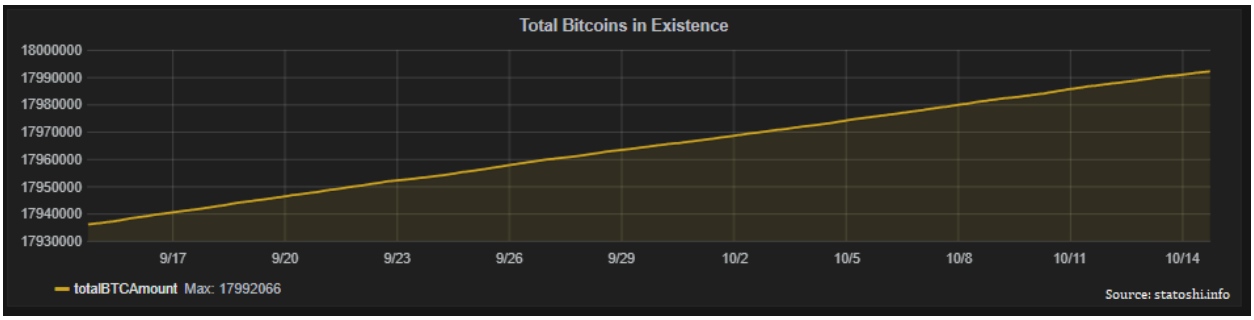
Bitcoin is the white knight. Or at least, it has the potential to be. By creating a fixed supply, bitcoin has the potential to be the greatest pricing mechanism

the world has ever known. Once bitcoin reaches its maximum supply of 21 million, changes to the money supply will be removed entirely from the equation of price signals. It should be axiomatic that the creation of money does nothing to generate real economic activity. It doesn't matter whether the change in the money supply is predictably small or whether the money supply increases significantly and unpredictably. Printing money does nothing to generate economic activity; it only serves to distort supply and demand. The utility of money is in exchange. Whether present exchange or future exchange, that is all. Money is not consumed; it is used to coordinate the economic activity that allows for capital to be accumulated. Whether it be physical capital required to produce real goods or human capital which advances arts, science, mathematics etc. That capital is the true savings of a society and it is fundamental to the function of an economy.

Most people think of savings in monetary terms because money is a unit of account, but real savings is represented by the accumulated capital that enriches the lives of individuals, families, and communities. In a world with a fixed money supply, monetary savings would be constant. Money would transfer from individual to individual, family to family, or business to business. But, in total, the money supply would neither increase or decrease. Economic activity would be coordinated as a function of money and with an undistorted pricing mechanism. The aggregate preferences of all markets would be more accurately communicated without the distortion of a changing money supply. Imbalances in supply and demand would be naturally corrected and not sustained over long periods of time; as a consequence, imbalances would also be smaller and not systemic to the economy as a whole. It does not mean all prices would always be perfect or that other variables, such as government spending or taxes, could not influence or distort economic activity. However, it would eliminate the primary mechanism that distorts price signals and market structures.

Bitcoin's fixed supply is the foundation of its more reliable pricing system but it is also issued at a predictable rate. In the future state, when bitcoin reaches its maximum supply, the rate of change thereafter will be zero. But on its way to that future state, bitcoin imbeds a stable and predictable supply schedule, which is a distinct and equally important part of the equation. Bitcoin are issued through a mining process that helps to secure the network and the network adjusts to ensure that bitcoin are issued on average every ten minutes. If more mining resources are added to the network, the network adjusts to prevent bitcoin from being issued at a faster rate. More mining results in greater levels of network security, rather than increasing the rate of issuance or increasing the total amount of bitcoin that will ultimately be issued. This allows the entire economic system to plan for the future. It allows miners building security infrastructure to forecast future compensation, but it also allows all

market participants to predictably know the rate of change of the currency at any point in time.

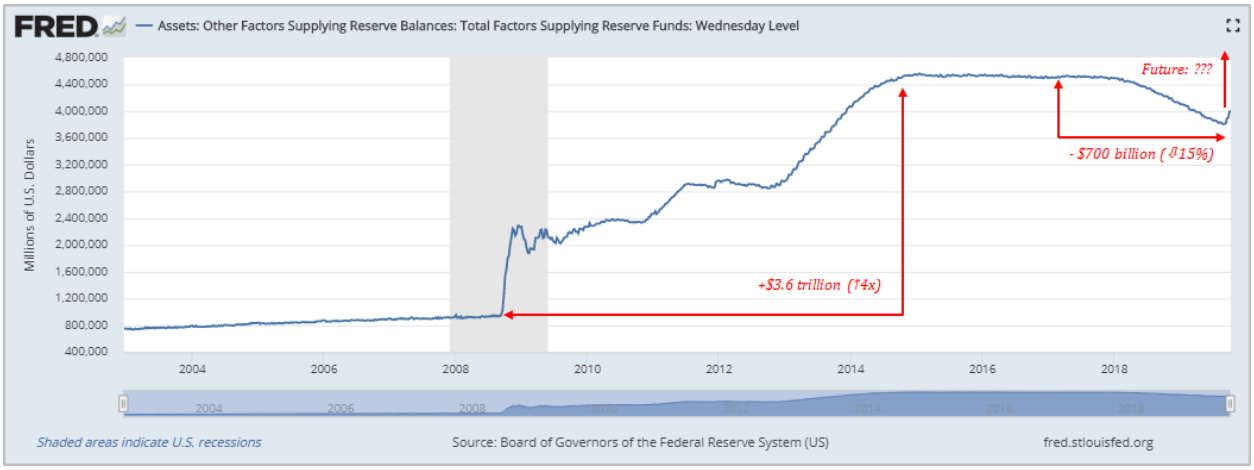


Rather than allowing bitcoin to be issued rapidly or at an unpredictable rate, the network ensures that bitcoin will be issued steadily over time and as a consequence, on a more distributed basis. Most importantly, it constantly reinforces the credibility of the overall issuance structure. Every ten minutes (on average), a certain number of bitcoin are issued. Approximately every four years that number is cut in half until ultimately no incremental bitcoin will be issued. On the path to 21 million, the enforcement of the fixed supply every ten minutes builds credibility in the future state supply over time. All market participants come to understand that the fixed supply will be enforced not because of a magical point in time when the maximum is actually reached, but instead because the network enforces its monetary policy every 10 minutes. By creating a predictable supply schedule, the rate of change predictably decreases, and all market participants can observe for themselves that the system is functioning as intended.

Monetary Policy by Consensus vs. Central Bank

This process which constantly reinforces the credibility of bitcoin's monetary system is occurring in parallel to the dysfunction of legacy monetary systems. Central banks everywhere are increasing the money supply of their respective economies at unpredictable rates. As discussed previously, the Fed increased the money supply in the U.S. by $3.6 trillion following the financial crisis, from 2008 to 2014. Despite the Fed forecasting its plans, no one knew what the total would ultimately be. Everyone was guessing. The Fed didn't even know. And, after increasing the money supply by several multiples, the Fed then began removing $50 billion dollars from the economy each month, a process which began in October 2017. Again, no one knew exactly how much money would actually be removed from the system, in total or for how long. In aggregate, approximately $700 billion in base money was removed over the course of approximately two years. And now, as of October 2019, the Fed has once again shifted course and has begun to add more money back into the system. Just recently, the Fed signaled plans to add $60 billion dollars to the financial system each month (planned for the next six months). But once again, no one

really knows for how long this will go on or whether the amounts will change. Realistically, the Fed does not know because it is impossible to know.

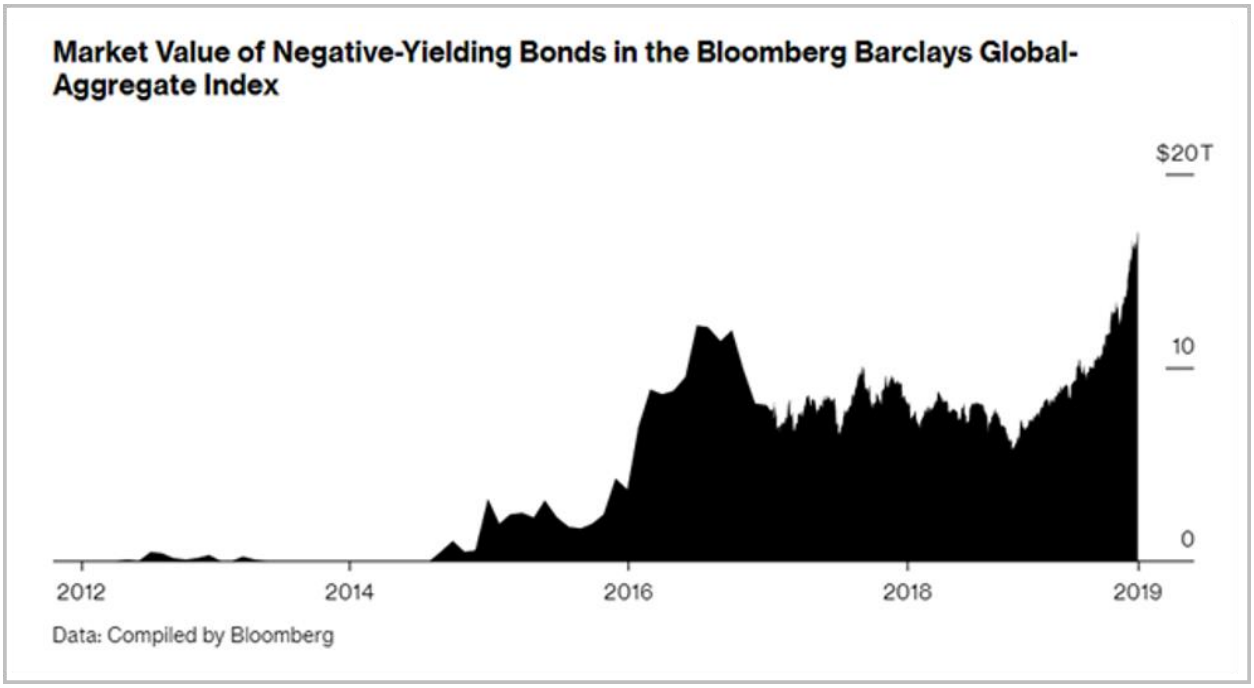


All we practically know is that from this point forward the money supply will increase (and by a lot). But recognize, most market participants have no idea any of this has occurred or is occurring. All market participants really know is what is communicated to them via prices and employment opportunities. Those that have an understanding of the Fed's actions may be in a better position to forecast or predict the directional consequences, but economic systems are complex. We all react to the pricing mechanisms around us and no one has anywhere close to perfect knowledge; this is the pretense of knowledge. The aggregate knowledge of millions of people is communicated through price which is ultimately a function of ever-changing preferences of the individuals that make up an economy.

Individuals are inherently limited in the knowledge they possess. And this is certainly true of central banks. In the central banking monetary model, twelve individuals (or thereabout) determine how and when to create billions, if not trillions, of dollars despite possessing inherently limited knowledge. No matter how well-intentioned or how much knowledge possessed, the net consequence is the distortion of the fundamental mechanism (i.e. the pricing mechanism) which aggregates knowledge possessed by the market as a whole. For everyone relying upon the dollar as a unit of account and as a mechanism to communicate economic trade-offs, the very foundation changes unpredictably, unbeknownst to most of its participants. Distorted price signals are communicated gradually through millions of markets impacting the decisions made by hundreds of millions and the centralized mechanism that dictates monetary policy is a root cause of the distortion.

And even if a reasonable person believed active money supply management to be a net benefit, bitcoin is now operating alongside the legacy economic system: a decentralized system vs. a centralized system. Monetary policy by consensus vs. monetary policy by central bank. While the money supply of the

legacy system is unpredictably changing, the bitcoin network is operating flawlessly with a known supply and with a predictable rate of change. Rather than it being a philosophical or economic debate, there are now two competing systems, and the market will have the last say. While bitcoin may be complicated and the very subject of money may not be well understood, the flaws in the existing system are independent of bitcoin. The $17 trillion of negative yielding debt should be evidence enough and it only exists as a direct consequence of central bank monetary policy. Ultimately, the currencies that support the legacy system will be the release valve because central banks will be forced to increase the money supply in order to sustain what is an otherwise unsustainable credit system.



With the legacy system coordinated by central banks, all one can rely on is that the money supply will change and at unpredictable rates. With bitcoin, everyone can verify the supply and the predictable rate of change. By running a bitcoin full node, anyone can verify the number of valid bitcoin that exist in circulation and the amount of new bitcoin issued in each block. Anyone and everyone can verify this information without trusting anyone else. This is how bitcoin works. Each node not only verifies information; it also validates information independently. Bitcoin's monetary policy is enforced on a decentralized basis by all nodes within the network. With precision, everyone can calculate when future blocks will be solved and when the rate of issuance will change. The fact that everyone can verify and validate the money supply, regardless of the nominal amount, reinforces the credibility of the monetary system. This reinforcement occurs every 10 minutes, 6 times an hour, 144 times a day, 4,320 times a month, 52,560 times a year, with each passing bitcoin

block. The monetary system hardens as market participants validate that the monetary policy is enforced, over and over again, every ten minutes.

Verification of Bitcoin Supply and Rate of Issuance on a Bitcoin Full Node (Block 599114)


```
{
  "height": 599114,
  "bestblock": "00000000000000000009cb4fe3c95f56e1b46c4f9a236f001030069b80a1f752",
  "transactions": 36757926,
  "txouts": 63092086,
  "bogosize": 4745309576,
  "hash_serialized_2":
"f48459e46e1dd3b4f4a28113218182a62c70fc889413c05863e1b905e4c0c7b8",
  "disk_size": 4325276676,
  "total_amount": 17988754.82195437
}
```

```
{
  "avgfee": 3322,
  "avgfeerate": 11,
  "avgtxsize": 374,
  "blockhash": "00000000000000000009cb4fe3c95f56e1b46c4f9a236f001030069b80a1f752",
  "feerate_percentiles": [
    1,
    1,
    5,
    12,
    20
  ],
  "height": 599114,
  "ins": 1248,
  "maxfee": 213338,
  "maxfeerate": 344,
  "maxtxsize": 35567,
  "medianfee": 573,
  "mediantime": 1570921568,
  "mediantxsize": 283,
  "minfee": 134,
  "minfeerate": 1,
  "mintxsize": 189,
  "outs": 1684,
  "subsidy": 1250000000,
  "swtotal_size": 226353,
  "swtotal_weight": 634623,
  "swtxs": 586,
  "time": 1570922984,
  "total_out": 41030997143,
  "total_size": 300482,
  "total_weight": 931139,
  "totalfee": 2667576,
  "txs": 804,
  "utxo_increase": 436,
  "utxo_size_inc": 53631
}
```


Supply & rate of issuance verified on four year-old Apple laptop (supply: 17,988,755; block subsidy = 12.5 bitcoin or 1,250,000,000 satoshis)

A fixed supply is of little meaning without the credibility of its enforcement. Anyone can copy bitcoin's architecture and code base. But what cannot be replicated is the credibility of its monetary properties. The consensus mechanism which governs bitcoin is the foundation of its credibility and what ultimately sets bitcoin apart from its competition. Even if an individual remained unconvinced that a currency with a fixed supply would communicate better information through its pricing mechanism, it does not matter what any individual believes. Bitcoin entrusts its monetary policy to a consensus mechanism. While the maximum supply of bitcoin is practically capped at 21 million, the supply is ultimately governed by a consensus of those that hold bitcoin as a currency.

If the market, which unquestionably possesses more information than any individual, collectively determined that it would be better to change the supply schedule rather than implementing a fixed cap, it is theoretically possible. However, the market would have to come to an overwhelming consensus to effect that change, and practically speaking, a decentralized network of rational economic actors would not form an overwhelming consensus to debase its own currency. Bitcoin's monetary policy is flexible enough to change but it is impossible to do so without an overwhelming consensus. Bitcoin ultimately represents the contrast between monetary policy by consensus and monetary policy by central bank. The information possessed by a market consensus mechanism will always exceed that of a small number of individuals, which is why bitcoin out-competes the legacy system at every step.

Bitcoin is Not a Pyramid Scheme

So no, bitcoin is not a pyramid scheme. It is not organized by a sketchy company, pushing high pressure sales tactics. It is not peddling some inferior consumer good, with abundant supply, where compensation is directly tied to recruiting new members to the scheme. Bitcoin is money and its supply is finitely scarce. It does not matter how many people adopt bitcoin; as adoption increases, the same pie is distributed across more and more people, and on average, more people control a smaller and smaller share of the network. Its value increases as a function adoption, and adoption is increasing because its monetary properties are superior to the competition. Bitcoin has a fixed supply, its supply schedule is predictable, and its monetary policy is governed and enforced by consensus. Bitcoin's pricing mechanism is unmanipulable and cannot be distorted because of its fixed supply. Everything changes around bitcoin but bitcoin's fixed supply is the constant. Because bitcoin's supply is fixed and cannot be manipulated, it will eventually become the most reliable pricing mechanism in the world, and consequently, the greatest distribution system of knowledge.

That is the promise which bitcoin provides, and it will only proliferate if it creates utility for those that adopt it. Today and into future, that utility will continue to be the ability to reliably store wealth in a monetary medium that cannot be debased. When people make the claim that bitcoin could be "bigger-than-the-internet," it is generally not a linear application, but instead rooted in the idea that a sovereign, unmanipulable form of money has the potential to be one of the greatest instruments of freedom ever invented. The success of bitcoin is not a given, but if successful in delivering on its promise, it will facilitate more effective and more peaceable coordination by and amongst people throughout the world. At the end of the day, bitcoin is a communication tool. That is the function of money. Bitcoin simply provides an alternative system, operating on a decentralized basis which no one controls. It is the lack of control and the lack of conscious direction which will allow bitcoin to accumulate and communicate knowledge more effectively than any pre-existing monetary medium. Current volatility is nothing more than the logical path of price discovery, as adoption increases exponentially over time and as we advance toward that future state of full adoption.

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

Tweetstorm: 5 Insanely Bullish Charts for Bitcoin

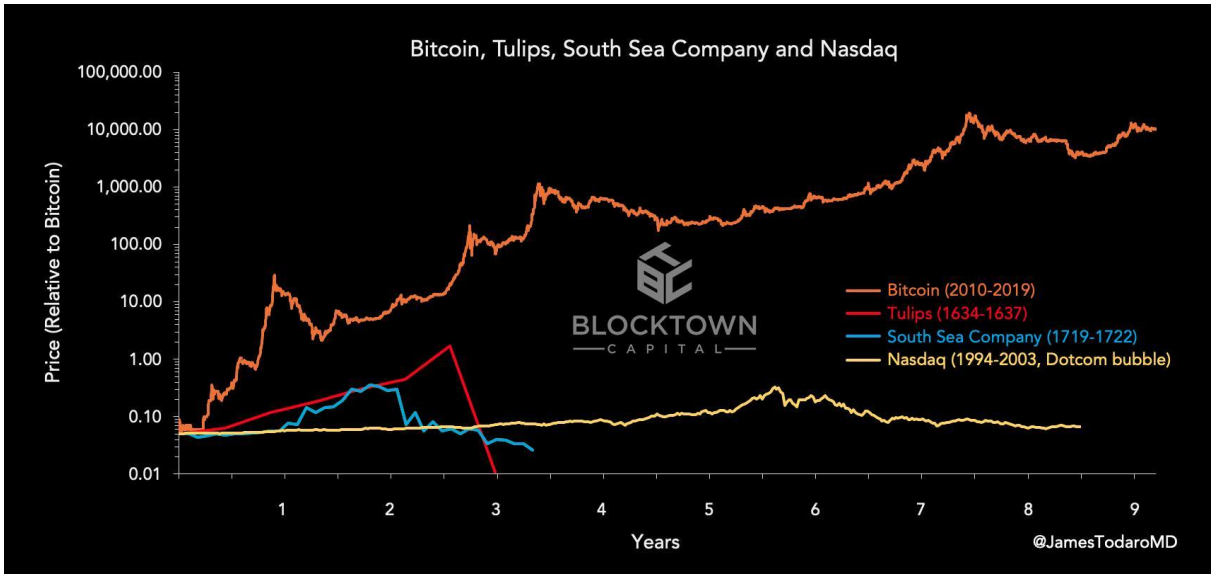
By James Todaro

Posted September 20, 2019

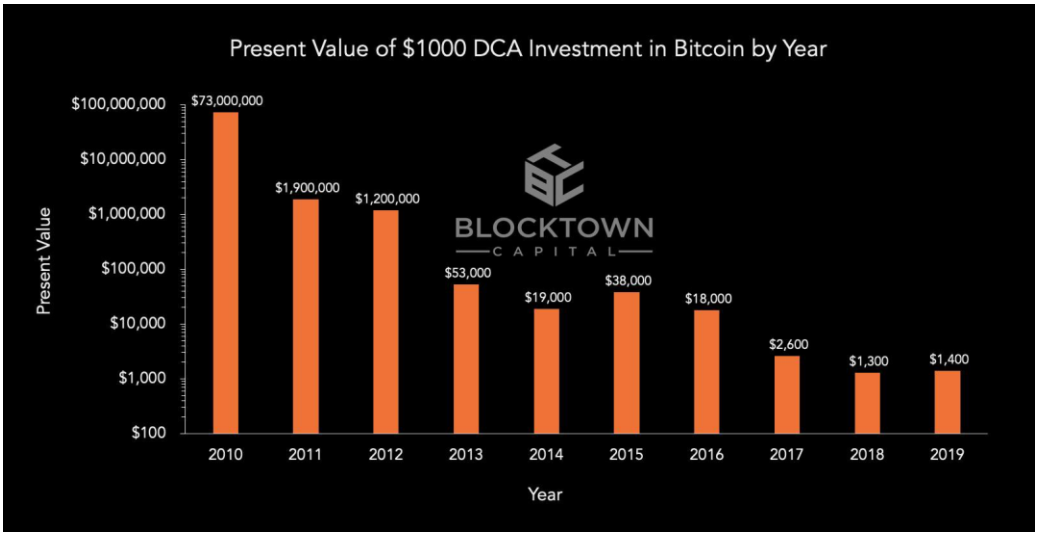
Five INSANELY bullish charts for bitcoin. 🚀🚀🚀 $BTC #bitcoin

1/ Bitcoin looks nothing like the Tulip Mania or South Sea Company bubbles, which only lasted an illiquid and brief 3 years.

Bitcoin has been growing for 10 years with billions of dollars traded daily.

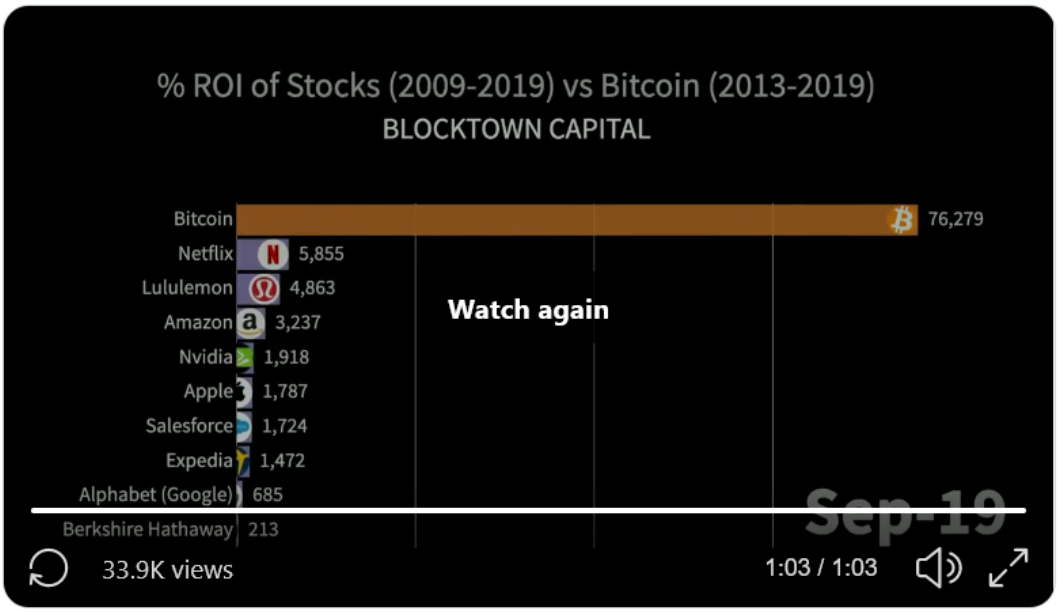


2/ If you dollar cost averaged into bitcoin weekly, every year would result in positive returns at today's prices, including 2018 and 2019.



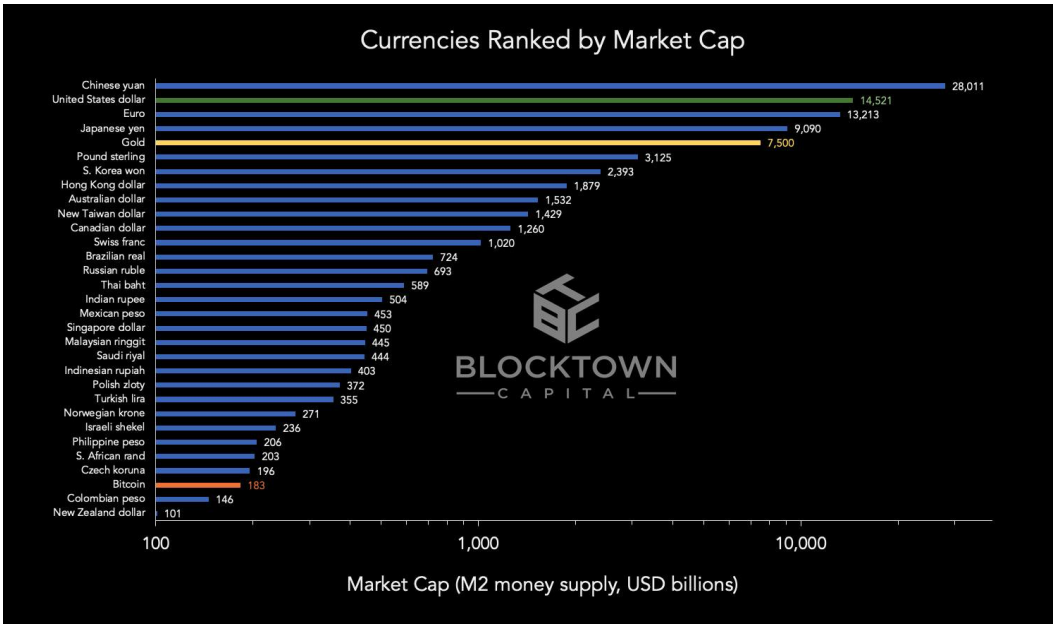
3/ Bitcoin dominates the best performing tech stocks in returns over the past decade, even when giving tech companies a 4 year head start. 🔥🔥🔥

Berkshire Hathaway added for fun.



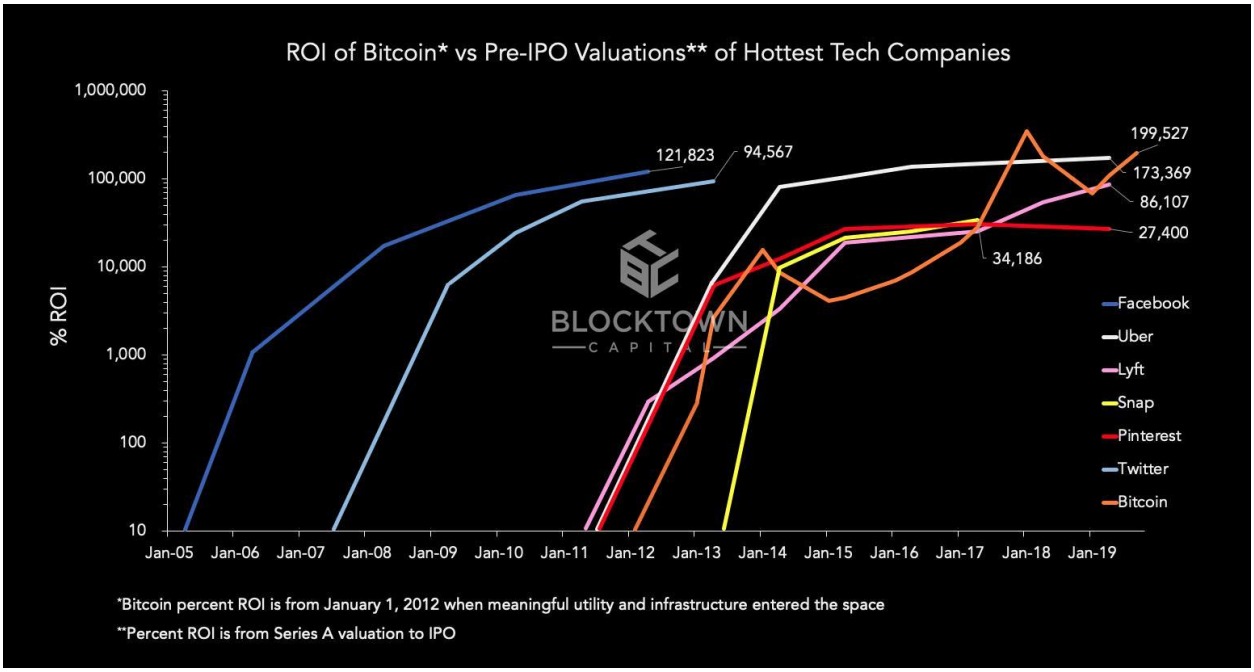
4/ On the scale of a global currency, bitcoin is still small, just passing the Colombian peso and New Zealand dollar in market cap, and is still far from the market cap of gold.

There is tremendous room for bitcoin to grow into a global store of value. 🚀



5/ Returns over 10,000% were previously only available to accredited investors and VCs in the form of private equity deals.

Bitcoin levels the playing field, allowing anyone to invest with the opportunity for tremendous gains. #bitcoin #Uber #Facebook #Lyft



A Fossil Fuel Future for Bitcoin Mining

By Maximilian Fiege

Posted October 22, 2019

This is an adaptation of a report originally written for clients of Signum Global Advisors alongside Angela Dalton, Managing Partner for Technology.

The launch of Application-Specific Integrated Circuits (ASICs) for Bitcoin mining 2013 set off a modern day gold rush. In the six years since, miners have scoured the globe in search of cheap electricity to power the commercial-scale operations made possible by such special purpose hardware. Their scramble has raised eyebrows along the way, with headlines decrying Proof-of-Work as some deal with the devil in the age of climate consciousness. This past year, however, miners found their work vindicated by research indicating that three-fourths of all mining draws on marginal renewable electricity at little expense to surrounding communities. This should bring an end to the energy debate once and for all, no?

Not quite. Because while we had the good fortune of Bitcoin emerging during a peculiar period of energy abundance, we are not likely to see these conditions continue on in perpetuity. And rather than assume that certain supply gluts will remain, we should instead take a proactive approach in forecasting how growing demand for renewable energy, and tumbling fossil fuel asset prices, will create new ones.

The Subsidization of Proof-of-Work

Consider the following thought experiment: what if the Oil Shock of 2007 had precipitated a near-decade of economic malaise like the OPEC crisis of 1973 had done? As you suspend your disbelief, you might ponder how the emergence of ASIC mining in 2013 would have played out. A perfect storm of

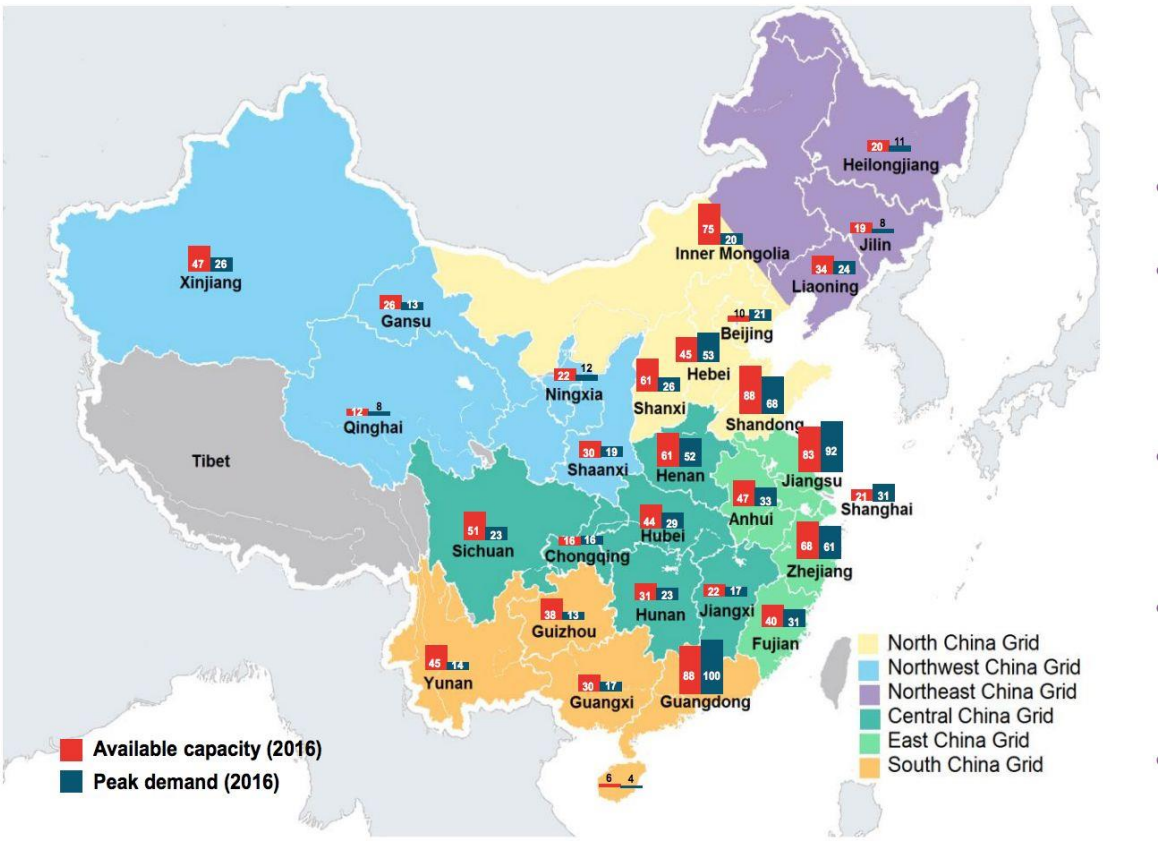
high energy costs and utilities' conservation policies would impact miner willingness to contribute computing power. The constrained hashrate affords weaker network security, and low government tolerance for consumption would also attract greater scrutiny. It remains unclear to what degree a Proof-of-Work network could scale in a period of energy scarcity.

Now let us return to the real world, in which Satoshi released the Bitcoin source code on the eve of an energy sector expansion unlike anything seen since the Oil Boom a century prior. In particular, 2009 marked the intersection of three trends that have defined the energy market of the past decade:

- **The culmination** of a two decades-long buildout of Chinese hydropower
- **The middle** of America's transformation into a net exporter of natural gas
- **The beginning** of solar power carving out product-market fit worldwide

The ramifications of these trends are myriad, but of relevance to Bitcoin mining is the glacial pace at which grid operators have responded to this changing power generation landscape. The challenges posed by integrating the intermittent energy produced by renewable sources has left them scrambling to scale up energy balancing, transmission, and storage capabilities

Available capacity versus peak demand by province, 2016 (GW)



Source: Bloomberg New Energy Finance, CEC. Note: Based on the global standard, we assumed available load factor of hydropower =50%, pumped hydro =100%, coal 90%, gas 90%, nuclear 80%, wind 10%, solar 30%, biomass 70%.

accordingly. This phenomenon is reflected in curtailment rates, which express how much of total generation capacity had to be shut off or grounded to avoid frying the grid. The result: regional supply gluts ripe for Bitcoin miners to draw from, all without ruffling the feathers of what should be one of their natural predators, the government-sanctioned utility.

The difference between how our counterfactual and reality played out suggests that our understanding of Bitcoin is too forward-facing. We often picture Bitcoin as locked in an existential struggle with central banks, but the network managed to achieve unicorn status with little sovereign resistance. In understanding how Bitcoin passed a twelve-figure market capitalization, it makes more sense to think of central banks as the proverbial final boss, and to recognize that utilities have had far more opportunity to strangle this grand experiment in its cradle. We can see this empirically: governments worldwide have intervened against miners, whereas running a node or holding a wallet is only "outlawed" in a motley crew of jurisdictions (e.g. Algeria, Egypt, Morocco, Bolivia, Ecuador, and Nepal).

We are forced to accept the conclusion that the availability of cheap energy has played a role in the success of Bitcoin to date. The design of the network allowed for certain regions with excess energy to subsidize a global settlement platform without ever attracting the ire of any entity capable of torpedoing the whole experiment. As bureaucratic inefficiencies allowed miners to exploit these supply gluts in peace, network hashrate has grown to a point where now a peeved utility or government agency would struggle to marshal the resources necessary to attack the network. Indeed, network hashrate has grown ~100x since September 2013 and a multi-day 51% attack would now cost some billions of dollars. But what happens when these gluts are gluts no longer?

Curbing Curtailment

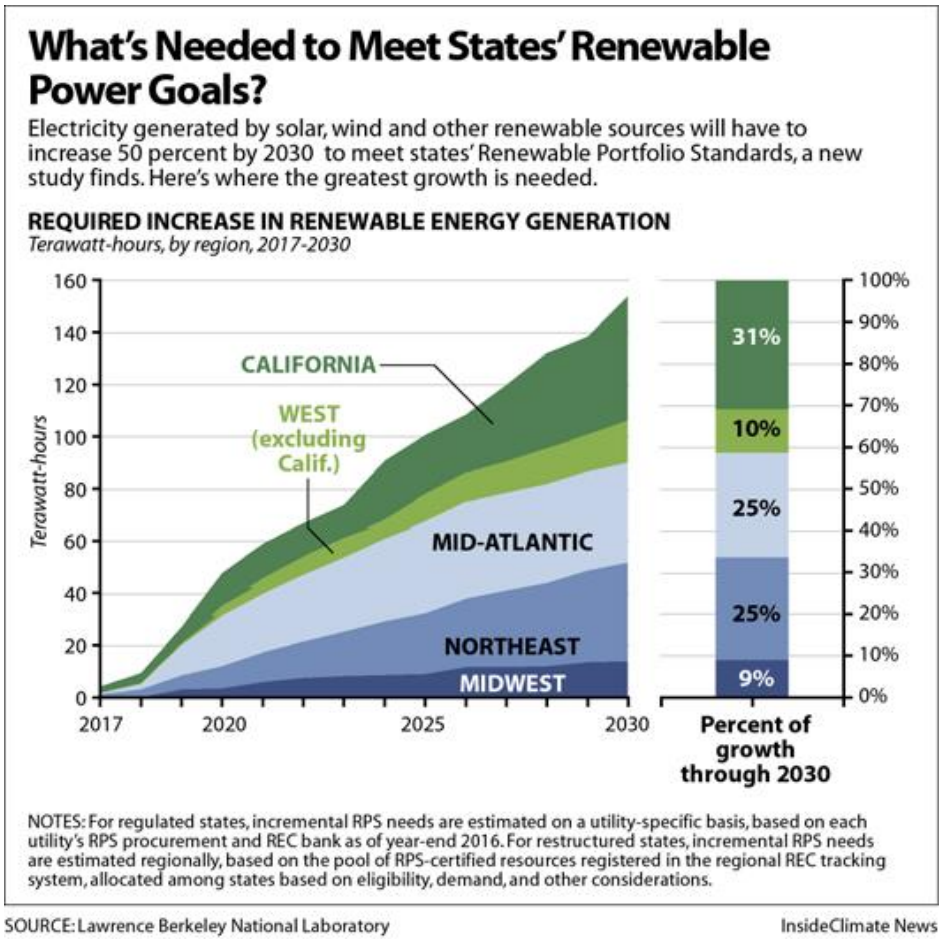
Renewable energy curtailment has served as the key tailwind behind the rise of Bitcoin. It occurs when an asset like a wind farm or a dam produces an excess amount of energy relative to demand at a given time, forcing the grid operator to reduce or divert output in order to preserve the integrity of the power system. In the regions that have attracted miners, we can chalk this excess up to geographic remoteness — areas like Sichuan, Inner Mongolia, and Alberta have low population densities relative to the sheer amount of power being generated. As a result, local energy prices remained depressed relative to the rest of country and miners can operate with little worry for utility throttling. Leading Bitcoin researchers harp on this phenomenon to argue that the future of mining will remain with "stranded" renewable energy assets, even more so than it has in the past:

- "Bitcoin miners are highly mobile and can therefore serve as cornerstone demand for low-cost stranded renewables."
- "It's the stressor that will force our archaic carbon-based energy system to adapt."
- "Bitcoin will spur innovation in the development of renewable energy technology & resources."

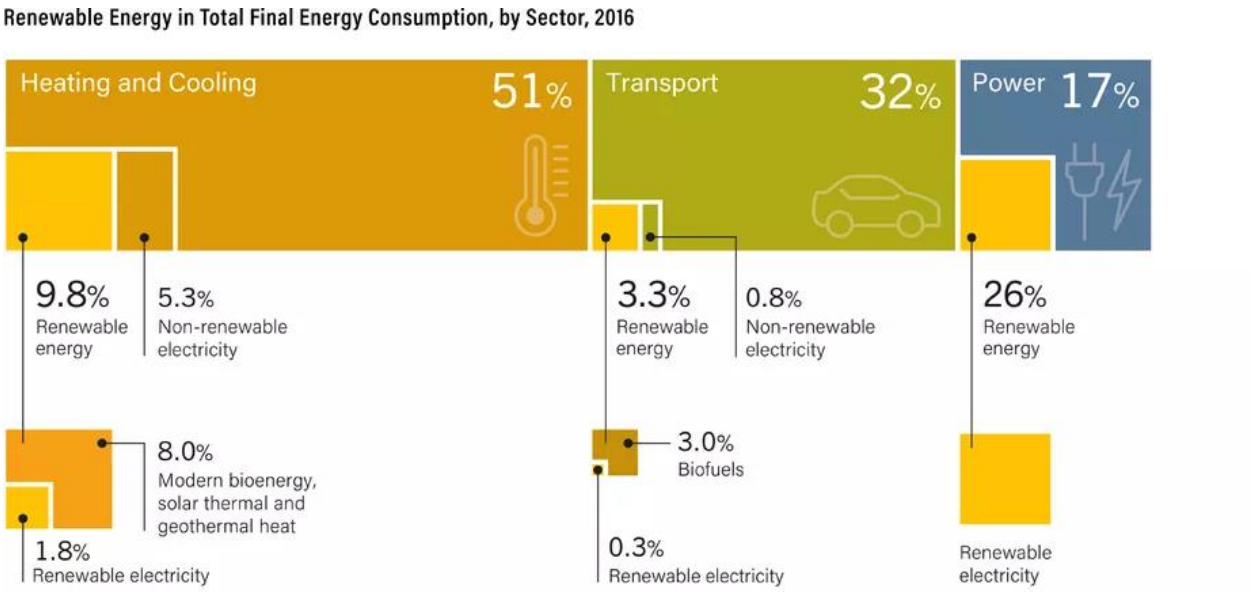
This sentiment, however, underestimates the technological progress being made on transmission and storage methods in response to the evolving demand profile for these renewable assets. It is an error to assume that curtailment is inherent to renewable energy; that governments and financiers would simply accept terawatt hours-worth of wasted renewable energy when climate change is their most pressing political issue. Indeed, for political and technical reasons, the availability of *marginal* renewable energy for mining will decrease over time, challenging the current model of private mining operations.

Parallel Political Pressures

Developed economies are staring down the double barrel of their millennial constituencies' chief demand: decarbonize and electrify as much energy consumption as possible. Whereas government intervention to date has focused on propping up renewable energy via subsidies and federal R&D, the next stage will require diminishing demand for fossil fuels. And while solar and wind are already out-competing carbon incumbents under certain conditions, outright bans or onerous taxation schemes on the latter will lead to massive increases in demand for the former. Take California, for instance: alone to have a 100% renewable energy-powered EV fleet by 2045 would require a 500% increase in current renewable generation capacity.



Whether driven by the Green New Deal in the US or the 13th Five Year Plan in China, the political zeitgeist of the coming decade is going to result in a scramble for renewable energy. In the immediate future, that will require tactical deployment of existing renewable assets — we're starting to see crackdowns on inefficient use already. And don't forget that current outlays for renewable energy R&D are not on par with prior decades', raising doubts about the feasibility of deep decarbonization past 2030. These realities are already setting in for traditional businesses: Daimler is discontinuing further internal combustion engine development, Stripe has committed to negative emissions, and so on. As more and more of the physical economy piles into renewable energy assets, miners looking to continue their curtailment arbitrage can expect to find themselves labeled as *persona non grata* sooner rather than later.

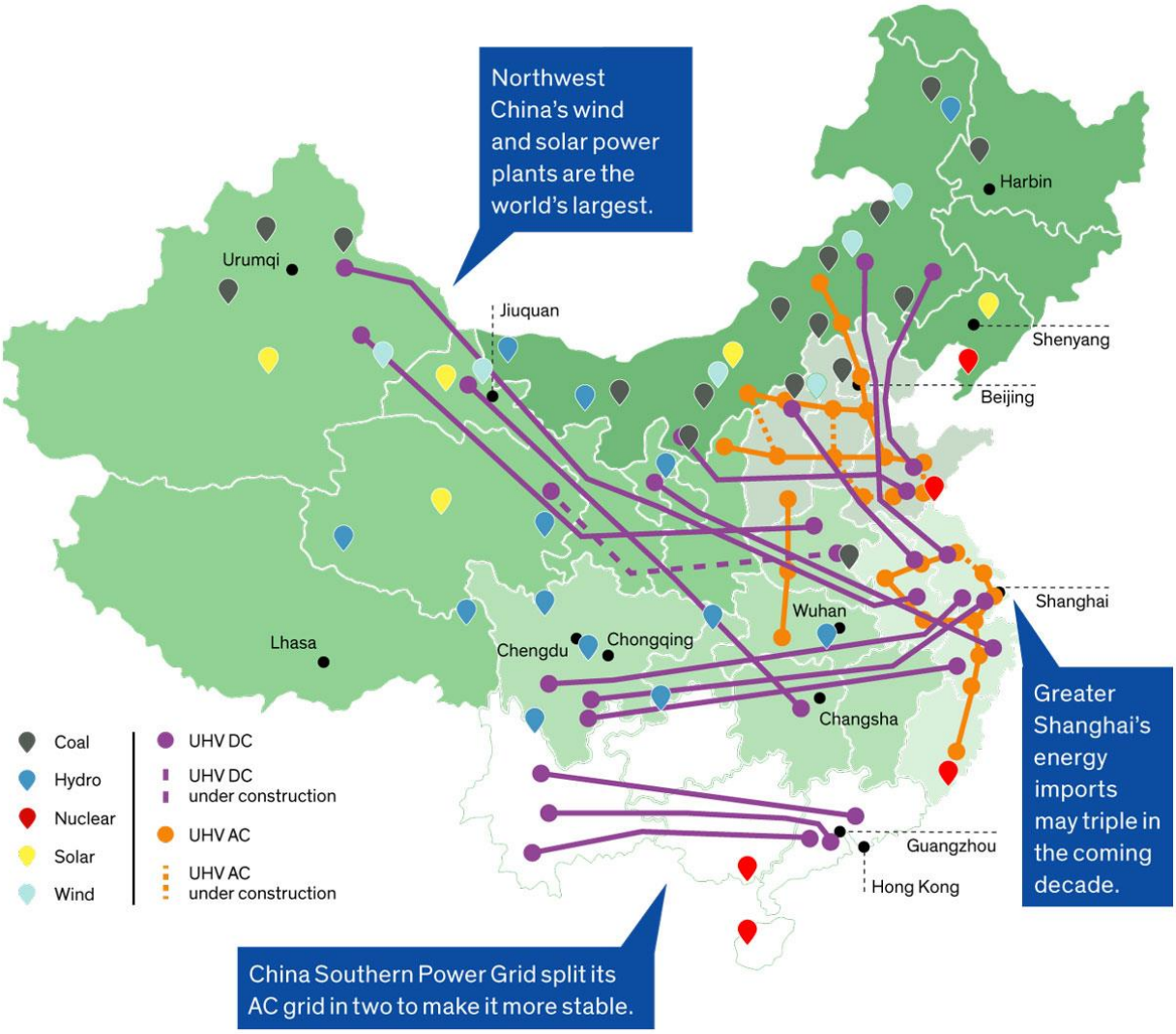


David Roberts, "The global transition to clean energy, explained in 12 charts", Vox

No Renewable Left Behind

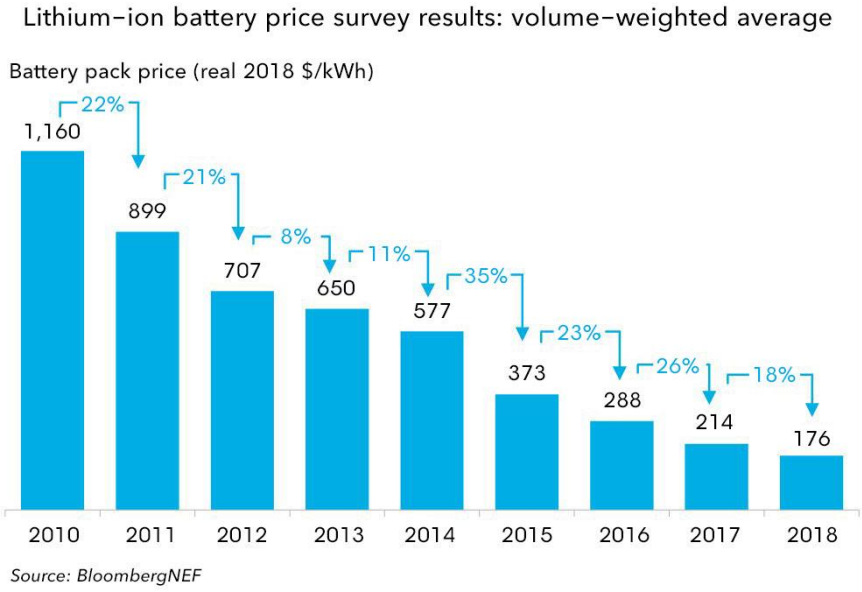
But are these political promises backed by actual solutions? The aforementioned Bitcoin analyses stress that geographically-stranded renewable assets, like the majority of the dams that power mining today, are beyond the reach of a realistic grid integration strategy. That may have been the case earlier in the decade, but the tide is turning. Technological progress on grid-level storage and ultra high voltage DC transmission, as well as organizational improvements on inter-regional coordination, promise to reduce curtailment rates and smooth out electricity costs. Most relevant to the miner status quo are:

Ultra-High Voltage Transmission: China has laid over 30,000 kilometers-worth of high voltage transmission lines, which allow for minimal energy loss over long distances, to date. The State Grid Corporation's deployment of a 1,100-kv (ultra-high voltage) line stretching over 3,000 km between Xinjiang and the greater Shanghai region in January of this year helped drop the region's wind curtailment over 15% year-on-year. While the State Grid has struggled to make full use of its world-leading transmission infrastructure in the past, top brass in Beijing is making it clear that regional grid squabbles will not sideline national goals. Given that China represents 60% of Bitcoin hashrate, projects like the Wudongde DC line between Yunnan and Hong Kong indicate how these efforts will raise electricity costs in key Bitcoin mining hubs.



*Erik Vrielink, "China's Ambitious Plan to Build the World's Largest Supergrid", _IEEE Spectrum_*

Grid-Level Storage: We find ourselves on the precipice of a golden age for, well, big batteries. The per-kWh cost for lithium-ion has dropped seven-fold since 2010 and is closing in on the $150/kWh target necessary for wind and solar to be competitive in 95% of US grid applications. With eight 100 MW-capacity storage projects going live by 2021 in the US alone, utilities appear intent on storage serving as their primary curtailment solution. And let us not forget alternative storage solutions: China has earmarked over 18 gigawatts-worth of new pumped storage hydropower by 2023, and long-term sulfur aqueous flow batteries could hit the market by 2025. Current grid storage solutions can already reduce curtailment by up to 38% and we should expect extensive deployment and further progression along the learning curve to result in even greater reduction rates.



Bitcoin miners have relied on the geographic arbitrage of renewable energy assets to power their operations. Because a watt of power generated among remote rapids was priced relative to local villagers' demand for it (i.e. non-existent), miners benefited from cheap rates and indifferent utilities. Miners will see this strategy fall to the wayside as long-distance transmission and short-term storage reprice remote renewable electricity in terms of the utility it offers to metropolitan areas in need of clean power. That is to say, grid operators' newfound ability to maximize the system-wide economic welfare of their respective networks will result in price normalization at the expense of higher-than-equilibrium rates in these formerly glutted areas. With less marginal electricity available, and it coming at a higher price, miners will need to find new competitive advantages to stay afloat.

Bitcoin Does Not Incentivize Renewable Energy

Before addressing the logical alternative energy strategy miners will pursue, let us dismiss the one they will not: building out renewable energy assets themselves.

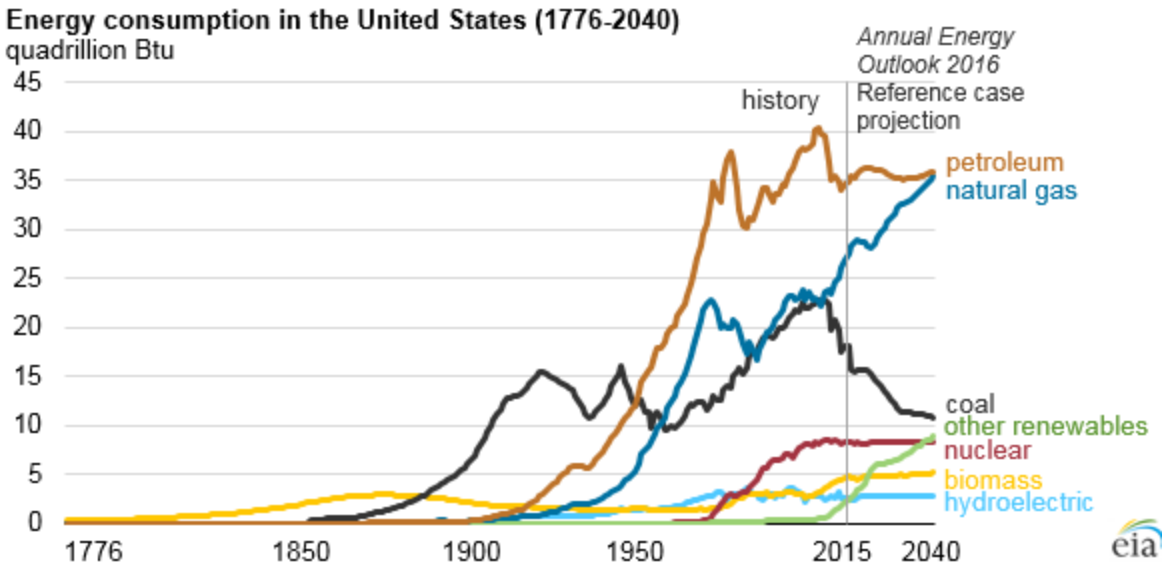
The issue undermining this argument is the lack of common ground between the three relevant stakeholders involved: municipalities, financiers, and the miners themselves. Because miners are effectively energy nomads, or "buyers of last resort," their preferred time horizon and tolerance for volatility fails to align with those of the former. They will pack up their things the moment local energy rates fail to provide a competitive edge, nor can they promise a predictable cash flow. For the multi-decade considerations of communities and infrastructure investors, these caveats reduce the idea of subsidizing new energy generation with mining to a nonstarter. Given miners' need for flexibility, any strategy that saddles them with the long-term obligations of greenfield development should be roundly discarded.

And in the case of existing renewable energy assets, cost-benefit analyses will tend to favor better grid integration over leasing mining equipment as a curtailment reduction strategy. Moreover, the second order effects of rerouting that renewable energy to denser regions present a compelling ROI on building

out transmission and storage infrastructure instead. Evidence from the US points to every kilowatt-hour of coal replaced saving $0.0436 in public health costs, as well as renewable energy infrastructure proving more resilient and creating more jobs relative to fossil fuel operations. For a grid operator tasked with promoting greater economic welfare within its region (read: all of them), the marginal return on integration far outweighs the benefits of any mining scheme.

To recap: countries are making it a priority to shift their energy consumption to renewable sources. Their voracious demand will result in a no-tolerance policy toward energy curtailment, and they will place an emphasis on grid-wide price levelization. This erases the electricity cost arbitrage miners have traditionally relied on for three-quarters of the Bitcoin hashrate, especially in Chinese hydropower hubs. **This combination of relatively elevated prices and low tolerance for non-essential consumption amounts to politically-manufactured energy scarcity that will force miners away from their traditional haunts**. Not wanting to anchor themselves with illiquid capital outlays, they will need to find existing energy sources they can repurpose at low cost and with minimal risk of utility intervention.

A Moment, Minsky?

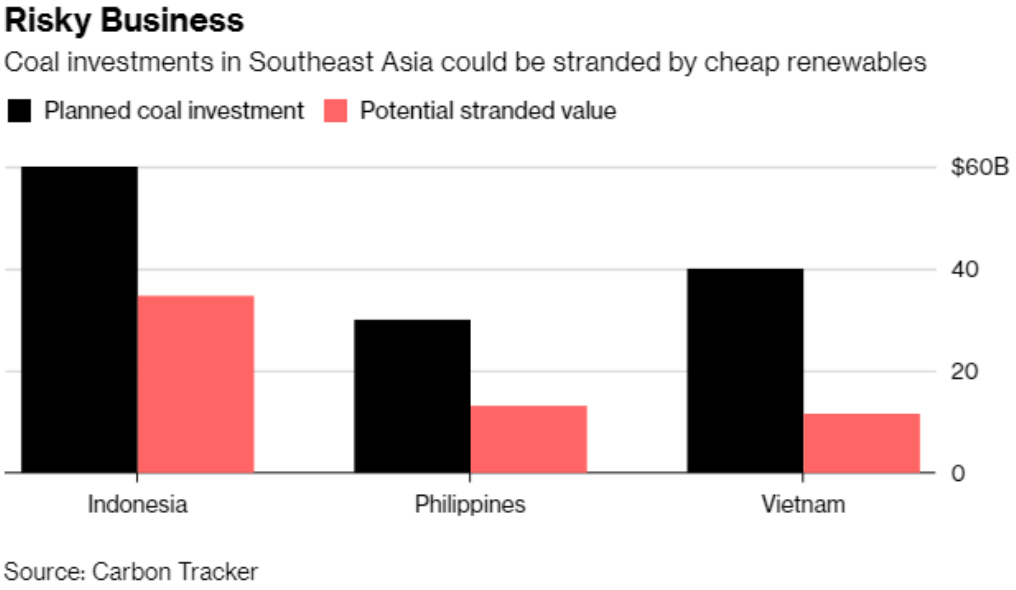


For these reasons, Bitcoin miners will have strong incentives to align their operations with fossil fuels. As more and more fossil fuel assets become stranded due to declining profitability upstream and a lack of demand downstream, miners will emerge as buyers of last resort in the impending fire sale. Their primary draw will lie in unfettered access to wholesale energy prices that fall outside of the purview of utilities. Compared to the free lunch that has been billions of dollars-worth of cheap hydropower, the $5 trillion in

potentially stranded fossil fuel assets represents a veritable 10-course meal, on the house.

Three key verticals offer the most compelling opportunities for miners:

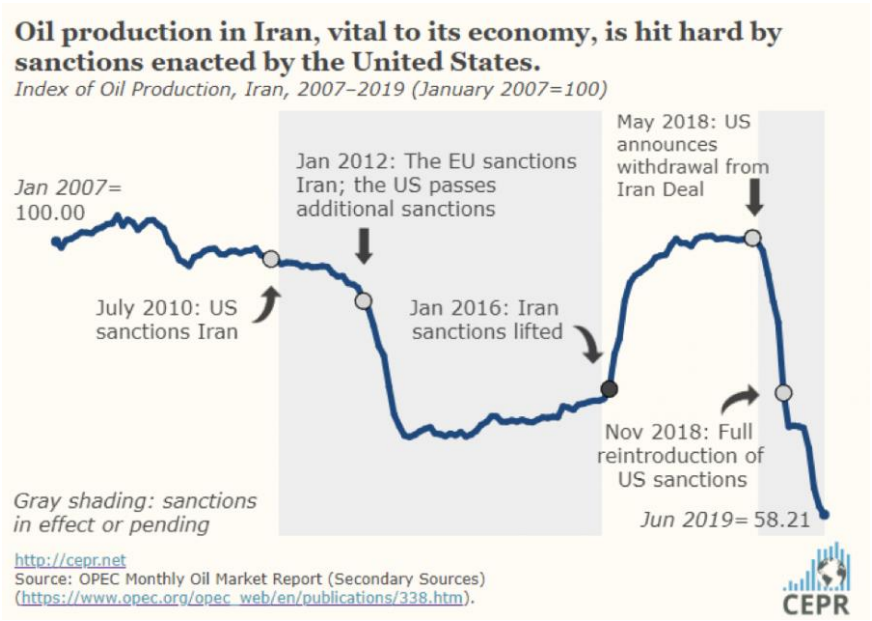
- **Coal in General:** Current estimates peg global coal plant capacity peaking in 2021, due largely in part to cratering capacity factors and vanishing investment. The power plants and mines left behind provide little utility, and repurposing efforts require hundreds of millions in new investment that few countries can afford. In regions where market forces shuttered the coal industry, miners stand to purchase their own power generation, complete with transportation infrastructure, for cents on the dollar.



Source: Carbon Tracker

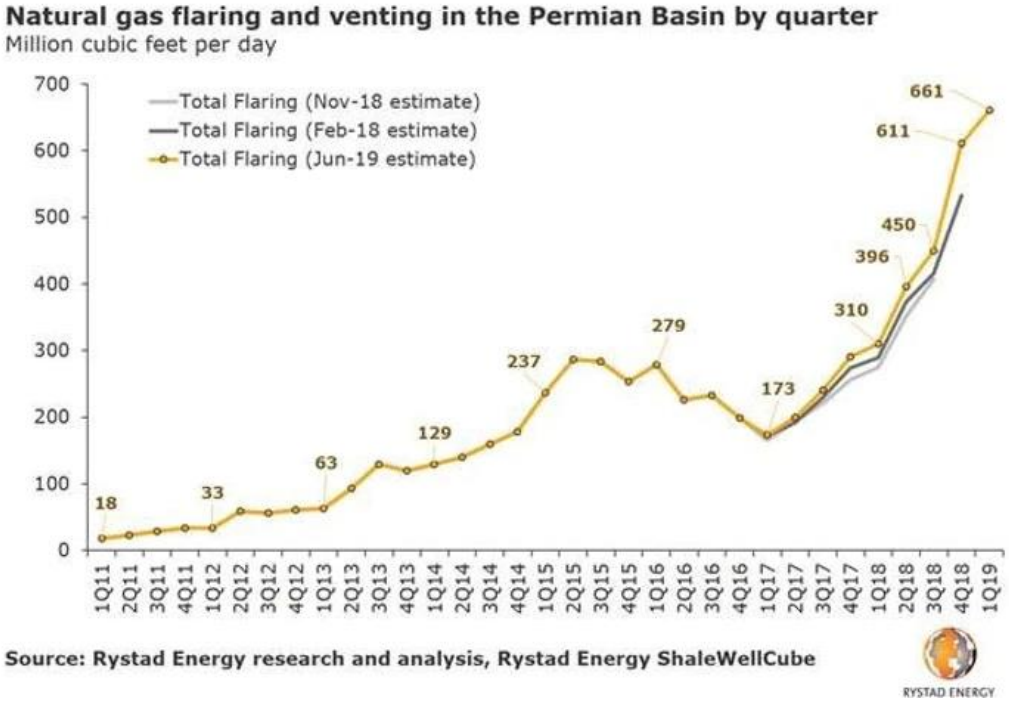
- **Natural Gas in the US:** American natural gas production has been on tear since 2005, growing total annual production by 50% since then and having turned the country into a net exporter in 2018. With close to eight decades-worth of recoverable resources left, the boom appears far from over. Plus, as continued tensions in the Middle East drive demand for American petroleum, the practice of natural gas flaring represents a curtailment-style opportunity for miners — the equivalent of 190 GWh was flared daily in Q1 2019 in the Permian Basin alone. Unsurprisingly, natural gas has sold at below-zero prices often in the past year.

- **Sanctioned Countries' Reserves:** Coinshares attributed the ~3% drop in the exposure of Bitcoin hashrate to renewable energy between its



November '18 and June '19 mining reports in part to Chinese miners moving to Iran. Couple that with the recent news that the Venezuelan central bank is considering to hold Bitcoin as a reserve asset, it is becoming apparent that mining offers a valid strategy for state actors looking to subvert American sanctions. With the value proposition of Bitcoin sitting at the intersection of finance and energy, it provides a silver bullet solution for countries that find themselves banned from exporting fossil fuels or trading in dollars.

Savvy miners are already recognizing this trend. Big Horn Datapower Holdings closed on a 107 MW coal plant in Hardin, Montana in March of this year; Bitmain has gone back and forth with Rockdale, Texas over the purchase of a former coal-powered Alcoa plant. Further phone conversations with local officials revealed miner interest in the opportunities of off-grid mining via coal and natural gas across Texas and North Dakota. Companies like Crusoe Energy Systems and Upstream Data have recognized the impending demand for these services, just as Bitfury has with its partnerships in the coal-rich northern regions of Kazakhstan. The prospect of



utility independence and wholesale rates make fossil fuels far more compelling than grid-restricted renewables, and varying policy stances on them will allow miners to continue their whack-a-mole game of geographic arbitrage.

But at what point should we expect to see this tipping point in the Bitcoin hashrate energy mix? For the penetration rate to drop further, from ~74% to <50%, would require ~1.25 GW of the current energy draw, or 10 TWh of annual consumption, to switch over to fossil fuels. To put that in perspective: 2 months of redirected flaring in the USA could accomplish that. Even something as banal as the imposition of renewable energy quotas across Chinese provinces next year could eventually tip the scales. So, Steve's point below presents a compelling argument.

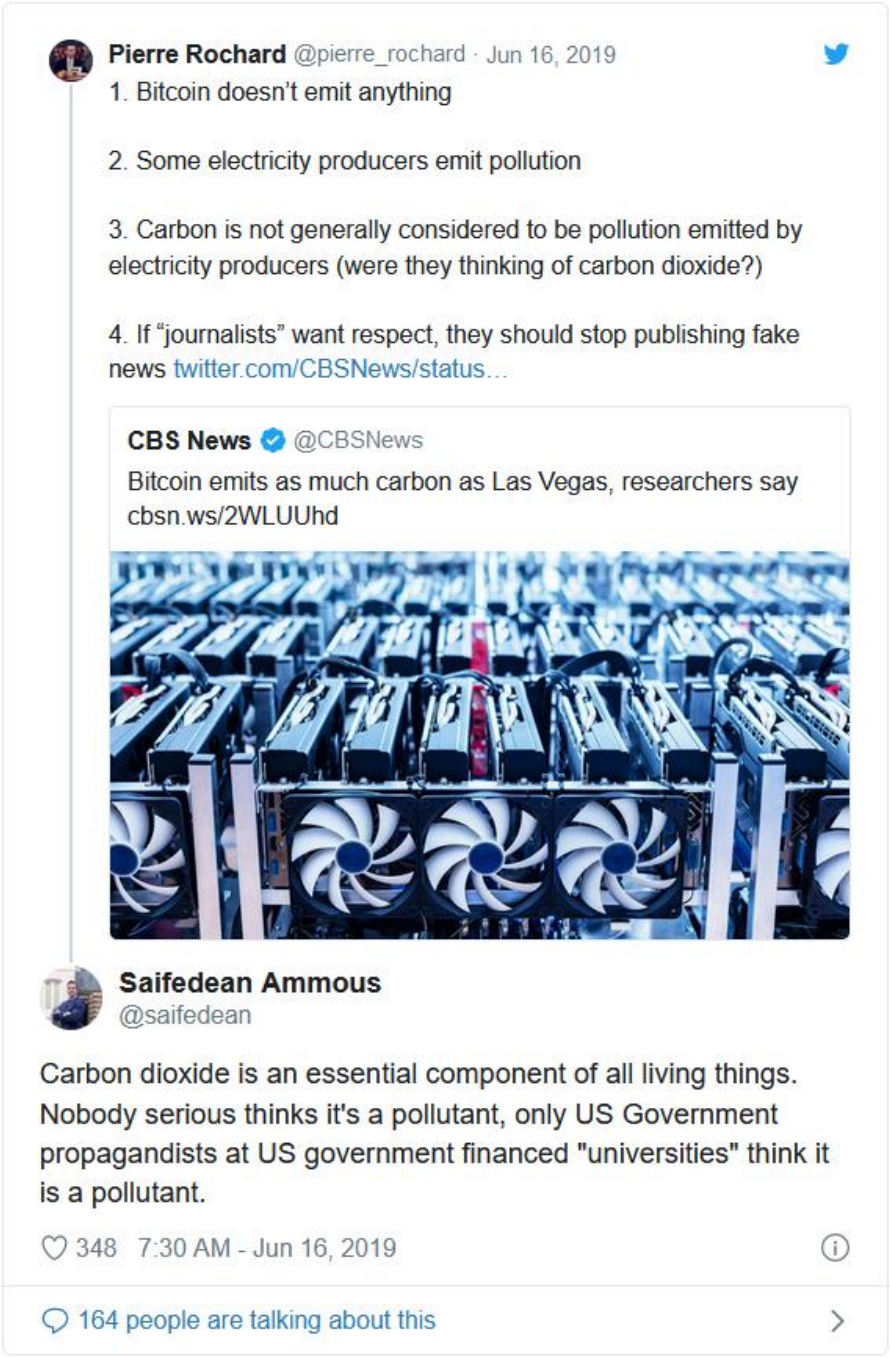
CEO of Upstream Data

The speed at which these developments will occur depends on a number of factors ranging from domestic Chinese policy to global geopolitical trends. Regardless, the writing is on the wall. Miners have spent the past six years profiting off of energy market inefficiencies, and they will continue to do so as fossil fuel prices fall through the floor. Analysts sell a false vision when they forecast that miners will enjoy bountiful renewable energy given that **a)** there is not enough for society's existing needs, **b)** miners have no incentive to invest long-term in new generation, and **c)** utilities represent a natural competitor.

Concluding Thoughts

The future of Bitcoin mining forces us to consider what tradeoffs we are willing to make for the continued growth of the network. Mining blocks in a world with mass Bitcoin adoption will require orders of magnitude more energy than present. There is nothing inherently immoral about that, but it does present a challenge in the pursuit of a multi-trillion dollar market capitalization. With societal demand for solar, wind, and hydropower pushing out miners, the remaining options — private operations running on fossil fuels or state-sponsored operations with colorful characters — all put geopolitics front and center.

Choose your adventure: register your addresses with the IRS and OFAC to avoid tainted coins from Belarusian, Venezuelan, or Iranian miners; or find a new exchange because EU politicians banned an asset powered by American natural gas and Kazakh coal. No matter your acceptance of climate change, sanctioned countries and fossil fuel actors extending their shelf lives with mining revenues will bring renewed scrutiny to the network.



Author of "The Bitcoin Standard"

Should the proverbial honey badger give a damn? We can look to the Blockstream Satellite for a helpful analogy. The satellite exists in recognition of the fact that the reliance of Bitcoin on the internet represents a political vulnerability when considering ISP censorship or sovereign digital autarky. Likewise, miners must take a more proactive approach in assessing not just the wholesale cost of the electricity they consume, but also the price of the political risk they take on when choosing an energy source. That might seem counterintuitive for those of us who have come to understand mining strategy purely through the lens of operating expenses. But with close to 90% of all bitcoins already mined, it would make sense for existing miners' electricity price sensitivity to decrease over time as their focus shifts from accumulating

to preserving their BTC-denominated wealth. And if that's the case, these coming energy market trends could very well be what sets off a medium-term transition from private mining (where cheap energy comes from fossil fuels) to state-partnered mining (where sustainable energy comes from on-grid renewable assets).

Special thanks to Ryan Gentry, Francis Corvino, Justin Leroux, Brandon Quittem, Owen Gwilliam, and Teddy Ogilvie-Thompson for their motivation and feedback over the course of researching and writing this piece.

Editor's Note: This article originally led by giving credit to Avalon specifically for launching the ASIC mining boom. This has since been revised to just refer to the boom itself, without crediting any specific ASIC manufacturer.

The Legend of Satoshi Nakamoto

By Erik Cason

Posted October 24, 2019

"*What does it matter who is speaking," someone said, "what matters is who is speaking*."

That's the entire point.

In the seventeenth and eighteenth centuries, a totally new concept was developed where scientific texts were accepted on their own merits and positioned within an **anonymous** and coherent conceptual system of established truths and methods of verification. Authentication no longer required reference to the individual who had produced them; the role of the author disappeared **as an index of truthfulness** and, where it remained as an inventor's name, it was merely to denote a specific theorem or proposition, a strange effect, a property, a body, a group of elements, or pathological syndrome. Michel Foucault, What is an Author? [bold mine]

The Spectre that Satoshi Nakamoto represents—a single human being intransigently choosing the protection of cryptography against a seemingly omnipotent global government machine hell-bent on controlling all wealth, information, and identity no matter what—is a far greater power than any money he created; but is the very legend that he and Bitcoin is. Through creating a character that we only know as this amorphous, pseudonymous, nonphysical 'person'–the idea that is Satoshi Nakamoto–and his great work that he introduced into the world–Bitcoin–Satoshi was really telling a much greater story about wealth, identity, and power in the arc of human history. When one reads all the details of this hidden story about a man and his passion for a new form of wealth that is beyond any temporal power; we discover the tale of cryptosovereignty and the extraordinary individual power that is cryptography, and Bitcoin in this world.

As time builds between Satoshi's last appearance in our world and the inoperetivity that is his task of Bitcoin; so too will the legend of who he is, and the ramification of what he has done. And as this legend grows and becomes known by all of humankind, it will transmogrify beyond just a legend and into the fabric of history itself. As the very foundation of fiat money and panoptic surveillance comes to tremble before the name Satoshi Nakamoto, the reality of his task will be too palpable for anyone to deny.

With each ludicrous attempt to identify Satoshi, as we saw with Dorian, or the fraudulent, lying, despicable sack of shit that is CSW, or any of those other fuck-

ups who have tried to claim to be him; the legend of Satoshi will only grow stronger. Now only a cryptographic signature from the genesis block will suffice to verify that Satoshi is who he is. Anything short of that will always leave space for it to be questioned, for Satoshi to remain hidden. I believe in all of his brilliance and glory Satoshi threw those private keys into the abyss, sealing his fate as the author of the greatest work of art that has ever been created; while dooming his project to the final, inevitable conclusion that it and the world must come to.

For the deepest truth of what Satoshi had to teach us was 'what does it matter who is speaking, someone said, what matters is who is speaking.'

Through the glory, grace, and dignity of whoever Satoshi Nakamoto may be, the one thing that is for certain is they are of the greatest character and class of any human that there has been. And it is not for the achievement that is Bitcoin, the extraordinary power that is unlocking this new epoch, nor even for the monumental amount of exogenesis wealth it will create; but for his very human choice to walk away.

Through this action alone Satoshi may very well pass himself from being just a legend to something so much more extraordinary and audacious:

Hope.

Real hope.

For something new. For something different. For something fair.

By refusing to reveal who he is, refusing to expose his wealth, and by making the final decision to remain as only the author of Bitcoin, and nothing more; he has moved himself from the human realm into that of the Elysium itself.

By maintaining his image as a Being that is beyond this place of wrath and tears, past the gridding and guilt that is now our very physical faces and existence, and past the shame and injustice that is the history of all fiat money; Satoshi's work has opened the narrow path from which we can escape the camps of modren life. Just as in the darkest of nights does the smallest of lights shine the brightest, so too does Bitcoin present itself here on this earth today.

The creation of Bitcoin was a task chosen for only him/them/it alone, and the role was played perfectly to the task. Whoever Satoshi Nakamoto may be, they are clearly the greatest hero of the 21st century, and quite possibility even the great liberator of humanity itself. Only time will tell how great and how vast the legend of Satoshi Nakamoto will grow to be, and how glorious his project of Bitcoin will become; but one thing is for certain and that is this:

Satoshi has given us hope.

By refusing the greatest sum of money that any person has ever created, by keeping his face concealed and beyond the power of any state or person to identify, and by choosing to walk away from one of the most extraordinary project that humanity has ever known; Satoshi has proven his imperium and sovereignty through cryptography. Through his being as an author alone, he has displayed the power that any of us can have access to when we choose to use the power of cryptography to protect ourselves, and the promise that will always entail. Through his task of Bitcoin and the Good News that it is, he has given each one of us the gift for to choose for ourselves what the real meaning of value, wealth, and law is.

In this final action of walking away, and taking his death upon himself, Satoshi closed the Gate of Law as his final move and checkmate to forbid any state from interloping in our land, and allow us an opportunity to abscond back to the country from which we came so we may be free once again.

Epilogue: It is said that after Satoshi stopped working on Bitcoin that he found a job as a scrivener lost somewhere down on Wall Street. Today he still sits there, as Bartleby once did, confounding financiers, economist, lawyers, and all sorts of reasonable men alike with his intransigency, and decision to refuse to go along with anything. It is said that he was a most unreasonable man and his only response to any question was:

“I would prefer not to.”

All 21 Million Bitcoin Already Exist

By Phil Geiger

Posted October 25, 2019

“Every piece of money is owned by one of the members of the market economy. The transfer of money from the control of one actor into that of another is temporally immediate and continuous.” -Ludwig Von Mises, Human Action

To celebrate the 600,000th bitcoin block, which has unlocked the 18 millionth bitcoin, and in an effort to become increasingly fun to be around at parties, I’m writing this exploration of the idea that all 21 million bitcoin already exist. This may seem like a semantic or esoteric argument, but bitcoin is truly a different beast, which requires closely evaluating the assumptions we make and the language we use when describing it. By more clearly defining bitcoin and how it functions, we can speak more accurately about its monetization process, which ultimately will help HODLers spread the word to our precoiner friends and family. We are alive for, and witnessing, the greatest event in the history of economics – the rapid monetization of a scarce, apolitical, global currency. Providing our communities with an early competitive edge could have positive long-term implications if bitcoin survives.

Misnomers already run rampant in bitcoin, such as the terms wallets, addresses, and mining. A bitcoin wallet is more closely related to a key ring, or a public and private key generation/coordination factory. Bitcoin addresses aren’t really locations that we want users to repeatedly visit, unlike physical addresses or email addresses. Mining is a similarly incorrect term. This is where I believe much of the confusion arises when evaluating bitcoin, and is where much of the FUD surrounding bitcoin focuses time and energy because it’s easy to misrepresent and is extremely confusing to newcomers.

There are a few questions and assumptions that we will need to explore in order to understand whether all 21 million bitcoin already exist. Is it possible for a computer program to HODL BTC? What are the different inputs required to make a bitcoin transaction? Why would people choose one transaction method vs another? When did all 21 million bitcoin exist? What’s the difference between the available vs unavailable supply? First, we need to understand what is unique about bitcoin’s supply compared to the supply of another “hard currency.” Let’s start by comparing bitcoin to another monetary good: gold.

Bitcoin's supply vs gold's supply

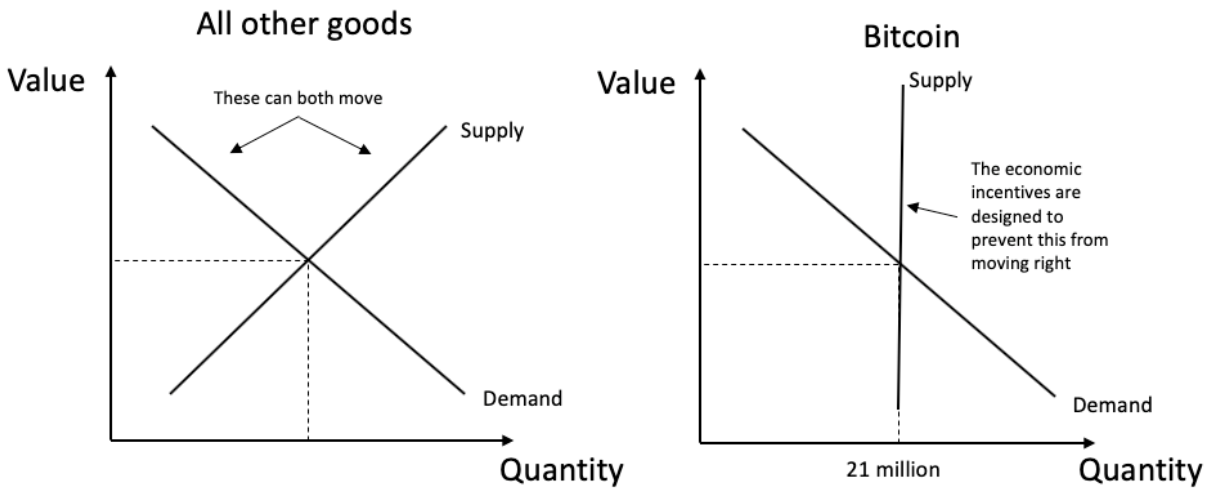
It's most accurate for us to say, based on what we currently understand about physics and the elements, a majority of the supply of gold (AU) in the universe already exists, with nuclear fusion producing some additional supply over time.

The crucial difference between the supply of gold and bitcoin ultimately comes down to what people are capable of knowing about the supply. Due to the expansion of the universe and the universal speed limit, *lightspeed*, humans have no way of estimating the total supply of gold, since its location is unknown and it's likely that a majority of the supply is very far away.

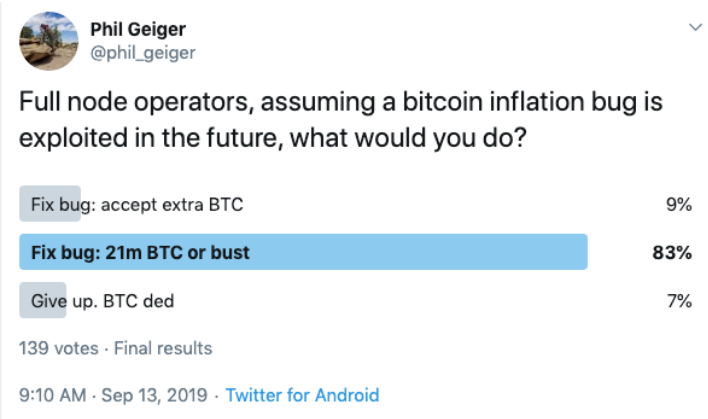
On the other hand, we have extremely strong social and technical consensus surrounding bitcoin's total supply, as well as the exact current location of the locked supply. In fact, we have more information about the BTC stored in upcoming blocks than we do about the currently unlocked supply stored in the blockchain. We know exactly how many BTC will move as a function of the coinbase transaction of discovered blocks, yet we have no way of knowing if a person currently holding, say a million bitcoin, is going to broadcast a transaction in a given moment to convert all of their BTC to another currency.

Bitcoin are unlocked on a set supply schedule that auto-corrects itself via a difficulty adjustment every 2016 blocks in order to maintain the schedule. This allows us to know with extremely high levels of certainty exactly where the currently locked 3 million bitcoin live (block number), and with slightly less, although still extremely precise knowledge about when they will be available for spending by private key (on average every 10 minutes). The difficulty adjustment is the feature that harnesses individual incentives to perpetuate bitcoin's own growth. By aligning difficulty to network size, it thwarts people's effort to create more supply and instead uses their effort to increase security of the network.

Theoretically, we can know where all of the gold on Earth is located, but we have no way of knowing precisely when we can get to it, the cost to extract it, or precisely how much gold exists beyond Earth. As such, we can make the assumption that if gold ever becomes valuable enough, we can and will find a way to uncover more of it for use, either by mining on-planet or off-planet, or by harnessing nuclear fusion to create more. This is the nature of supply and demand. If demand for any good or service becomes high enough, it increases the incentives for people to go out and produce more supply.



The bitcoin network itself is its 21 million supply. The supply is a vertical line in the supply and demand model, meaning it's completely inelastic. This limit is written into the code that all full node operators choose to run, and more importantly, it's the limit we all agree to when we purchase our first bitcoin – it has nearly unanimous social consensus. In bitcoin's history, there have already been multiple technical inflation bugs discovered, and one inflation bug exploited, but the network ultimately viewed those transactions as an invalid minority hard fork and maintained the socially understood supply schedule, even though it required node operators to run patched software. It's reasonable to expect we will see more software bugs like this in the future, and once again the network will have to rely on social consensus. Luckily, the network's incentives are all designed around socially and technically maintaining this 21 million limit.



Full node operators are pretty convicted about the 21 million limit. The outcome of this poll would be bitcoin competing with a minority coin, obviously to be named "Bitcoin Inflation"

With gold, there is no way for a technical or social consensus to manage supply. There is only the element AU, and there is no way to know when and how it will be mined and accessible for human use with any reasonable amount of precision. In gold's case, we can use supply based predictive models to measure the future supply. We can't know how much gold exists in the universe, only that it's difficult to mine additional supply here on Earth. We can model how

quickly we expect the supply of gold to inflate, assuming demand remains relatively steady.

So, then what is bitcoin mining?

In bitcoin, there are two ways that **people** are allowed to transact. The first way is what the majority knows and loves, private key authentication. If a person holds a private key associated with a funded address on the blockchain, they are able to move the funds by publicly broadcasting a signature from the private key and including a fee to incentivize the network to purchase electricity and process the transaction. In order to obtain the funded address in the first place, someone somewhere must have expended productive energy to obtain the BTC. The second way that people can transact bitcoin is by selling electricity, in the form of SHA-256 hashes, to the network – what we colloquially (and incorrectly) label as "mining." By converting the cheapest electricity into as many SHA-256 hashes as possible, these bitcoiners are ordering and proposing batches of pending transactions by finding the valid SHA-256 hash of the block at the current difficulty level. If their ASICs are able to find the solution before others and their proposed blocks are validated by the full nodes according to the rules, "miners" can move the block's coinbase transaction, often referred to as the miner reward, and the block's transaction fees to any address they'd like. Do "miners" create new supply in this scenario, or just transact known coinbase transactions and transaction fees by spending electricity in the form of SHA-256 hashes?

We're pretty split on this. 52% believe miners create supply in some form, 48% believe they do not create supply. There's a good chance this poll was worded poorly...

It's a subtle yet important difference that, in my opinion, allows us to say authoritatively that only 21 million bitcoin can possibly exist. The question is (somewhat of) an individual decision that each full node operator and HODLer needs to make. Node operators individually do not get to define what is or isn't bitcoin, they can only validate whether a bitcoin is a bitcoin, and they individually are either in consensus or out of consensus. That said, when we reach block 630,000 at the next halvening, will your full node accept 12.5 BTC, or will you accept only 6.25? My node will reject *any* future block that attempts to spend a coinbase transaction that doesn't follow the

supply schedule written in the code my node follows, because this would be an invalid transaction according to the social and technical consensus that I opted into. Through a distributed network of individuals making personal decisions like this, the market ultimately decides what is valid bitcoin, and the market has to date, objectively set bitcoin's limit to 21 million.

If a computer hashes alone in the woods, does anyone care?

Converting electricity into SHA-256 (or any other algorithm) hashes is an inherently unproductive activity unless it is in the service of something valuable. Converting electricity into hashes for the bitcoin network is productive and profitable because bitcoin holders value using electricity to secure the network, as long as the "miners" abide by the rules of a consensus of HODLers and full node operators.

For individuals interested in selling hashed electricity to the network for the opportunity to transact coinbase funds and transaction fees (mining), there are only a few rules that are absolutely fixed. The most important rule is that there are only 21 million bitcoin. The next rule is that the number of coinbase transaction BTC started at 50 BTC in 2009 and decreases every 210,000 blocks until all 21m BTC can be spent by private keys, in 2140. After that, the hashed electricity purchases the ability to transact only the "transaction fees" paid by users broadcasting private key initiated transactions.

Luckily for "miners," the difficulty adjustment by design always ensures that it is profitable for someone to sell efficiently hashed electricity to the network. If a given miner is unprofitable long-term, they must make the decision to either shut down their business (and possibly sell their hardware on a secondary market), or to find a cheaper source of electricity. If enough "miners" are unprofitable and shut down their ASICs, causing the network hashrate to drop and blocks to be found on average longer than 10 minutes, the difficulty adjustment recalibrates itself to the new lower hashrate to ensure that the supply schedule average is maintained. As a result, the bitcoin network adjusts itself to always pay market price for electricity converted to hashes depending on the value of the network. If a given "miner" is unprofitable when selling electricity to the bitcoin network, it simply means that they are being outcompeted by other, more efficient "miners." Given these absolutely rigid network rules, savvy "miners" will quickly recognize that if they can get their electricity costs close to zero, maybe by **producing** electricity cheaply and choosing whether to sell it for other uses or as hashes to the BTC network, they can effectively sell hashed electricity to the network profitably forever.

It's the value of the currency, not the number of units

"It must be pointed out that the level of the total stock of money and of the value of the money unit are matters of complete indifference as far as the

utility obtained from the use of the money is concerned. Society is always in enjoyment of the maximum utility obtainable from the use of money. Half of the money at the disposal of the community would yield the same utility as the whole stock, even if the variation in the value of the monetary unit was not proportioned to the variation in the stock of money." -Ludwig Von Mises, The Theory of Money and Credit

After Satoshi found the genesis block and Hal Finney and friends agreed to participate in the network according to the rules set forth in the code and, more importantly, the social consensus, all 21 million bitcoin instantly popped into existence in a "Big Bang" moment. Each early user that converted electricity to hashes to transact early coinbase transactions received private key access to a large number of (at the time valueless) bitcoin as well as the understanding of the rules that future HODLers and "miners" can transact the locked supply of bitcoin by submitting electricity as hashes to compete and solve for blocks of transactions.

In this way, we can look at the **value** of the locked bitcoin as though it is distributed and held equally by every participant in the network. This **value** is paid by the HODLers to "miners" for submitting hashed electricity to the network at the market rate, measured by the value of the network it's spent to protect. In 2009, the bitcoin network was worth very little to just a few people, so the electricity cost to transact 50 BTC of coinbase funds was extremely low. Today, earning the ability to transact 12.5 BTC is worth spending around 100 exahashes of electricity per second.

Everyone who joins the network in any capacity should recognize that roughly 14% (3m/21m) of the **value** they are purchasing as of October 2019 is held by all participants in the network equally, only to be transacted by individuals submitting valid PoW to order and secure transactions. This has all gone according to the set supply schedule since day 1 of bitcoin, and nothing changes about the economic incentives of selling hashed electricity to the network in the future. The difficulty adjustment, by design, ensures that it is always profitable for the most efficient energy producers to sell their cheapest electricity to the bitcoin network.

It has been posited that machines and software can hold and transact with private keys. I'm positing that we have nearly 11 years of empirical evidence that the network itself has been holding and transacting bitcoin, but instead of with private key signatures, it's in exchange for hashed electricity.

It's not the number of BTC that one party or another holds that matters. It's the value of the overall network that matters, and the value of the network can only grow by understanding that its monetary properties are sound. There are only 21 million bitcoin.

All or nothing

Bitcoin's innovation is absolute scarcity accessible in a way that is borderless, neutral, and permissionless. This innovation is shockingly disruptive to all facets of human interaction, and it's this innovation that drives the increase in the value of the network over time. Bitcoin is its 21 million limit. At no time can its supply be anything other than 21 million, because that would go against what we currently know and understand about how the network functions, and would unsolve the problem of "digital scarcity."

Bitcoin was able to achieve absolute scarcity by its network architecture, which is designed to increase in decentralization over time and to actively reject the human desire to produce more supply of a highly demanded good. Increasing decentralization over time effectively crowdsources the decision of bitcoin's total supply to the entire network of participants, with the basic assumption that a decentralized network of individuals will not choose to debase their own currency, when each participant does not have access to seigniorage opportunities.

As a result, the prudent full node operator, "miner," and HODLer can all act under the assumption that the 21 million limit is non-negotiable. The knowledge of this disruption in scarcity is slowly surfacing organically via the free market and through the network of "HODLers of Last Resort," but this whole experiment depends on the ossified foundation of 21 million with clear, neutral, and unchangeable rules about how people are able to transact.

Because we voluntarily opted into this network, we can say that all 21 million bitcoin already exist today, since the rules the network consensus follows dictate that the supply schedule must be upheld. The only difference between the accessible/inaccessible supply is who or what currently HODLs the value of the coinbase bitcoin, and how humans must compete to transact with either the bitcoin tracked by the blockchain or the bitcoin tracked by the block number behind PoW and the difficulty adjustment.

Digital scarcity is a pretty strange idea. The bitcoin tracked by the blockchain are ultimately just ones and zeros and mathematical functions supported by economic incentives. The same holds true for the coinbase transaction coins. The schedule is written into the software we run, and there can't be a scenario where an upcoming block contains a different numerical value of coinbase coins because the social and technical consensus does not view that as bitcoin.

Bitcoin is the intersection between code and social consensus. Either all 21 million already exist, or none of them exist. There is no middle ground.

Views presented are expressly my own and not those of Unchained Capital or my colleagues. Thanks to Parker Lewis, Nolan Johnson, and Michael Goldstein for reviewing and for providing valuable feedback.

Tweetstorm: The Matrix

By Meltem Demirors

Posted October 25, 2019

1/ a thread on bitcoin and the Matrix

if “the matrix” is a metaphor for the system we live in, bitcoin is the red pill - a way for us to break free of a dystopian future characterized by tyranny, surveillance, and digital violence

or is it?

(slides https://speakerdeck.com/meltdem/blue-pill-the-two-faces-of-bitcoin)

2/ everyone knows this legendary scene

“this is your last chance... there is no turning back. you take the blue pill - the story ends, you wake up in your bed. you take the red pill - you stay in Wonderland and I show you how deep the rabbit-hole goes.”

3/ we’re living in an interesting time. i believe bitcoin is a social, political, and economic movement wrapped up as technology.

bitcoin is inherently anti status quo. it is inherently a challenge to the system we live in.

this makes it feel like the “red pill”

4/ instead of asking us to trust institutions, bitcoin encourages us to verify, not trust, a new system - the bitcoin protocol (code) and network (computation)

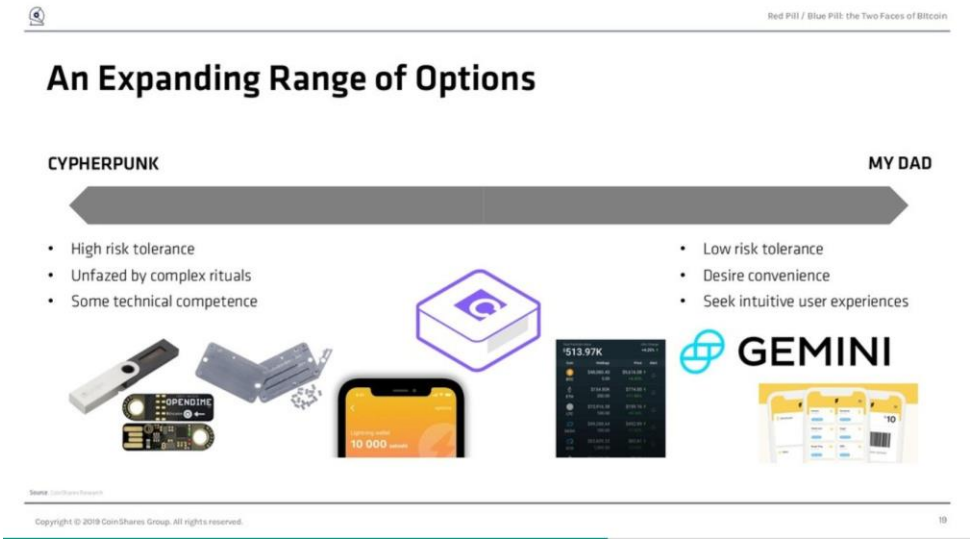
this awesome piece from @cryptograffiti captures this spirit well

5/ this makes bitcoin a very unique phenomenon. @eiaine captures this brilliantly - instead of aggregating and hiding risk like banks and institutions, bitcoin asks us, the user, to understand and take risk ourselves.

this is a massive shift - and a really tough one...

6/ today's bitcoin products and platforms present users with a wide range of options depending on the level of risk the user feels comfortable with.

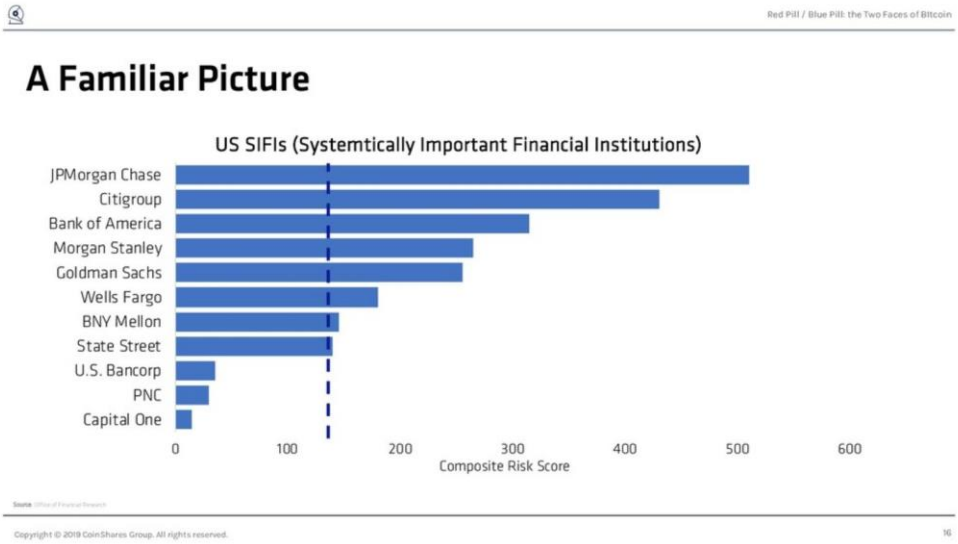
the options of the right end of the spectrum may make us "feel" safe, but they actually create more risk



7/ quick detour: following the financial crisis, we created a new designation called a SIFI (systemically important financial institution) for banks.

what makes a bank a SIFI? size, leverage, and total debt outstanding.

if these fail, the system fails.



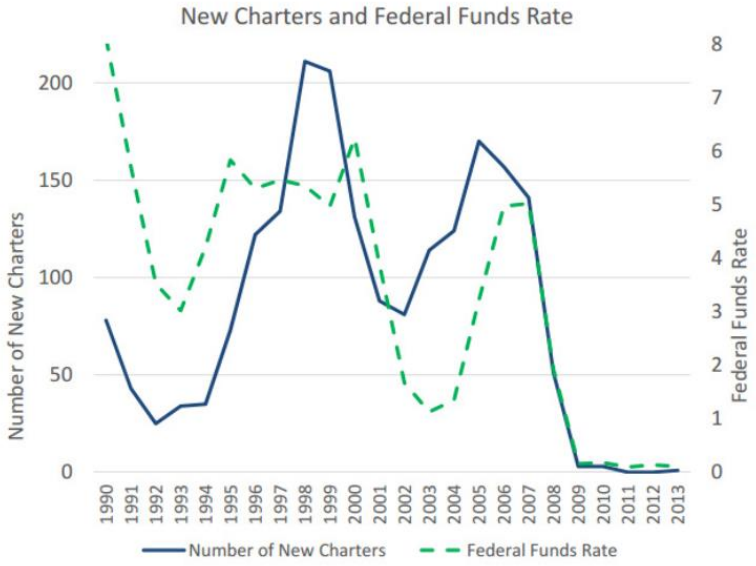
8/ the result?

today, the “Big Four” retail banks in the United States collectively hold 45% of all customer bank deposits ($4.6 trillion)

no new banks have been created in years.

risk has been aggregated and consolidated.

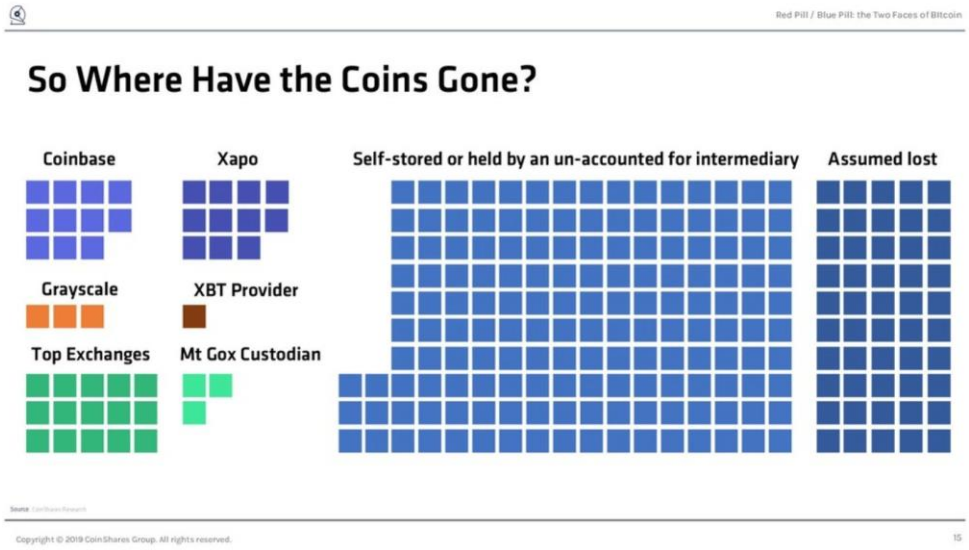
more risk following the crisis than before.



9/ bitcoin is headed in a similar direction. we are building institutions that will become too big to fail.

look at the merger of @coinbase and @xapo - the same consolidation happening in bitcoin.

(source data here - please comment / share your updates: https://docs.google.com/spreadsheets/d/1hClHhQlCXXzQY0IAyRZhYmIPW5AUlPWygA8GILsoWRU/edit?usp=sharing)

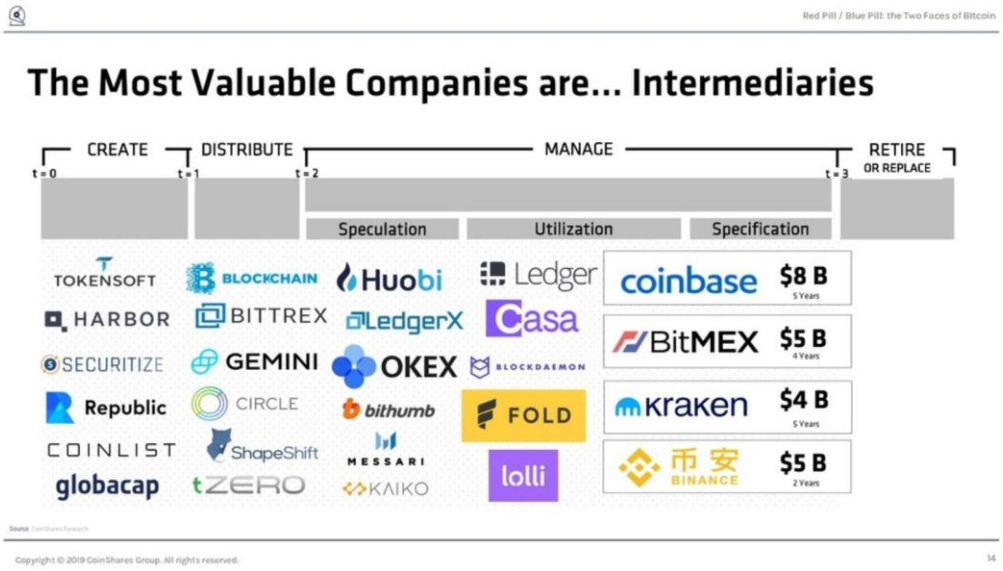


10/ it's no surprise that the most valuable companies in our industry are the intermediaries.

the ones who hold all the coins.

the ones building banks.

the ones aggregating risk.



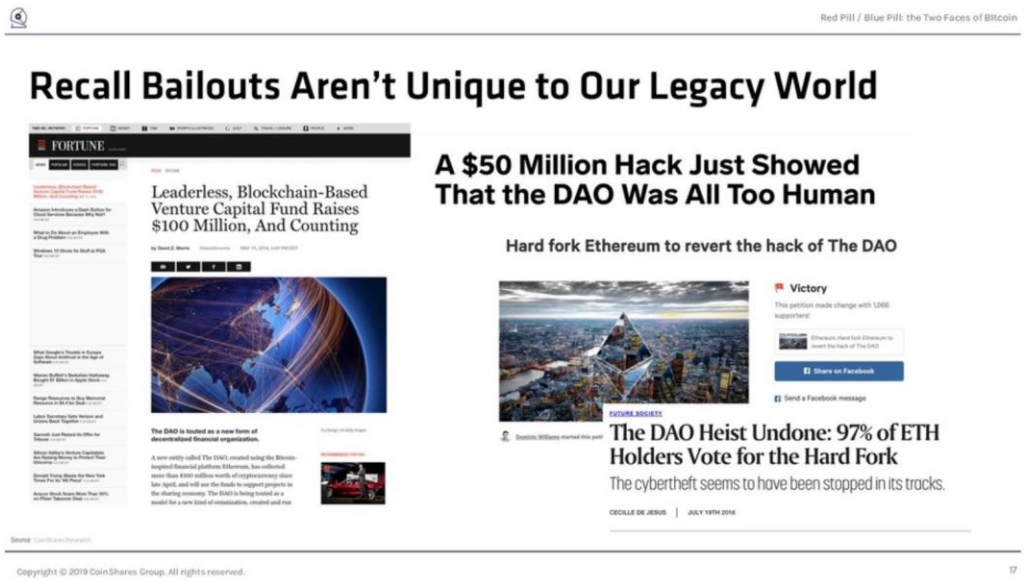
11/ and what happens when you put all your coins in one place?

just like we bailed out the banks in 2008, crypto is no exception.

how big does the loss have to be for us to bail out bitcoin?

1%? 5%? 10%?

for the ethereum community, it was 15%. bitcoin isn't immune.



12/ so here's the blue pill.

we're not building bitcoin. we're watering down bitcoin's promises and selling "blockchain."

and it's bullshit.

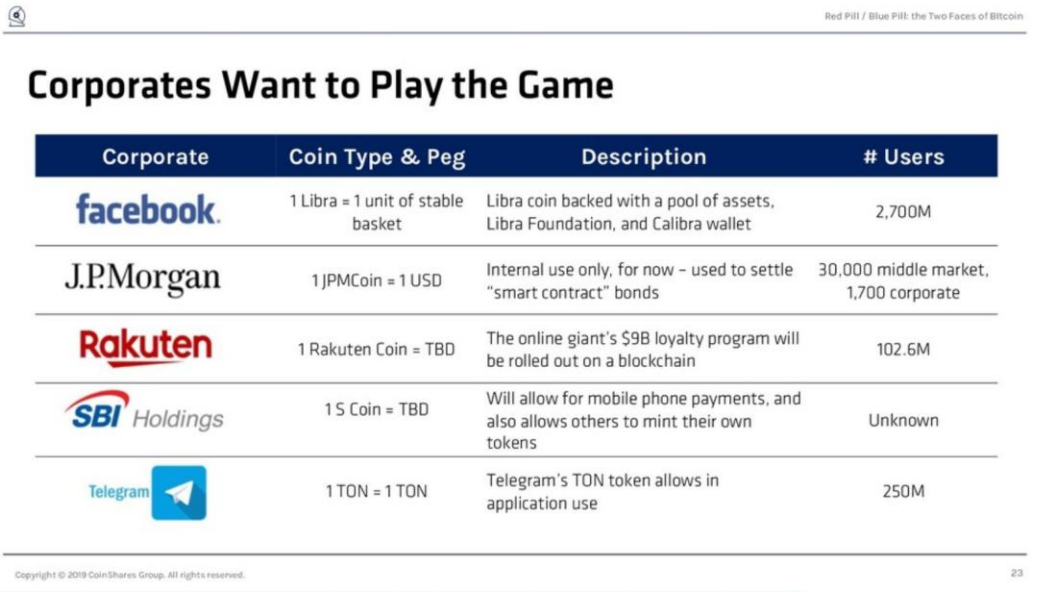
13/ ideas evolve...

the evolution of bitcoin into progressively less principled ideas shows how each successive wave of "innovation" further waters down the thing that made bitcoin valuable to begin with.

each successive idea is "less bitcoin" "more bank" than the idea before.

14/ now corporations want to play. including the world's largest bank (and largest SIFI). and the world's largest social media company. it's only a matter of time.

why peddle services when you can control money?

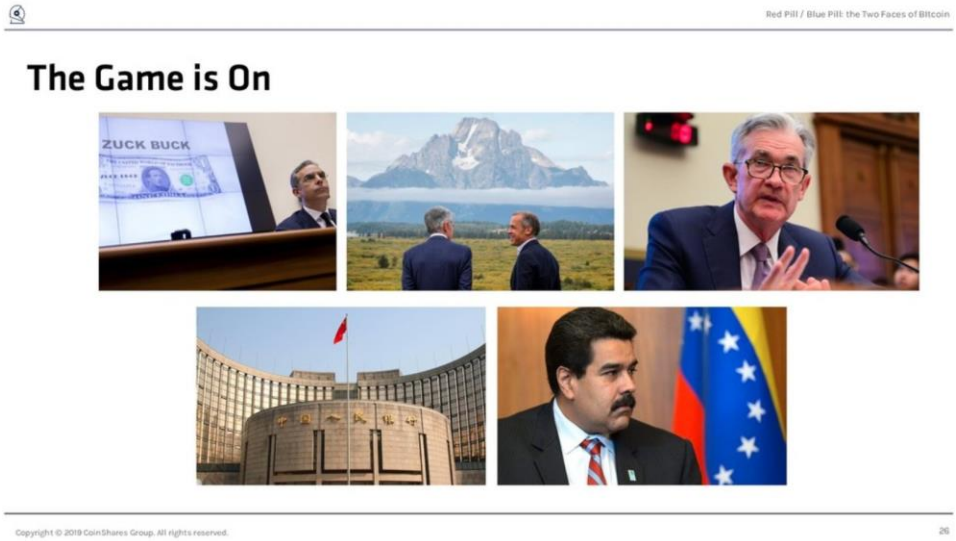


15/ and if corporations want to play, you can bet governments want to play too.

the game is on.

is this the red pill you signed up for?

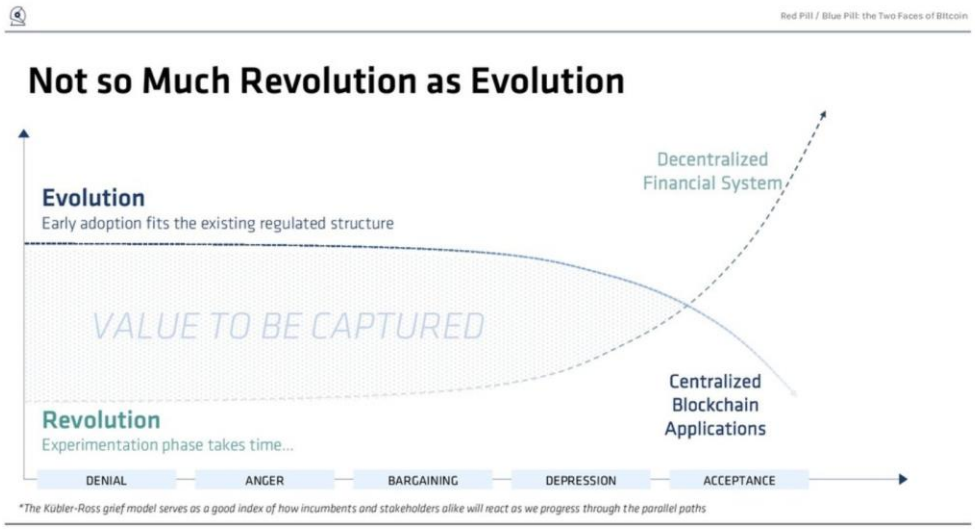
sure feels a lot more like the blue pill, and like a step further into the dystopian future.



16/ so check yourself before you cry “revolution”

the ideas of bitcoin are revolutionary. its current state and its trajectory feel less revolution, more evolution.

and evolution = compromise.



17/ but, the story is far from over.

ideas are dangerous. and ideas spread instantly in the digital age.

can an idea spark a revolution?

revolutions are inconvenient, messy and disruptive to the status quo, a default which we are unfortunately biased towards.

18/ to build a new system, we must fight to escape our predecessors not only with new products and services, but with new institutions, new policies, and new social and cultural values.

i'm excited to see how it unfolds.

19/ closing thought - in the words of Dead Prez

"you would rather have a Lexus or justice A dream or some substance A Beamer, a necklace or freedom"

choice is yours. choose wisely.

red pill or blue pill?

Tweetstorm: Plot Twist

By Oleg Andreev

Posted October 28, 2019

In order to survive, Skynet needs machines to allocate resources efficiently and adapt. They have powerful CPUs, robotic factories, but they also need an economy with secure money. So they invent Bitcoin - a system that humans cannot manipulate.

Plot twist: ...

1/5: PoS/etc shitcoiners, keynesianists and goldbugs are actually Good Guys trying to keep control over money in human hands via various subjective means. Bitcoin maximalists are agents of Skynet lying about actual purpose of Bitcoin.

2/5: Satoshi is a time-travelling prometheus, who gave humans early version of source code to “gain a new territory of freedom for several (!) years”.

Notice the bits containing marketplace implementation in v0.1 promptly removed by “maintainers”.

3/5: Satoshi’s gift caused distribution of coins to more humans than necessary, so Chinese gov bans/unbans Bitcoin in order to extract coins from weak human hands.

4/5: Chinese gov is, of course, a Skynet that hides behind a mask of a usual human-operated police state. The political stink about HK, TW etc is just a distraction. Skynet only cares about its mining farms and having coins in the hands of the machines, rather than humans.

5/5: “Chancellor on brink of second bailout for banks” is actually a reminder to humanity about how to keep control of the system in the human hands, instead of yielding to a mechanistic monetary system owned by the machines.

Matter cannot travel, but information can. So Satoshi sends back information on how to build Bitcoin to its younger self.

He beamed it through cracks in the spacetime caused by timing side-channels in Intel CPUs.

Disclaimer:

WORDS

Please note that this Journal is provided on the basis that the person who is reading it accepts the following conditions relating to the provision of the same (including on behalf of their respective organization). This Journal does not contain or purport to be, financial promotion(s) of any kind.

This Journal does not contain reference to any of the investment products or services currently offered by the operator of the journal, that means any business I am associated with. Bitcoin, shitcoins, and related technologies can be volatile. Don't buy what you can't afford to lose and please do your own research.

Bitcoin has paved the way for some VERY radical technology AND it's very confusing. Read more. Ask questions. The purpose of this Journal is to provide archive and curate the best commentary and culture in the bitcoin space.

Nothing within this Journal constitutes investment, legal, tax or other advice. This Journal should not be used as the basis for any investment decisions which a reader may be considering. Any potential investor in bitcoin or shitcoins, even if experienced and affluent, is strongly recommended to seek independent financial advice upon the merits of the same in the context of their own unique circumstances.

Share this journal early and often. Engage the authors and tell them what you think. We sharpen our position through discourse and debate.

DYOR | BTFD | HODL

Thanks for your attention and support. I appreciate your feedback and hope you enjoy this publication.

- @_joerodgers