

The background of the entire image is a dense, chaotic web of thin, glowing lines in various colors including orange, yellow, blue, and purple. These lines are tangled and looped, creating a complex, almost organic pattern against a solid black background. In the upper right quadrant, there is a white rectangular frame containing the word "WORDS" in a bold, white, sans-serif font.

WORDS

July 2020

A collection of commentary from the
brightest minds in Bitcoin.

Contents

Contents.....	2
Goals and Scope.....	3
Support WORDS	4
There will be bitcoin.	6
Bitcoin: A Global Standard of Value	13
Freedom Money – Bitcoin and the First Amendment.....	20
Masters and Slaves of Money.....	24
Soft money, Soft minds.	62
Bitcoin is more like ham radio than the early internet.....	65
Accepting Scarcity: A Bitcoin Meditation	69
The Path to Taproot Activation	74
Taproot: Why Activate?	84
3 Reasons I'm Investing in Bitcoin	95
Ten Years of Bitcoin Market Data	123
The Alchemy of Hashpower, Part I.....	126
Debunking Common Bitcoin Myths	144
Bitcoin: Separating Money From State.....	156
Bitcoin mining has the potential to save distressed heavy industrial businesses	166
Disclaimer:	171

Goals and Scope

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

History

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

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

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

Support WORDS

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

 Support WORDS

Spread the word

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

Follow us on social media

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

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

 Twitter

Subscribe to our newsletter

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

Subscribe

Our pledge

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

There will be bitcoin.

By Steve Barbour

Posted June 23, 2020



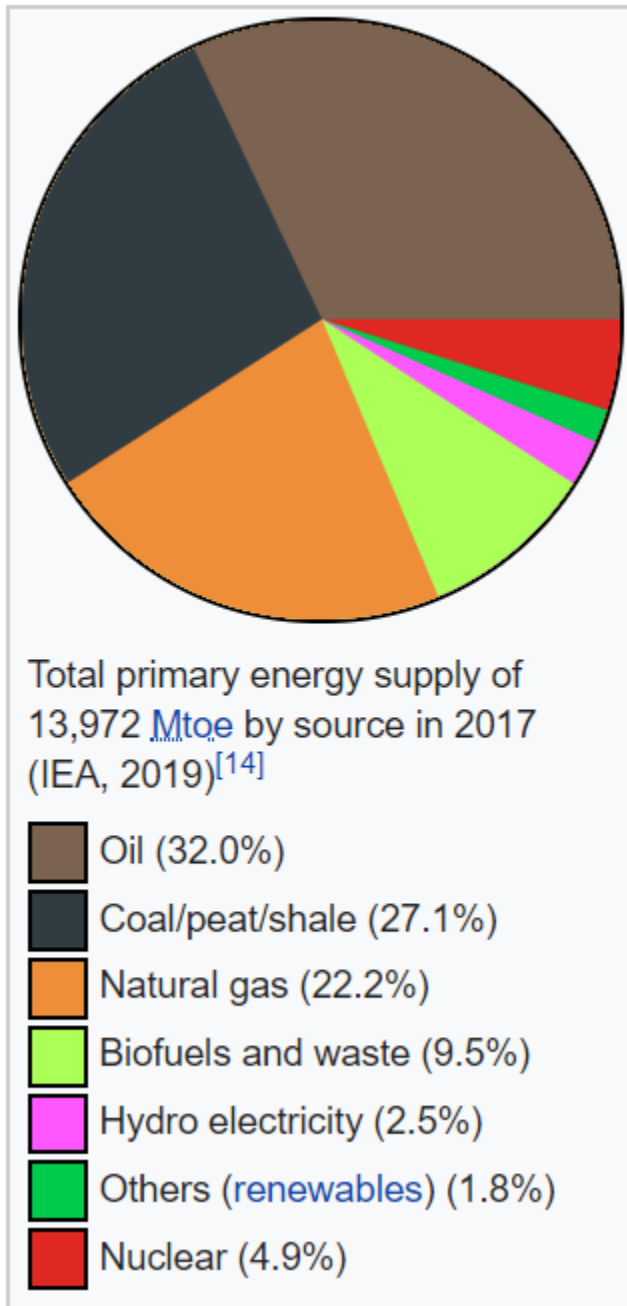
Black, digital gold.

The future of bitcoin mining is oilfield.

There is no greater quantity of stranded and wasted energy in the world than there is in oilfield.

Some quick facts:

- Natural gas flaring volumes reported to be 145 billion cubic meters in 2018, representing approximately 5% of total natural gas production globally. [Source: World Bank]
- Venting and flaring volumes are largely under reported by oil and gas producers, volumes likely significantly higher. *I can also attest to this fact from direct field experience.* [1]
- Economically stranded gas wells represent a massively growing liability. *I wrote about this here:* [2]
- Oil and gas still accounts for the lions share of energy produced annually:



Oil and gas continues to dominate the global energy production mix.

No, sweetheart, oil and gas is not going away.

Let's just get this fact straight first.

It has become increasingly fashionable in recent years to bash oil and gas as being "dirty", despite there being no actual "cleaner" alternatives that scale or do not rely on fossil fuels and their seemingly endless useful byproducts.

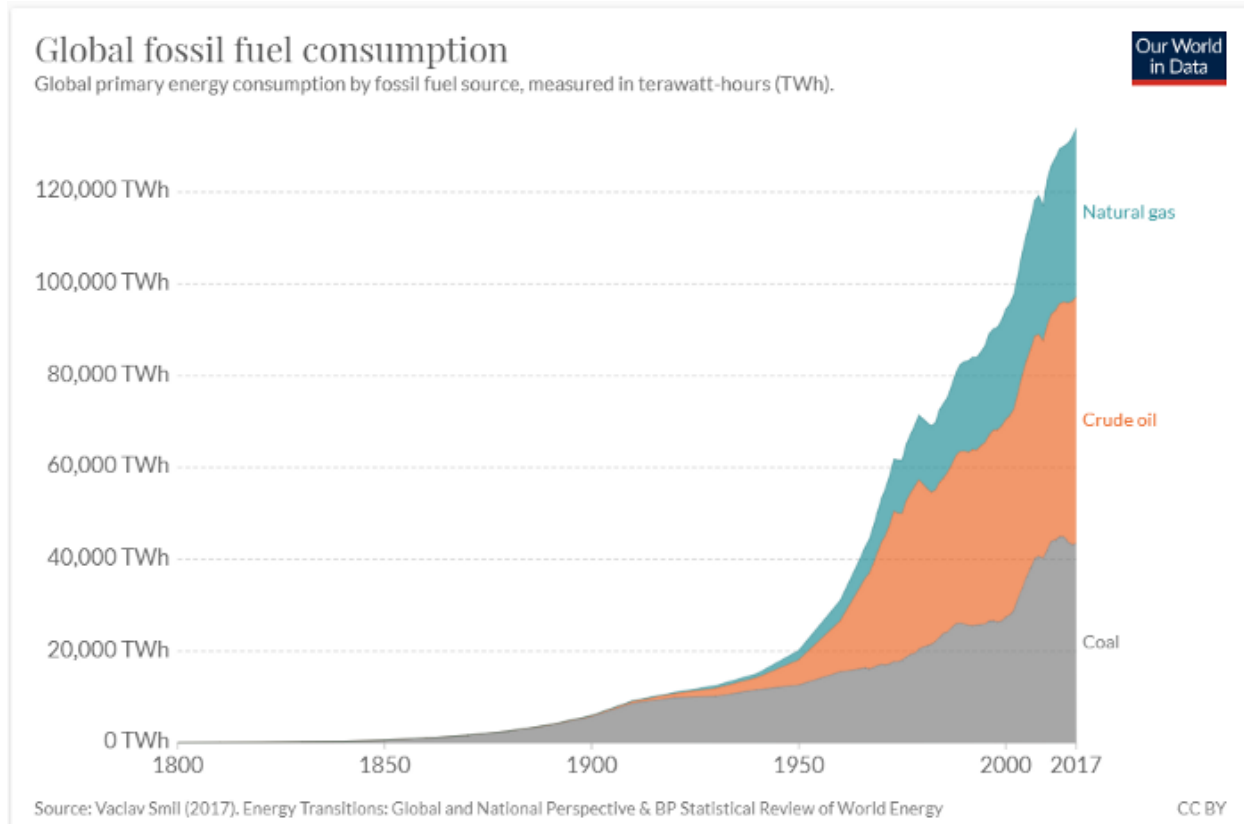
The error they make is to overlook how integral and essential fossil fuels are to every aspect of daily life. Literally nobody in the first world can do basically anything without using fossil fuels, it is built into all of our infrastructure.

You'd think this wouldn't need an explanation but apparently for some people it's easy to forget that roads are paved in oil.

Despite the feel good narratives to the contrary, fossil fuels are the ***basis of modern human civilization*** now and for the foreseeable future. It's time we all accept that and focus on how to make better use of our limited resources.

Oil and gas production continues to grow.

If you look at the data the only time we ever see a flattening or decline in annual boe production is when there is an economic recession. E.g. early 2000's, 2008–2009 and likely 2020 numbers will soon show the same. But they are typically small, insignificant blips in the grand scheme:



Despite the last few decades of cave-dwelling academics and the brain-dead media conglomerates incorrectly predicting and hyping the decline of the oil and gas industry, it turns out that oil and gas production is correlated to consumer demand and not with feel good, 'clean-tech' narratives. Who could have thunk it?

The data shows no signs of oil and gas demand slowing, in fact the very opposite appears to be the case as third-world countries propel themselves to first-world, populations continue to grow and people continue to spend more money on more goods, bigger houses and longer vacations.

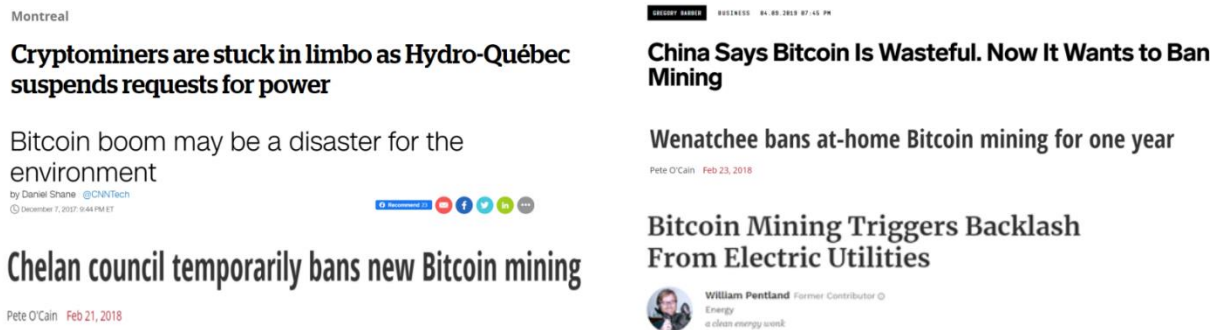
Consumerism is alive and well my friends, they are literally banking on it.

Grid miners will lose market share.

To date bitcoin mining has been dominated by cheap grid energy, largely that located in China due to a significant oversupply of hydro-electric capacity. This has simply been very low hanging fruit enabled by massive capital misallocation by the Chinese State — dams built to accommodate demand that has yet to surface.

Generally, Utility companies who control the grid welcome bitcoin miners in the same way that any business welcomes new demand for their product.

However, when bitcoin miners start competing with the core customer base for the energy, things may get... hairy.



Miners getting #rekt by Utilities / Politicians.

In most jurisdictions energy projects are largely subsidized by government grants, tax incentives or other forms of financial subsidies (**cough-low-interest-rate-financing-enabled-by-monopoly-money-printing-cough**).

The reason these projects are socialized with taxpayer money is to attempt to bring affordable energy to the taxpaying residential, commercial and industrial customers. These projects often require enormous capital and the end users get many years to decades to pay out the investment.

Indeed, regulations protect the taxpaying end-users by preventing utilities from jacking up prices (utilities are generally monopolists, after all). The point is that Utilities that are subsidized by taxpayers / financiers will therefore give the taxpaying base the priority and preferred pricing for the energy, it is their mandate to do so.

This means we should expect increased discrimination against bitcoin miners by utilities and politicians going forward.

What, do you think that they are going to shut off power to residential areas when the next bitcoin bull run and subsequent mining hysteria causes grid overload? Nope. They're going to go after miners by jacking up electricity prices at the very least. We've already seen it many times and we're barely out of the gate.

Lets also not forget that mining is possibly the easiest "job" on the planet, simply plug a computer in the wall and you're "working". The barrier to entry for grid mining is so low that competition will inevitably continue to drive up energy prices for grid miners. With ASIC's becoming cheaper and cheaper due to rapid hardware commoditization, it is only getting easier for everybody to join the race for the next block.

And I won't even touch on how the black market bitcoin miners who steal power, don't pay taxes, bribe politicians and circumvent other costs that white market miners have to comply with and become disadvantaged by third party rules.

It is simply not going to be an easy road ahead for grid mining.

Why oilfield and not renewable energy?

There is a popular meme about how bitcoin mining is good for renewable energy advancement. The logic is that the large % of wasted or curtailed energy related to wind or solar farms can be instead used to operate bitcoin mines and therefore improve the project life-cycle payout by monetizing the energy that would otherwise be wasted.

This is certainly true for existing renewable projects in which capital has already been sunk, but as for driving new renewable projects? I have my doubts.

Yes, energy demand directly at the source is great for renewable energy and helps them become more efficient, but the same also applies to all energy sources. Energy demand also makes coal, natural gas, diesel and nuclear more efficient as well.

A bitcoin mine is effectively a "smart" load bank. "Dumb" load banks are already widely used in practically all power generation industries to help regulate load for a variety of needs and applications, sometime intermittently and sometimes continuously. For example, load banks are often used to keep large reciprocating engines above a minimum load to prevent them from being damaged from carbon build up, etc.

Controlling load is generally useful for all power generation technologies, so there's probably not enough evidence yet to say if mining does more for renewable sources relative to the alternatives. Considering I know of very few mines that exclusively use wind or solar energy, I have my doubts.

Regardless, my biggest issue with this meme is that bitcoin mining simply does not solve the energy storage problem that plagues wind and solar energy sources.

The entire purpose of large scale renewable projects is to **displace** fossil fuels like coal and natural gas off the grid. Adding a bitcoin mine to a solar or wind farm does not do anything to meet this goal because both wind and solar energy still cannot respond to grid demand. The reason for this is because they have no associated energy storage mechanism that is practical (generally speaking). They produce electricity only when the wind blows or the sun shines and a bitcoin mine does **nothing** to make the sun shine any

harder when the grid demands it, so the grid still relies on some means of stored energy (i.e. fossil fuels).

We could argue that the solar and wind farms just need to be oversized for the expected energy demands of the grid, but that simply represents massive capital waste and up-front carbon emissions and defeats the purpose entirely.

I simply do not see how a bitcoin mine helps renewable energy displace fossil fuels, which is the only point of large scale renewable energy projects in the first place.

Subsidies mean unsustainable

Then there's the matter of subsidies, perhaps the elephant in the room on this topic. Renewable projects require massive subsidies to fly and do not actually make economic sense to pursue otherwise (*which means they are anything but "green", but I digress*).

If bitcoin mining does not meaningfully displace the reliance on reliable fossil fuel energy stores then logic follows that bitcoin mining only makes sense to help *existing* wind and solar projects improve pay back rather than drive new capital to be deployed into new wind and solar projects.

But if this is the case then we have to ask — why would the State continue to subsidize renewable energy projects with taxpayer dollars if it ends up simply subsidizing bitcoin miners while failing to significantly displace fossil fuel sources?

And, maybe the greater question, why would the State subsidize bitcoin miners when bitcoin is literally anti-State money that competes with their ability to conduct seigniorage?

Last I checked businesses and organizations don't usually like subsidizing their competition.

Conclusion

As a demand on energy directly at the source, bitcoin mining helps all energy producers operate more efficiently.

With the majority of the world's energy continuing to come from fossil fuels, along with the majority of wasted and stranded energy sources, I'm going all-in on bitcoin mining being dominated by fossil fuel producers in the next few decades and beyond.

And to be honest I feel really good about it. There is absolutely nothing dirty about fossil fuels, just like there is nothing dirty about human civilization.

I want humanity to find more efficient energy technologies as much as anybody, but I do not believe that denigrating oil and gas workers for doing the work in which we hire them. Oil and gas projects are paid partially by you and your own consumption habits, mind you.

Until we have actual alternatives to oil and gas that scale we should all be working together and help our current energy producers innovate and operate more efficiently.

Bitcoin is simply another tool on our belts.

♡ Steve

Bitcoin: A Global Standard of Value

By Paul Knight

Posted February 1, 2020

Wences Casares, in an interview with Laura Shin, said this about bitcoin:¹

If Bitcoin succeeds, it will become a global standard of value and a global standard of settlement. Gold was the value and gold is the one that resembles most Bitcoin in that it wasn't controlled by any one country and it was truly apolitical. The way Bitcoin is apolitical.

If I want to compare the square footage of the first cabin my grandfather had in Patagonia back in 1940, with the square footage of some grandparent of yours Laura, who came to the US and had a cabin or a house somewhere. It's very easy to compare the square footage. Your father had a house that was 1500 square-foot and my grandpa had one that was 1000 square-foot. [But] when we want to compare how much they paid for it, even if we have access to exact amount they pay, we have to adjust that number to compare them. And we can adjust them to inflation. And in inflation we have to choose the inflation of the currency that we're using or we can turn it into some other, into gold at the time. There are many different ways we can adjust it and in choosing the way we we're going to use, is somewhat subjective and therefore the final number is somewhat subjective. Where the result being that **the comparison that we are doing of value is a very subjective comparison and it shouldn't be. It should be as objective as comparing square footage.**

And today we can't do that and I think a world in which Bitcoin succeeds, it's one in which **Bitcoin becomes this non political and objective measure of value.** That when you ask for things that matter globally like the price of a currency, the currency is priced in Bitcoin and commodities are priced in Bitcoin and an international trade is done in Bitcoin. It doesn't mean that any currency in the world disappears. It just means that the meta currency that connects all of those currencies is now a non political currency. With non political value and with non political settlement. Where absolutely anyone can settle in that currency on a Sunday at 2:00 AM with anyone. And that's new. That has never happened before and it will be very powerful.

The concept of a *global standard of value* is intriguing, especially considering the role time plays in changing the things we value and the games governments play against one another in manipulating their currencies. In Wences's example above, we should be able to compare the values of two different houses at two different times just as we can compare

their square footages. But this isn't the system we have today. As Saifedean Ammous said in his book *The Bitcoin Standard*, allowing currencies (measures of value) to float as they do today is like "attempting to build a house with an elastic measuring tape whose own length varied every time it was used."

These concepts of values and standards have been rolling around in my head as I've been thinking what I'm actually buying when I buy bitcoin. *How much value (or scarcity, unforgeable costliness², utility, or collectibility) am I buying per bitcoin? How does that compare to other assets?*

The theoretical supply limit of bitcoin is fixed at 21 million. To date, approximately 18.2 million³ bitcoins have been mined. It is estimated that approximately three million bitcoins have been permanently lost⁴, leaving a current supply of 15.2 million bitcoins. **A single bitcoin, then, represents approximately $1/15,200,000 = 0.00000657\%$ of the current total supply.** That number will get smaller at a fixed schedule until the theoretical supply limit of bitcoin is reached, estimated to occur in the year 2140.

Now that we have a number that represents a specific proportion of this scarce asset, we can ask ourselves, *"If I owned an equivalent proportion of gold (ie, an equivalent percentage ownership of the total above ground supply of gold) how much would that be worth?"* Let's do the math.

Total above-ground supply of gold: 6,824,531,328 ounces⁵
Valuation: \$1,592 per ounce

1 Bitcoin $\Leftrightarrow 0.00000657\% \times 6,824,531,328 \text{ ounces} \times \$1,592 \text{ per ounce}$

1 Bitcoin $\Leftrightarrow 449.2 \text{ ounces of gold} \times \$1,592 \text{ per ounce}$

1 Bitcoin \Leftrightarrow \$715,058 of gold

Given that 1 bitcoin represents 0.00000657% of the total bitcoin stock, if one wished to purchase an equivalent share of gold's stock they would need to buy 449.2 ounces (or 28.1 pounds) of gold at a price of \$715,058.

This observation is useful if we think of bitcoin as digital gold. If we argue that bitcoin possesses similar if not superior properties to the metal, then we can see that, at bitcoin's current valuation of \$9,400 per bitcoin, it is dramatically undervalued relative to gold by some 76 times. If bitcoin is to attain a status and worldwide recognition as digital gold, we can see that its USD price has a lot of room to the upside.

But what about other assets of limited supply? And assets that aren't as readily comparable to bitcoin? Let's look at U.S. cropland.

Supply: 253,700,000 acres⁶
Valuation: \$4,130/acre⁷

1 Bitcoin \Leftrightarrow 0.00000657% x 253,700,000 acres x \$4,130 per acre

1 Bitcoin \Leftrightarrow 16.7 acres x \$4,130 per acre

1 Bitcoin \Leftrightarrow \$68,960 of U.S. arable cropland

Again, we find that, relative to U.S. cropland— a limited, hard asset — bitcoin is undervalued. This comparison is meaningful if we want to compare bitcoin to the limited land area within the U.S., but we may want to explore other types of land, because not all land is of equal location, utility, or disposition. We'll do this in a few paragraphs.

But now notice that we have assigned two different assets, gold and cropland, values in similar terms, that of net scarcity through bitcoin. This allows us to easily compare the two assets with a simple ratio of one to the other. The result ($\$715,058/\$68,960=10.3$) is the realization that we (as the total market of buyers, the generators of demand) place a higher premium on the inherent value of gold than we do on the inherent value of cropland. **Gold has a monetary premium approximately 10 times higher than that of cropland.** Gold's *value density* is greater than that of cropland's.

Before using bitcoin as a standard of value in this way (a standard of scarcity), it was impossible to directly compare gold to land. Gold is priced at \$1,592 per ounce and cropland at \$4,130 per acre. But we cannot directly compare ounces of metal to acres of land. To say that an acre of arable land is worth 2.6 ounces of gold is a useful metric if we place all other items in terms of gold. But the inherent value of gold fluctuates over time which is caused by market cycles, changing preferences, and ad hoc changes in the gold stock (the true scarcity of gold is ultimately unknowable). An ounce of gold today may or may not carry the same inherent value as an ounce of gold 100 years ago or 100 years from now. Instead, **I propose that a better intermediary is to use a common unit of scarcity.**

“Scarcity is money's most important property. If supply of the unit of measure were constantly and unpredictably changing, it would be very difficult to measure the value of goods relative to it, which is why scarcity, on its own, is an incredibly valuable property. While the value of the underlying measurement unit may fluctuate relative to goods and services, stability in the supply of money results in the least amount of noise in the relative price signal of other goods.” — Parker Lewis⁹

We could pick any number we'd like for this unit of scarcity: one percent, or 10 percent, or 12.64298 percent. The actual number doesn't matter, we just have to use it consistently and define it as the standard. So what number do we choose?

The scarcity of bitcoin is a universally recognized and secure fixture of scarcity. Because of its framework and infrastructure, **Bitcoin can be the**

yardstick of value. Think of this in a similar way of how the meter was originally defined in terms of the circumference of the Earth. When the meter was established, it was pegged to something tangible (at least conceptually tangible). **The Earth is a tangible and conceptual basis of physical dimension; Bitcoin can serve the same purpose for value.**

Assets Priced in Bitcoin Scarcity

When disparate assets are assessed relative to bitcoin, they can then be compared directly to each other, their units cancelling out leaving only a magnitude. This magnitude is an expression of relative value. Using our new bitcoin yardstick, the table below compares various assets.⁸

Asset	Supply	Units	Valuation	Bitcoin Standard Value
Gold (above-ground stock)	6,824,531,328	ounces	\$1,592/ounce	\$715,055
Manhattan Developable Land	9,600	acres	\$177,000,000/acre	\$111,885
U.S. Arable Land	253,700,000	acres	\$4,130/acre	\$68,960
Silver (above-ground stock)	56,438,400,000	ounces	\$18/ounce	\$66,861
Rough Diamond	142,000,000	carats	\$110/carats	\$1,027
Atlanta Homes w/ Mortgage (City Limits)	58,721	households	\$265,700/household	\$1,027
Atlanta Homes w/ Mortgage (Inman Park)	3,748	households	\$471,400/household	\$116
Vermeer Painting	24	paintings	\$40,000,000/painting	\$63
The Hope Diamond	46	carats	\$7,700,000/carats	\$23
Honus Wagner Baseball Card	57	cards	\$2,000,000/card	\$8
Sources				
https://www.bitcoinblockhalf.com				
https://fortune.com/2017/11/25/lost-bitcoins/				
https://www.gold.org/goldhub/data/above-ground-stocks				
https://www.statista.com/statistics/201762/projection-for-total-us-cropland-area-from-2010/				
https://www.nass.usda.gov/Publications/Todays_Reports/reports/land0818.pdf				
https://www.point2homes.com/US/Neighborhood/GA/Atlanta/Inman-Park-Demographics.html				
https://www.point2homes.com/US/Neighborhood/GA/Atlanta/Inman-Park-Demographics.html				
http://www.paulzimniskv.com/2017-global-natural-diamond-production-forecasted-at-142m-carats-worth-15-6b				
https://seekingalpha.com/article/4310421-how-much-silver-is-above-ground				

Table comparing various assets, their nominal valuations and inherent (ie, Bitcoin) valuations.

Many interesting observations can be made from the above table:

1. Of the assets listed, gold has the highest value density.
2. While the price-per-acre of land in Manhattan is over 42,000 times more expensive than that of U.S. farmland, the actual value density of Manhattan land is only 1.6 times that of farmland (\$111,885/\$68,960=1.6). The market values Manhattan land higher than farmland, but, as it turns out, not unreasonably so.
3. Owner occupied homes with mortgages within Atlanta city limits are 10 times more valuable than those within the specific neighborhood of

Inman Park, even though Inman Park homes are almost twice as expensive in nominal USD terms as the average Atlanta home. Said another way, it is more important (more valuable) to the market to be within the city of Atlanta than it is to be within a particular neighborhood; that value comes out as a monetary premium on the average lesser-priced home.

4. Rough diamonds carry a monetary premium of 44 times that over the famed Hope Diamond. While there is only one Hope Diamond, there are very few entities that could purchase such a stone; alternatively, there are millions of carats of rough diamonds with millions of buyers willing to pay a premium to have a small piece of the stock.
5. Atlanta homes and rough diamonds share equal inherent values (\$1,027 unit of scarcity).
6. Honus Wagner baseball cards are the least valuable items on the list \$8 while the market collectively gives the work of dutch master painter Johannes Vermeer a premium of eight times \$63 over the most treasured of all baseball cards. That said, one could ask: Only eight times? What might that say about our culture?_

Analyses like these can help an investor weigh the current value of bitcoin and make educated best guesses about where it might be headed, but it can also allow us to compare the relative values of everything in our lives. This paper proposes that Bitcoin represents a secure and stable standard by which we can weigh these values. But like the actual supply of gold, the actual supply of available bitcoins is unknowable because the exact number of lost bitcoins is ultimately unknowable. Therefore, **to make Bitcoin a true standard, we can use the knowable, theoretical supply limit to arrive at the following: 1 bitcoin / 21,000,000 bitcoins = 0.00000476%. This is the new, universal constant of value, and can be applied to all assets of limited supply.**

But Value Is Subjective

But wait, you protest. Isn't value subjective? And doesn't it change over time? Yes, value is subjective on a micro level and it does indeed change over time. The subjectivity of value is constrained on the micro level. We like to think that we are unique creatures operating independently as free-thinking individuals. The reality is we're more like ants: our collective preferences and decisions agglomerate together to form quite a singular thing we call *the Market*. The Market is where a few dozen (or million or billion) buyers and sellers meet at the margin and decide what something is worth. Sure you might buy the blue sweater and I might buy the red one (a reflection of our respective individualities), but the Market has determined that blue is *in* and red is *out* and so, a week later, my red sweater shows up on the clearance

rack for 50% off while your blue sweater is displayed in the store window priced at a substantial premium. That's value; and it changes over time.

Let's take a Vincent van Gogh. Back in his day, few people valued his artwork and were only willing to pay a few hundred Francs for it. But what does that actually mean? How do we, modern purveyors of US dollars, make sense of that? How do Francs compare to US dollars? How do their respective inflation rates compare? Perhaps we could figure it out by comparing those few hundreds francs to the cost of living at the time to our cost of living today, but what was *their* standard of living? And how does that compare to ours? There are so many questions as to how the painting was valued that it makes it impossible to paint an accurate picture.

Now let's assume that M. van Gogh had instead priced his paintings in bitcoin and that a buyer had paid 0.001 bitcoin for a single painting. And let's further assume that, today, the same painting just sold for 2,000 bitcoin. With everything pegged to bitcoin then and now, all the earlier questions we had of local currency and standard of living is already discounted in the price paid in bitcoin. **Bitcoin, through its fixed supply, is the full representation of relative value at any given time.** While the painting became more valuable relative to everything else over time, value is a zero-sum game: value was pulled away from something else and directed toward the van Gogh painting because the painting became more valuable at a much larger rate than all the other goods and services one can purchase at any given moment. **Our bitcoin yardstick can act as a measure for value, allowing us to see with precision how we (the market) assign value, assess how that changes over time, and help lead us away from something nominal toward something more absolute.**

This is a working paper. I welcome any and all comments and contributions. Thank you.

Footnotes:

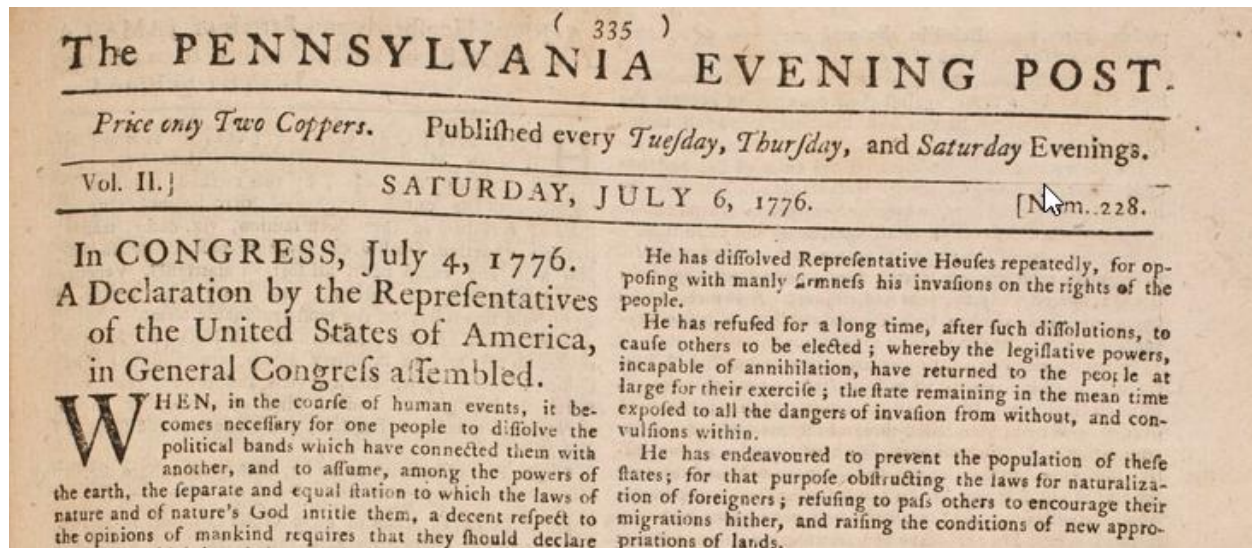
1. <https://unchainedpodcast.com/xapos-wences-casares-on-how-bitcoin-makes-a-fairer-world/>
2. <https://nakamotoinstitute.org/shelling-out/>
3. <https://www.bitcoinblockhalf.com>
4. <https://fortune.com/2017/11/25/lost-bitcoins/>
5. <https://www.gold.org/goldhub/data/above-ground-stocks>
6. <https://www.statista.com/statistics/201762/projection-for-total-us-cropland-area-from-2010/>
7. https://www.nass.usda.gov/Publications/Todays_Reports/reports/land0818.pdf

8. Note on the calculation of Manhattan's developable land: I subtracted Central Park from the area of Manhattan (figures obtained from Wikipedia), then multiplied the remainder by 70% to account for streets and parks. This left me with about 9,600 acres of developable land. I then applied this to the total land valuation obtained here:
<https://www.sciencedirect.com/science/article/abs/pii/S0166046217300820>
 9. <https://nakamotoinstitute.org/mempool/bitcoin-is-not-backed-by-nothing/>
-

Freedom Money - Bitcoin and the First Amendment

By Hector Rosenkrans

Posted July 4, 2020



The Declaration of Independence was first made public in the Pennsylvania Evening Post

Living in 2020 means witnessing a revolution in our tools of communication. The last time this kind of shift happened was with the invention of the printing press, where individuals were empowered to freely communicate, share ideas, and organize with each other. The press put the power of the written word, from the Bible to the Federalist Papers, into the hands of ordinary people, and led to both the Reformation and the American Revolution. The framers of the Constitution understood this deeply, and enshrined these ideals atop our most important legal framework.

Freedom of the (Printing) Press

As the cornerstone to the Bill of Rights, the First Amendment lays out the core freedoms central to the idea of America. Our rights to speech, assembly, and religion are fundamental to our humanity. Recognizing this is a prerequisite to to sustain a government of the people, by the people, and for the people.

Freedom of the press is critically important as well, and it relies on technology for their realization. Freedom of speech empowers anyone to ask hard questions of their elected officials and powerful institutions, but we need

technology to make their answers available to the public. Freedom of the press ensures that information can be published on a blog or in a newspaper, and broadcast over TV, radio, and streaming services.

At their core, the freedom of speech relies on the right to leverage technology to coordinate ideas and actions among individuals at scale. The printing press granted us ability to economically copy and distribute the written word at massive scale. Ideas from the Gutenberg Bible to the Common Sense were widely distributed, and could be interpreted by anyone who could read. The soft technology of the written word was turbocharged by the hard technology of mechanical innovation, and led to the revolutions that lifted the world into modernity.

Digital Speech



With the advent of the internet, we have exponentially improved on the power of the printing press. Overhead costs to reproduce ideas have again fallen to fractions of their previous levels. More importantly, instantaneous world-wide distribution of anything that can be expressed on a screen went from impossible at any cost to practically free. For a brief period of time, speech was freed at global scale for anyone with access to the internet.

Unfortunately, freedom of speech that transcends borders has come at a cost. Our traditional methods for filtering quality ideas from gossip have broken down. Worse still, they have been replaced with algorithms trained to optimize for our attention at any cost. Competition for advertising revenue has driven an arms race for our time, leading to sensational headlines, click-bait, and constant ‘nudges’ from our pockets. The reason for this battle is that the world of networks, power accrues to scale, creating winner-take-all markets in information. In the wake of the Web 2.0 wars, we are left with a few large companies in nearly complete control of our tools of communication.

In the process of winning their respective networks, these companies have accrued an incredible set of data about our daily lives, enabling levels of surveillance and potential censorship unimaginable in the wildest dreams of a Stasi or SS officer. Google has recognized this growing responsibility since the early days of 2000 and 2001 when their “Don’t Be Evil” motto was introduced. Their decision to remove this language from their core message is troubling.

Overtime the risk that these tools will threaten liberty compound. Legal pressure from governments, political pressure from the mob, and economic pressure from advertisers and investors could push Facebook, Google, and others to decisions that threaten our freedoms. Today we are protected only by promises. America’s founders deeply feared the monopolist’s power, but they could not have imagined that the biggest threat to freedom would come from companies that can monopolize communications, rather than a government that monopolizes force.

A Revolution in Privacy

The Internet scaled our tools of communication over the past 30 years at an unprecedented clip and has dominated our popular understanding of computers. At the same time, another technology revolution has been quietly playing out in parallel. The development of strong public key cryptography began in secrecy in the 1970s at GHQC, the NSA’s British cousin, and was made public in 1976.

The importance of cryptography for everyday use is increasingly clear. We can now arm ourselves with tools to protect our ideas and our data at minimal cost, exposing them only to who we chose. In the era of mass communication and mass surveillance, free expression but automated censorship, strong and open cryptography returns power to individuals. We have the ability to restore the freedoms defined in the First Amendment to their full potential, but this time in an even more connected, open, and inclusive world.

The role of Bitcoin

While public key cryptography protects our ideas and information, it doesn't help with the content filtering problem that led to data monopolists in the first place. Markets and prices are the most effective tools for discovering value and quality, but only when the underlying money used to measure economic reality is stable and predictable.

Bitcoin solved this by creating a kind of money that operates on the same infrastructure and protocols as the internet itself, but cannot be freely printed like dollars or copied like click-bait. While technical limitations of ensuring trust in the system have prevented rapid integration at scale, steady progress is happening every day. Centuries after the invention of the printing press, we have finally found a method to store and exchange value using the same tools we use to store and exchange ideas.

Internet money will enable us to use markets to discover and filter valuable new ideas, without relying on a central authority or algorithm with its own motives. Bitcoin is fully open, ensuring the system that can be trusted by people with radically different ideas and cultures. It has the ability to serve as a common language that facilitates both trade and communication around the world.

Bitcoin offers far more than a break from the legacy financial system. It's a protocol enabling digitally native value. For America, breaking away from England was just the first step, she had to prove to the world that she could effectively govern herself and honor her professed values. Building trust is a massive challenge that takes time and patience, most people are happy to subject themselves to the convenience of central authorities and go about their lives. But when they work, open ideas offer a blank slate build a better world.

Masters and Slaves of Money

By Robert Breedlove

Posted July 5, 2020

Money is a tool for trading human time. Central banks, the modern-era masters of money, wield this tool as a weapon to steal time and inflict wealth inequality. History shows us that the corruption of monetary systems leads to moral decay, social collapse, and slavery. As the temptation to manipulate money has always proven to be too strong for mankind to resist, the only antidote for this poison is an incorruptible money — Bitcoin.



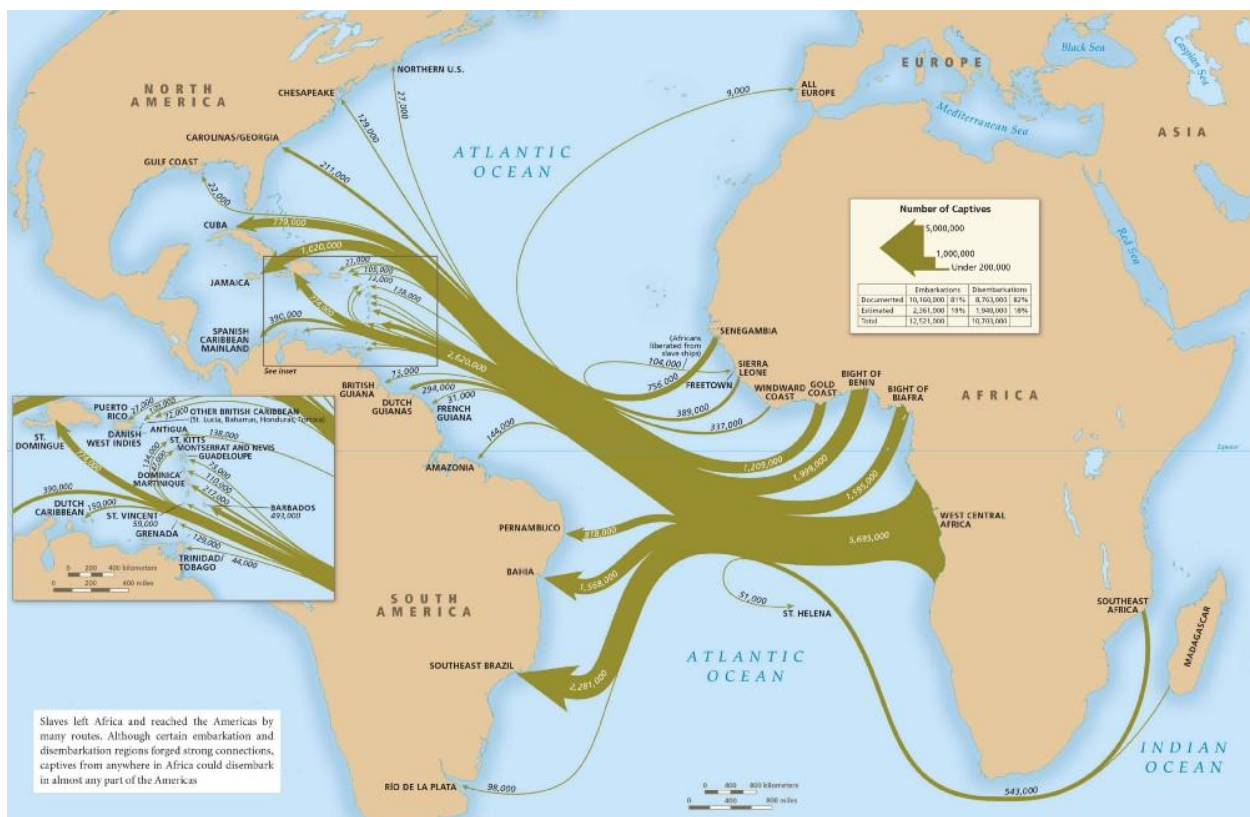
Counterfeiters are Slavemasters

“Knowledge makes a man unfit to be a slave.” —Frederick Douglass

In ancient western Africa, _aggry beads—_small, decorative glass beads—were used as money for many centuries. Of uncertain origins, these beads were a means of wealth transfer between people in trade (as money) and across generations (as dowries or heirlooms). When European explorers appeared in Africa in the 16th century, it was quickly apparent to them that aggy beads were highly valued by African locals. Since glass-making technology in Africa was primitive at the time, aggy beads were difficult to produce and, therefore, reliably scarce relative to other goods—a monetary property which supported their market value.

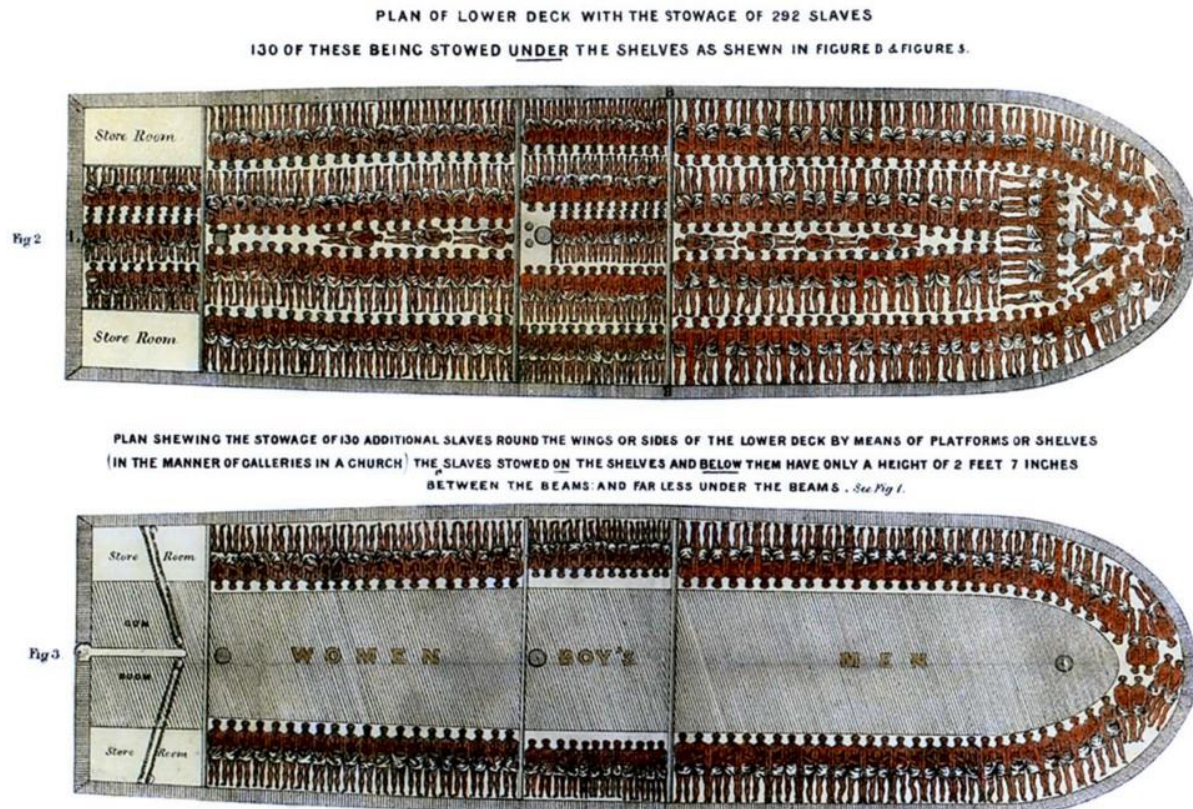
Back in Europe, glass-making technology was more sophisticated; counterfeit beads virtually identical to aggrы beads could be mass produced at a low cost. Seizing the economic opportunity, many crafty Europeans soon began arranging expeditions to western Africa, shipping in huge quantities of (indistinguishably counterfeit) aggrы beads expertly fashioned in European glass-making facilities. This scheme was one of the first known large-scale money counterfeiting operations in the world. What followed this seemingly innocuous exportation of glass beads was a multi-decade plundering of African wealth, natural resources, and—ultimately—time.

As European ships arrived on African shores, many with hulls packed full of glass beads, locals readily traded their hard-earned assets for what they believed were precious aggrы beads. Spanning the course of decades, this trading of real assets for counterfeit beads facilitated a surreptitious confiscation of African wealth by Europeans—a slow-motion criminal episode that crippled African society for centuries to come. Aggrы beads would later become known as “slave beads”; as newly impoverished Africans became desperate, some were forced to sell themselves or others as slaves to their European usurpers. Slave beads—one of history’s many monetary systems weaponized by counterfeiters—became instrumental in the multi-century trans-Atlantic slave trade.



Over the course of 365 years, over 12.5M slaves were transited from Africa to Europe and the Americas.

In a barbaric irony of history, ships landing in Africa stuffed with (counterfeit) aggrry beads later departed for European and American shores with full payloads of precious human cargo. Inhumane and unforgivingly precise, masters of these slave ships packed their hulls tightly with African slaves, just like the glass beads that were used to purchase their captive human cargo in the first place.



Like the counterfeit aggrry beads used to purchase them, African slaves were packed tightly inside the hulls of ships for transit to Europe and the Americas.

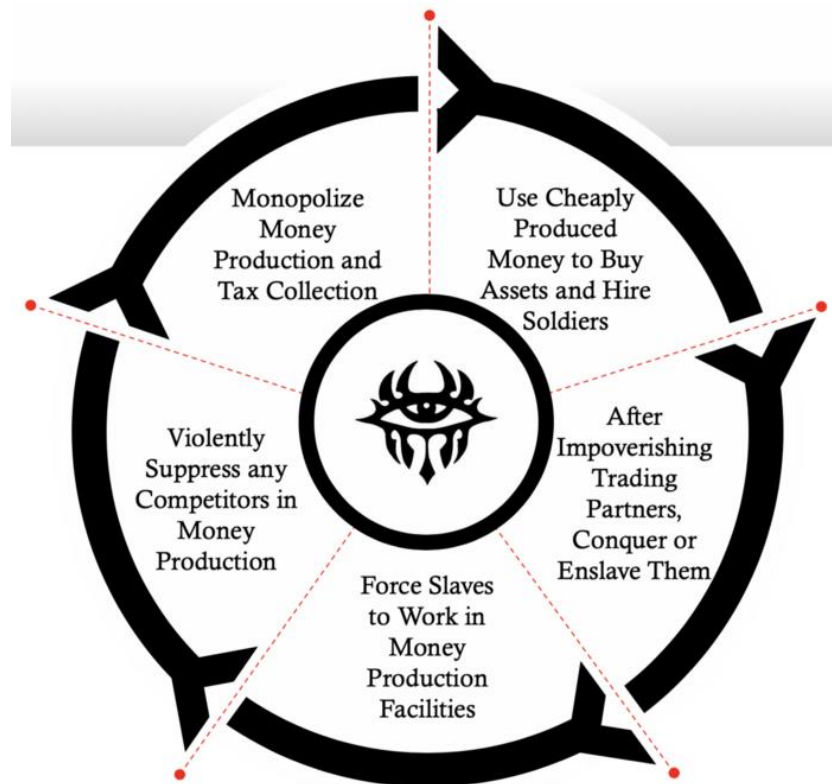
Unfortunately, this pillaging of wealth was not an isolated episode. Cloth strips were another form of money used in ancient Africa, which became a well-established transactional medium over many centuries of dealing with Muslim traders from the north. Local African tribes soon began producing these cloth strips—known colloquially as *panos*—but were outcompeted by the more efficient production methods employed by the Portuguese. A perversely profitable economic arrangement ensued, in which the Portuguese used panos to purchase African slaves who were then put to work producing the very cloth strips with which their freedom was stolen. As Scottish historian Christopher Fyfe described this dreadful trade relationship:

“Some of the slaves were weavers by profession, and wove the cotton into country cloths as they had done on the mainland. New elaborate patterns of North African type were introduced, and from the middle of the 16th century Cape Verde panos [cloth strips] were regularly exported to Guiné to be exchanged for slaves.”

Lured by a virtually limitless profit potential, Portuguese panos producers soon established a state-sponsored monopoly called the Grão Pará and Maranhão Company, which mandated the use of its warehousing and trading-post operations for all financial flows denominated in panos. This company enforced the use of panos for tax payments, to forcibly denominate slave trade contracts, and to hire soldiers. To name just one similar, non-coincidental example today: the US government enforces the use of dollars for tax collections, as legal tender, as the nominal currency for contracts on oil (the energy slave of modernity), and as the international reserve currency (the infamous “exorbitant privilege”).

Events strikingly similar to aggrary beads and panos are playing out today throughout the global economy: the US dollar in your pocket, the one you sacrificed so much to obtain, was recently mass-produced by the US government with a (near-effortless) keystroke. In the same way Europeans had access to superior glass-making technology that gave them the ability to counterfeit money at a low cost, or the Portuguese monopolized panos production, central banks have an exclusive privilege to produce money at near-zero cost, enabling them to confiscate wealth from all users of dollars at will. Although less visible and overtly violent, central banks today carry out operations using the same weaponized methods of theft as those wielded by wily Europeans against unsuspecting Africans.

Histories of human action related to aggrary beads and panos hold important lessons for societies suffering under central banking: ***those who can monopolize money production become de facto currency counterfeiting operations that steal human labor in perpetuity.*** When free market forces are manipulated, producers gain an asymmetric ability to set prices without regard to customer preferences, thereby converting economic democracies into dictatorships, and freedom into tyranny. For money, this implies monopolists can acquire human time (aka labor) in the marketplace at an unfair price. Said differently: money monopolists can steal human time—a malevolent power that effectively makes them ***slavemasters***.



An exclusive right to produce money without regard for competitive market pressures is an apparatus of enslavement—a vile privilege that monopolists can only preserve through deception and violence.

Counterfeit aggrary beads and panos were weapons used to acquire human time; acts which led to the direct theft of 12.5M human lives between 1501 and 1806 (and the indirect theft of their progeny). The trans-Atlantic slave trade was a slow-motion holocaust on Africans; roughly 2M died in transit through the infamous Middle Passage, and those who survived spent the rest of their waking lives toiling away, or bearing children to replenish their slavemaster's stock. Quantifying this atrocity from an economic perspective (not counting those born into slavery): assuming the average slave could labor 5,000 hours each year for 40 years, the staggering total time stolen amounts to over 2.5T (2,5000,000,000,000) hours, or 6.8B hours stolen per year for 365 years (source [link](https://bitcointalk.org/index.php?topic=1000000)).

SLAVERY IS THEFT - THEFT OF A LIFE,
THEFT OF WORK, THEFT OF ANY PROPERTY
OR PRODUCE, THEFT EVEN OF THE
CHILDREN A SLAVE MIGHT HAVE BORNE.

- KEVIN BALES -

LIBQUOTES.COM

The trans-Atlantic slave trade was a travesty as gruesome as it was gigantic; if only money production monopolies had faced free market competition, this horror of human history would not have reached such a colossal scale. In (non-violent) market competition, producer actions are guided by the preferences of customers: a dynamic that drives low prices and technological innovation. Absent this accountability, producers are incentivized to do anything necessary to expand their market share—up to and including violent coercion. Simply, market pressures keep people honest: as such, the structures of markets and moralities are mutually intertwined.

Markets, Sovereignty, and Morality

“To be moral, an act must be free.” — **Murray N. Rothbard**

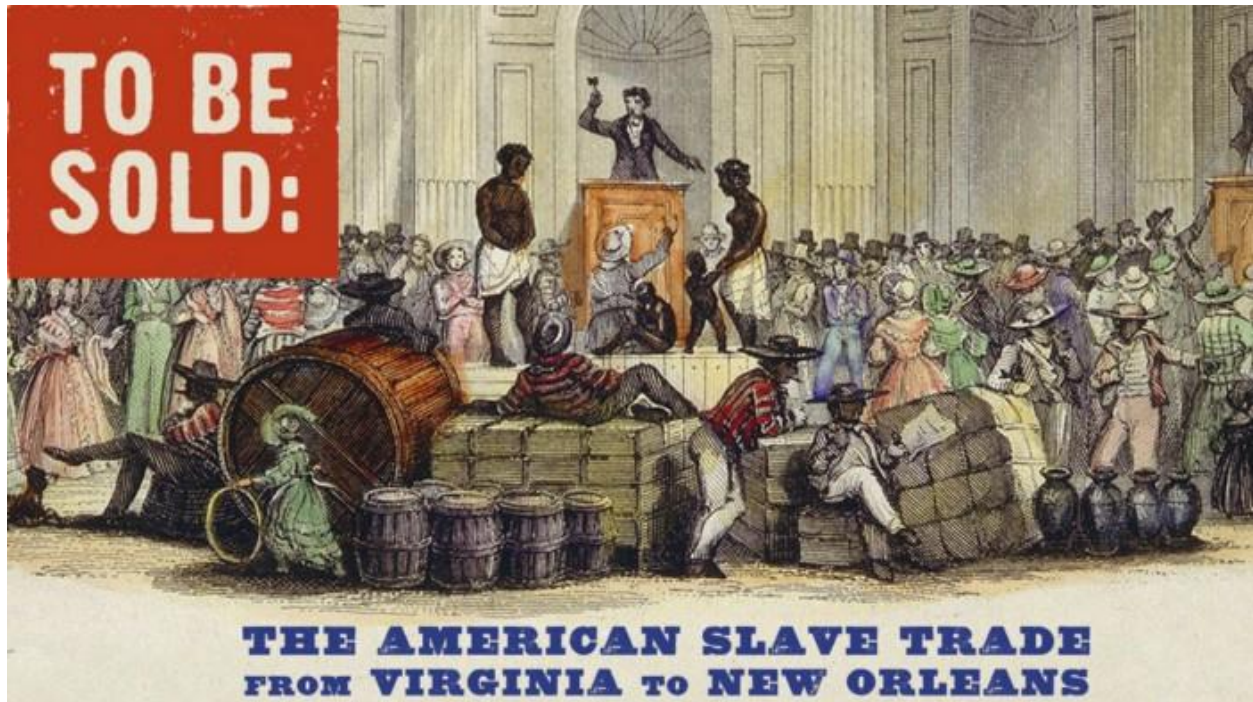
Competition is a natural process of discovery: in sports, it is the way we discover which team is more competent in any single game; throughout an entire season of play, repeated competition is how we discover which team is best overall. In free markets, competition is the set of games played to discover “satisfactions of wants”: each entrepreneur places “bets” (investments of capital, money, and time) as they attempt to prove their competitors wrong in the marketplace by delivering better, faster, or cheaper solutions to the problems their customers want solved. Market competition is the catalyst of honest work and true progress for civilization. As the American pragmatists said: “truth is the end of inquiry”—in this sense, the free market may be thought of as a setting of continuous inquiry that zeroes-in on *truth*. The ideas competition generates, which withstand its sustained

entrepreneurial inquisition, are our best approximations of truth—as William James said:

“Any idea upon which we can ride ... any idea that will carry us prosperously from any one part of our experience to any other part, linking things satisfactorily, working securely, saving labor; is true for just so much, true in so far forth, *true instrumentally*”

Pragmatically, truth is difficult to distinguish from that which is most useful. In forums of free exchange, truth is generated in the form of accurate prices, useful tools, and individual virtue. Prices dynamically represent market participant concurrences on relative exchange ratios, a derivation of countless trade decisions across time. A tool with superior usefulness is the manifestation of mankind’s sharpest present knowledge for solving a specific problem. Put another way: as entrepreneurs inquire about the nature of reality through experimentation, the tools they produce—and the knowledge structure with which these tools are configured—adapt according to customer preferences until one or a few favored solutions become market dominant. Virtue and competitive competency are the character traits infused into successful entrepreneurs that manage to survive the constant economic pressures holding them accountable for profit generation. This truth-seeking function of free markets is inherently iterative: prices, tools, and virtues are constantly changing according to market conditions.

“Points” in market-based games of discovery are denominated in *money* — the tool used to calculate, negotiate, and execute trades most effectively. Market competition is the process that keeps producers honest: when it is suppressed through coercion or violence—as it is within “legal monopolies”—truth becomes distorted into inaccurate prices, low-quality tools, and individual wickedness. For money producers, monopolization means dishonest producers become counterfeiters and gain a (deceptive and violent) dominion over human time.



Stealing human time through currency counterfeiting led to the the auctioning of slave labor.

Contrary to conventional wisdom, money is not “the root of all evil,” it is actually just a tool for trading time (or labor)—the means by which market participants signify sacrifices and successes to one another across the history of economic transactions. Like all tools, money has no independent morality of its own. Tools are *amoral*, meaning they can be used for both good and evil purposes alike. The moral outcome of using a tool is inextricably dependent on the intention of its user. Money is a temporal trading tool, but (as we’ve seen) it can also be wielded maliciously to steal time, in the same way a hammer can be used to build a house or bash a skull.

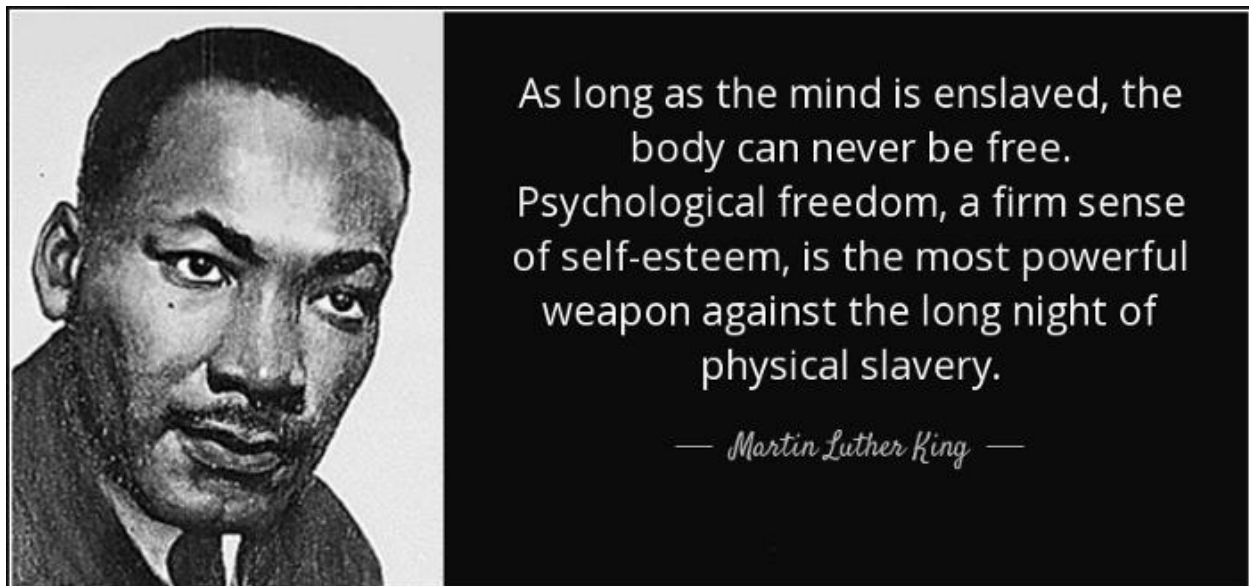
More accurately, money—along with its precursors action and speech—is “the root of all sovereignty”: the authority to act in the world as one sees fit. Sovereignty — a word etymologically associated with monarchy, money, and royalty — refers to the locus of supreme power in the sphere of human action. According to Natural Law, sovereignty inheres within the individual, as each person must consciously decide what actions to take, despite any exogenous influences they may face. An inner sanctum of sovereignty’s generative source lives within each of us — an inviolable principle of reason known as the *logos*. An interface layer between the primary domains of experience—order and chaos—the logos is the defining feature of humanity: our ability to tell and believe stories is what distinguishes man from animal. Victor Frankl calls this interiorized space the “last human freedom”:

"The last of the human freedoms: to choose one's attitude in any given set of circumstances, to choose one's own way. And there were always choices to make. Every day, every hour, offered the opportunity to make a decision, a decision which determined whether you would or would not submit to those powers which threatened to rob you of your very self, your inner freedom; which determined whether or not you become the plaything to circumstance, renouncing freedom and dignity..."

From sovereignty, we derive the word *reign*, which commonly refers to a period of royal rulership. Most of us now live in an era well-past submission to a royal family, and our civilizational conception of sovereignty has been steadily decentralizing over time, moving closer to a clear reflection of Natural Law. As Jordan Peterson [charts](#) this historical progression:

"First of all, the only sovereign was the king. Then the nobles became sovereign. Then all men became sovereign. Then came the Christian revolution and every individual soul, impossibly, became sovereign. That idea of individual sovereignty and worth is the core presupposition of our legal and cultural systems, so we all walk around acting as if every one of us is a divine centre of logos. We grant each other the respect of individual citizens who are sovereign and are equal before the law."

At the foundation of Western Civilization today is the precept that *the sovereignty of the individual is held higher than the state*: an embodied belief at the heart of legal principles such as habeus corpus, the presumption of "innocent until proven guilty," and freedom of speech rights.



Freedom of speech is essential to a peaceful society, as our ideas must be free to clash and resolve conflicts so that our bodies don't. Speech arose in humans as a direct result of our evolutionary development: once a vertical

stance was adopted by our ancestral primates, our visual field was expanded, and our hands became more adept at manipulating the natural environment since they were no longer needed for locomotion. Newly outfitted with opposable thumbs, we developed a dexterity that enabled us to particularize the natural world in useful ways—like sorting things, counting, and making tools. Fine musculature in the face and tongue evolved alongside this precision of hand, giving rise to spoken language, which complemented the hand's ability to categorize the world, and the mind's ability to comprehend it (even our internal dialogue is composed of speech). An ability to manually reconfigure the world reinforced our abstractive capacity to do so verbally, thereby forming a feedback dynamic between these two defining faculties of man. This co-evolution of craftsmanship and verbal articulation led naturally to trade, and (quite simply) the most exchangeable thing in any trading society is its most important tool—money.

Seen this way, money is a direct derivation of action and speech: all three of which are essential media for sovereign self-expression. In this sense, money may be considered a form of speech in and unto itself—*the language of value*. Placing limitations on the use of this language (the purpose of central banks) is commensurately catastrophic to restricting the freedom of speech (which can lead to absurdities like illegal numbers). Free speech digs the grave for despotism, whereas its suppression is the trademark of totalitarian regimes. Indeed, the first effort of every aspiring dictator is always to restrict the voice of dissent—to darken the light of inquiry radiating from the logos. The 20th century had many logos-suppressing dictatorships, we will name two:

“In 1917, the Russian Bolsheviks moved to limit freedom of speech the very day after the October coup-d'état. They adopted the “Decree on the Press,” which shut down any newspapers “sowing discord by libelous distortion of facts.” Similarly, only a few months after coming to power in 1933, German National Socialists started to burn books, and the Ministry of Propaganda introduced strict censorship.

Logos (λόγος) is a Greek word that means “ratio” or “word”—the principle at the core of interpersonal communications, which are largely conducted via words and prices (which are exchange ratios expressed in monetary terms). Both words and prices are “categorical comparatives,” protocols for encapsulating, comparing, and communicating different aspects of reality — herein lives the power of the divine logos to render order from chaos. In language, consider how all words only have meaning relative to one another: all definitions are comprised of other words. In markets, the intersection of subjective supply and objective demand is the price: a dynamic figure reflecting the consensus of the collective logos on any particular good's

exchange value for any other good (for simplicity, expressed in the common language of economic numeracy: money).

For money, governments corrupt the pricing mode of comparative expression by constantly violating the supply of money (via inflation) while simultaneously compelling its demand (via legal tender and tax collection laws). Distorting natural price discovery, a manipulation of the collective logos, is equivalent to perverting the *vox populi*—the voice of the people. George Orwell once said: “If liberty means anything at all, it means the right to tell people what they do not want to hear.” An inability to speak the truth (with words), or prove others wrong in the marketplace (with prices), is the death of liberty; as the 20th century so painfully taught us, restricting the logos is a slippery slope toward totalitarianism. Free expression in all forms is antecedent to proper moral action.



In Soviet Russia, freedom of speech was suppressed and dissent was punished. Independent political activities were not tolerated, whether these involved participation in free labour unions, private corporations, independent churches or opposition political parties.

Like speech, money lacks an intrinsic morality of its own. However, its economic character does influence moral standards—as Buddha taught us: “Money is the worst discovery of human life, but it is the most trusted

material to test human nature." Honest money encourages righteous action, and dishonest money induces moral hazard. To comprehend money's impact on morality, consider the (hypothetical) case of a winemaker living in a centrally banked economy. He knows that his central bank recently doubled the money supply by printing trillions of dollars to "save the economy," and is now faced with three options:

1. Continue selling his wine for \$20, knowing that the value of each dollar has declined 50% due to inflation*
2. Water down his wine or use cheaper ingredients, thereby decreasing the production cost and the quality of his wine, but continue selling it for \$20
3. Double the selling price of his wine to \$40, to get the same value for his wine denominated in post-inflation dollars

**For simplicity, we will ignore the spatiotemporal unevenness of inflation.*

If the winemaker chooses the first option, he incurs a 50% loss. If he decides to water down his wine, he defrauds his customers by selling them an inferior product. If he doubles his price to maintain quality, he risks losing customers to less honest competitors who are willing to compromise on quality. Since diluting wine with water is difficult to detect (for non-connoisseurs) and offers an immediate financial gain, all winemakers face strong incentives to defraud their customers when inflation strikes (a cause of wine scandals). In a similar vein, monetary inflation incentivizes sellers across all industries to deceive their customers. Inflation imposes the temptation of larceny onto seller's hearts, forcing them to weigh financial wellbeing against moral integrity. In this way, inflation is an infectious disease to society's moral fabric. Inflation-resistant money, then, is an antidote to an afflicted social morality. In this (critically important) sense, Bitcoin—the only money with a 0% terminal inflation rate—is the cure for many of the moral cancers riddling our world.



Inflation is a great immiseration on the soul of humanity—a source much moral sickness worldwide.

Money is a source of great temptation, as it can be considered the “list of who owns what,” since money can (by definition) be used to buy anything in the marketplace. When a singularly privileged group (a monopoly) can create money out of thin air, they can amend this “list of who owns what” arbitrarily, and have a powerful incentive to do so to their own benefit. This “money as an ownership ledger” angle sheds light on the underlying impetus for central banking—an institution which arrogates itself as “master of the list” with an exclusive privilege to advance the interests of its private shareholders, even at the expense of enslaving everyone else.

Since everything in the marketplace requires sacrifices of human time to produce (even land needs hands to sell), we can say that money is human time emblemized. In the same way a stock certificate is title to company capital, money is title to human time; people sacrifice time earning money which they can then spend on commensurate sacrifices from others. Clearly, a tool that can command human time is an object of great temptation, as it is a potent source of *power* (defined by physics as work over time). A lust for power is the motivation of most warfare—typically involving attempts to forcibly acquire capital, food, or territory. And a lack of power is closely related

to unhappiness, which makes its consolidation alluring—as Philo Judaeus said:

“No slave is really happy, for what greater misery is there than to live with no power over anything, including oneself?”

Money has always been a critical piece of mankind’s notions of sovereignty and slavery. When naturally selected by free market processes, money is a culmination of the collective logos: a synthesis of individual self-sovereign expressions. But natural money has been hijacked by artificial tyrants: the reason we call states “sovereigns” today is only because they are the gangs that hold most of the world’s freely chosen money — gold.

The So-Called Sovereign States

“I did not know I was a slave until I found out I couldn’t do the things I wanted.” —Frederick Douglass

For over 5,000 years, precious metals have been favored as money since they best fulfilled its five properties: divisibility, durability, portability, recognizability, and scarcity. Gold came to reign supreme because of all the monetary metals, it was the most *scarce*. Scarcity is arguably the most important property of money, as without an assurance of supply limitation, someone always gives in to the temptation to inflate and steal the value stored therein (see: aggrы beads, panos cloth money, or fiat currencies today).

Governments have always interceded in the market for money to commandeer gold coinage and warehousing operations, both of which sought to improve the divisibility, portability, and recognizability properties of money by issuing standardized coins or warehouse receipts. By monopolizing these “certification function” businesses, the state shifted the burden of trust from transacting parties onto itself. States throughout history have always made it their (exclusive) business to certify the value (weight or fineness) of money (coins or bars) and money-substitutes (paper warehouse receipts). Remember: insulation from competition interrupts the truth discovery process engendered by free markets; for this reason, trust placed in any monopoly always ends up shattered.



Government exists to protect property rights: a purpose it defiles by monopolizing and counterfeiting money.

All national currencies began as paper promises for real money. Today, these currencies are no longer redeemable for real money, and instead have been transformed into perennially unfulfilled promises called *fiat currencies*. Governments require societies (a restriction of the collective logos) to transact in these money-substitutes and reserve the exclusive right to manipulate their supplies as a means of siphoning wealth (aka stealing time) from citizens. In effect, fiat currencies are uncollateralized debts undergoing slow-motion default while their use is forced on society. All the while, central banks continue to hoard the real money—gold—and perform final settlement with one another in this authentic, free-market-selected medium of exchange.

Seen this way, “_printing money” actually refers to currency counterfeiting—the production of false promises, as currencies are no longer tied to real money. Said simply: fiat currency is a living lie. Regardless of whether you consider it a tool or a weapon (depending on the subjectivities of user intentionality), manipulating money supplies is objectively useful for only one thing: inflicting wealth inequalities (by stealing time). As G. Braschi puts it: “Every tool is a weapon (if you hold it right).” As a means of gaining an advantage in contests of will, currency counterfeiting is a weapon.

In war times, belligerent nations have made attempts to counterfeit opponent currencies to cause hyperinflation. For example, Nazi Germany had plans to bomb England with counterfeit bank notes to sabotage their

economy. And in Imperial Japan, the Noborito Laboratory experimented with currency counterfeiting operations as an economic subversion strategy. In peacetimes, currency counterfeiting is the exclusive domain of the central bank, whose “expansionary monetary policy” increases the money supply by, say, 7% per year—that is, stealing only 7% of dollar-holder wealth (an accumulation of time-savings) each year via counterfeiting operations.

Of course, when circumstances become too uncertain, market participants naturally flock back to the trust-minimization of physical gold, since money-substitutes are (at best) promises to receive money in the future, they are vulnerable to default. Unlike fiat currencies, gold is an expression of the collective logos, not compulsion from a counterparty. The self-declared “sovereign” state is a business model built on the confiscation of self-sovereign monies like gold and silver. The superior monetary properties of gold made it the most valuable form of self-sovereign money in history, a reign it has maintained since before the founding of ancient Egypt.

The Great Pyramids

“There are two ways to conquer and enslave a country. One is by the sword. The other is by debt.” —John Adams

Ancient Egypt is the archetypal tyranny in the Bible. Egypt is renowned for its Great Pyramids, monoliths which were built on the backs of slave labor. Indeed, the grandeur of these constructions owes a major debt of gratitude to the many slaves whose time was stolen by the Pharaohs—masters of Ancient Egypt. To gain a glimmer of understanding as to just how arduous the construction process was for even a single Great Pyramid, consider this data point from the book *Heroes of History* by Will Durant:

“According to Herodotus... the pyramid itself required the labor of 100,000 men through twenty years.”



Many slave hours went into building the Great Pyramids, but history has even worse pyramid schemes...

To quantify this time-theft from Egyptian slaves more precisely, again assuming that each slave spent 5,000 hours per year engaged in manual labor, a workforce of 100,000 slaves building for 20 years equals 10B hours of time stolen. A staggering amount of man hours condemned to the brutality of physical bondage during the construction of a single Great Pyramid, but (terribly) still less than the time stolen by the greatest pyramid schemes in human history—fiat currencies. As Henry Ford foretold:

“It is well enough that people of the nation do not understand our banking and monetary system, for if they did, I believe there would be a revolution before tomorrow morning.”

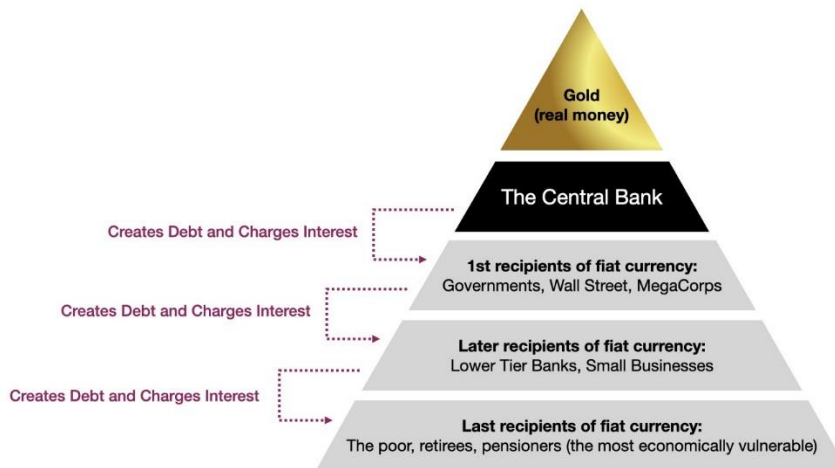
A pyramid scheme is an investment scam based on a hierarchical setup of network marketing, in which higher layer participants profit at the expense of those lower down. Fiat currencies are pyramid schemes erected by central banks, who restrict access to and suppress the price of gold, which would otherwise outcompete their inferior currencies on the free market, since gold is reliably scarce and holds its value across time. The use of fiat currencies is compelled via legal tender and tax laws. It may be hard to believe that the

world's most popular currency is a pyramid scheme, but the symbology of the US dollar tells its own story:



Novus Ordo Seclorum is Latin for “New order of the ages” — this symbol appeared soon after the founding of The Fed: perhaps it refers to the new system of slavery implemented under the monicker of “central banking.”

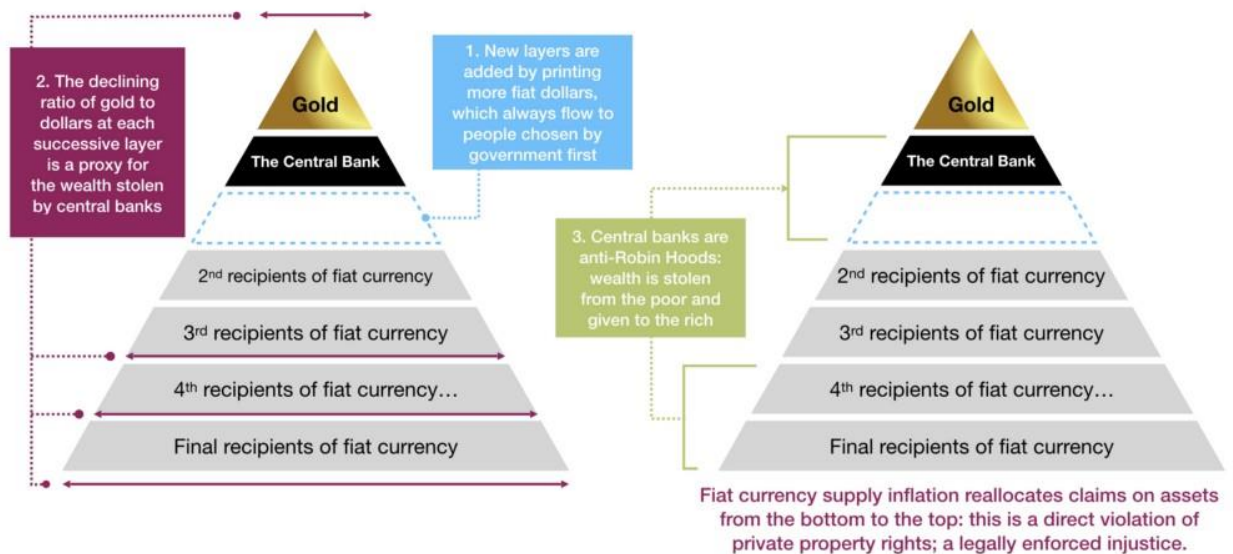
After a long-game legerdemain by governments, these pyramid schemes came to dominate the world. Fiat currencies are debt-based money-substitutes controlled by central banks, which impose these monetary networks on users and suppress all competition in the market coercively or violently (similar to the Grão Pará and Maranhão Company). Most despicably, it is the poorest people in society—who (by necessity) hold the majority of their wealth in fiat currency—that are most victimized by this fraudulent system.

All national currencies, including The US dollar, are Pyramid Schemes.

At the pinnacle fiat currency pyramid schemes is gold: a technology selected as money by the cumulative free choice (the collective logos) of countless entrepreneurs throughout history. Paper currency abstractions of gold were introduced purely to make it more convenient for exchange, not to replace it. Over time, the option to redeem currency for gold was eliminated, giving governments full control over currency scarcity, and therefore an unlimited capacity to confiscate wealth from their citizens by compromising its supply.

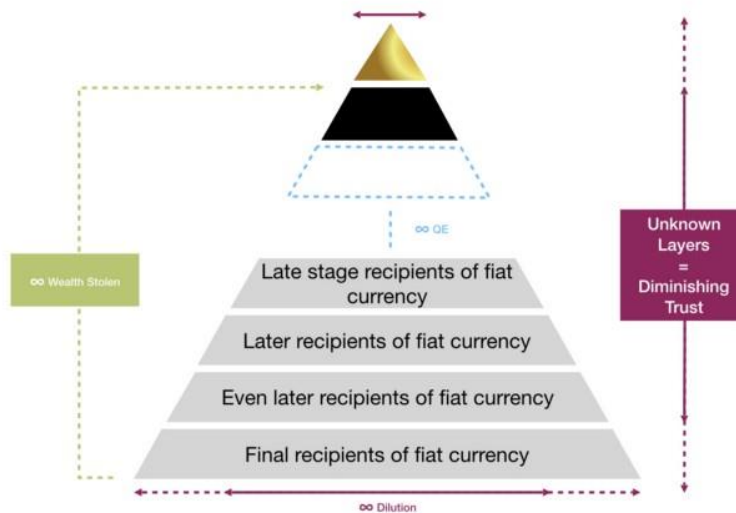
In effect, every time a new unit of fiat currency is printed (euphemistically called "quantitative easing" or QE by central banks), new layers to the pyramid scheme are laid from the top down, and the inflationary costs are externalized onto those using fiat as a store of value. Worse still, each unit of fiat currency is leveraged, so that one unit is multiplied by several orders of magnitude by the time it becomes part of the broad money supply. Looking at The Fed as a specific example: after netting service fee revenue for itself (to fund its operations and a 6% annual dividend to its undisclosed shareholders), The Fed uses the new fiat dollars to purchase US government debt. Freshly printed (more accurately, electronically generated) fiat dollars are then doled out at the discretion of government bureaucrats, who (unsurprisingly) tend to favor the bankers, corporations, and lobbyists that pay for their political campaigns. Detestably, this dynamic reallocates wealth from the poor to the rich (Robin Hood would be ashamed).

Governments collude with central banks to dilute fiat dollar holders by printing more and more, effectively “adding new layers” to their pyramid schemes.



So long as people remain sufficiently passive yet productive, these pyramid schemes can be built ever-higher, and continue to operate as a weapon of wealth extraction (time-theft) for their political perpetrators. However, since there are no free lunches in this universe, this fiat currency supply expansion cannot continue forever. As layers continue to accumulate in round after round of QE, and people are implicitly taxed harder and harder through price inflation, trust in the currency becomes diminished. Like Hemingway said about bankruptcy, this happens gradually at first, then suddenly as inflation gives way to hyperinflation: a total meltdown of the economic trust money is intended to facilitate in the first place. At this point, the “central bank master” has pushed his “fiat-slave citizens” too hard, as they finally reach the edge of their economic livelihoods.

Fiat currency pyramid schemes can be built up indefinitely until the currency collapses (hyperinflation) or people choose to opt out. As pyramids grow taller, people lose trust in the currencies and their scheming overlords.



Fortunately, thanks to Bitcoin, these financial pyramid schemes can no longer be shielded from direct competition (as they are from gold). All fiat currencies are critically dependent on the ability of central banks to subdue competition—the discovery process that would otherwise disrupt their illusion. Owning 20% of the global gold supply gives central banks significant influence over its price, which they actively suppress in the paper markets. Without intervention, fiat currencies would quickly collapse to the superior value proposition of gold as money, as people always favor a money that holds its value across time (by remaining scarce). In this regard, Bitcoin—the world’s only “digital gold”—represents a major breakthrough: a monetary technology that is disruptive to gold, resistant to competitive suppression by central banks, and the one-time discovery of an absolutely scarce money.

Bitcoin is Digital Gold—the only money completely immune to corruption.
Every layer is composed of real money, not paper promises, and its money supply is fixed at 21 million: Bitcoin has absolutely zero unexpected inflation.



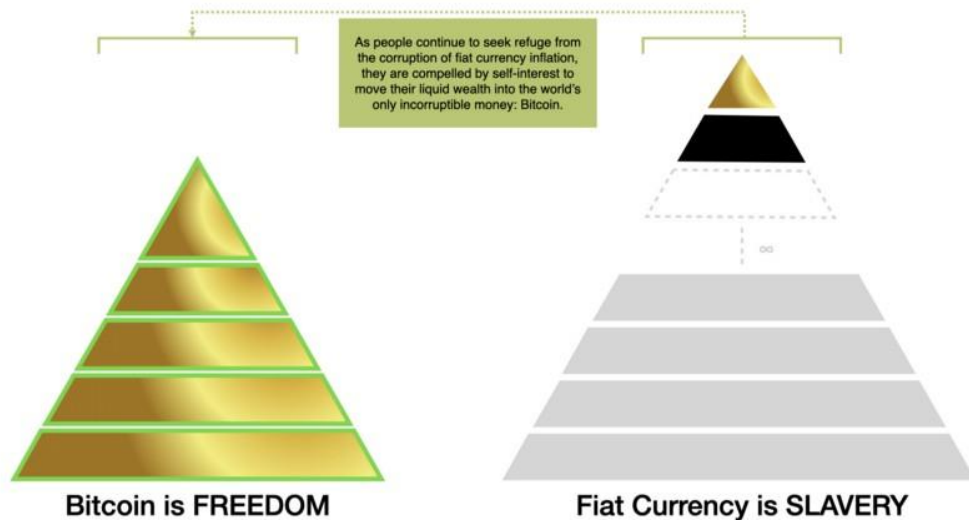
All monies exhibit a multi-level marketing valuation dynamic: for Bitcoin, early adopters benefit disproportionately by anticipating later adoption by others (the Bitcoin economic bootstrapping process is characterized by a virtuous cycle). But unlike the unknowable supplies of fiat currency pyramid schemes, Bitcoin has a universally known supply. For fiat currencies, the “early adopters” are perpetually those with access to the printing press; a positional asymmetry (a political privilege) that makes the game unfair.

A more symmetrical system, Bitcoin is uniquely characterized by [*perfect information*]([https://en.wikipedia.org/wiki/Perfect_information#:~:text=In%20economics%2C%20perfect%20information%20\(sometimes,utility%2C%20and%20own%20cost%20functions.\)](https://en.wikipedia.org/wiki/Perfect_information#:~:text=In%20economics%2C%20perfect%20information%20(sometimes,utility%2C%20and%20own%20cost%20functions.))) meaning that all market participants can see the rules that govern it, verify that there will never be more than 21 million units, and determine precisely when each will be produced—meaning all unexpected supply inflation for Bitcoin is optimized for holders at absolute zero. Perfect information is a prerequisite to the economic concept of perfect competition: an ideal (yet unattainable) market condition where competitiveness is entirely unhampered by unnecessary regulations and wealth generation is maximized. A great promise of Bitcoin is to pull global markets closer toward this state of perfection by separating money and state.

Laid in layers of permanence, this “digital gold” pyramid outshines the inherent uncertainties of fiat currencies. Since money is “insurance against uncertainty,” its demand is centered on the relative certainty of its monetary properties; and Bitcoin optimizes for all five: it exhibits the divisibility, durability, portability, and recognizability of pure information; and the scarcity

of time. Like death and taxes, the certainty of “21 million bitcoin” is a concept that cannot be refuted. Coupled with the incentive to front-run future adoption of this digital, absolutely scarce, and theft-proof money makes Bitcoin a game-theoretic gravity-well that the market for money simply cannot escape. Paradoxically, it is precisely this inescapability that is leading to the liberation of more and more fiat-slaves worldwide.

As fiat currency pyramid schemes continue to grow taller and less trustworthy, each will gradually (then suddenly) collapse into the superiorly trustworthy monetary network of Bitcoin—the world's only incorruptible money.



Symbolized by its fixed height in the image above, the absolute scarcity of the Bitcoin monetary pyramid increasingly outcompetes fiat currency pyramid schemes as they grow comparatively taller and less trustworthy through supply expansion. Eventually, these proverbial “houses of cards” collapse into the full transparency and certainty of Bitcoin. Whether it is understood or not, in the sphere of money, the known serves as protection from the unknown.

Viewed this way, we have much to be hopeful for in the world, as there is finally an incorruptible alternative to the completely unethical system of central banking. Bitcoin is honest money freeing the world from the falsehood of fiat currency. In a transcendental sense, Bitcoin may actually be what the ancient alchemists spent centuries pursuing: the incorruptible substance—called the *lapis philosophorum* in archaic texts—that would serve as an antidote to the corruption of the world. As Jordan Peterson wrote of alchemy in his profound book *Maps of Meaning*:

“The sequence of the alchemical transformation paralleled Christ’s Passion, paralleled the myth of the hero and his redemption. The essential message of alchemy is that individual rejection of tyranny, voluntary pursuit of the unknown and terrifying — predicated upon faith in the ideal — may

engender an individual transformation so overwhelming that its equivalent can only be found in the most profound of religious myths...The ***lapis philosophorum*** is “agent of transformation,” equivalent to the mythological redemptive hero — able to turn “base metals into gold.” It is, as such, something more valuable than gold — just as the hero is more valuable than any of his concrete productions.”

Alchemical methodologies were “proto-science”: experimental processes practiced for thousands of years that were foundational to the later development of the scientific method (even Isaac Newton was an alchemist). As a school of thought, alchemy was a “fork” off of The Church premised on the belief that redemptive knowledge could be found in the laboratory of nature (a heretical concept at the time). Standing at the vanguard of human technological achievement, existing as the only money characterized by a manipulation-proof supply, and inspiring earnest transformations in the lives of true believers, perhaps Bitcoin actually is the ***lapis philosophorum*** pursued by alchemists for centuries—the incorruptible substance giving rebellion to state tyranny and, in doing so, bringing mankind closer to God. Bitcoin is the truth, and by one definition, God is expressed in the truthful speech that rectifies pathological hierarchies. Or as Benjamin Franklin said:

“Rebellion to tyrants is obedience to God.”

Like freedom, love, and truth—God is timeless. I am not talking about a “guy in the sky” here: the ancient idea from Genesis is that God is the force that freely confronts the chaos of potential with courage, truth, and love to convert it into good and useful order. Being made in the image of God, we are all sovereign individuals imbued with the logos, a self-generating power responsible for our ability to harmoniously reconfigure the natural world into good and habitable space. Our future is seeded in our imaginations, a reality we call forth by freely exercising the logos in thought, speech, and action. The logos is the divine spark intrinsic to us all; realizing that words can only miss the mark of spiritual truth, we can venture to say: ***God is the anti-entropic principle eternally propagating through all life.*** As G.K. Chesterton said:

“A dead thing can go with the stream, but only a living thing can go against it.”

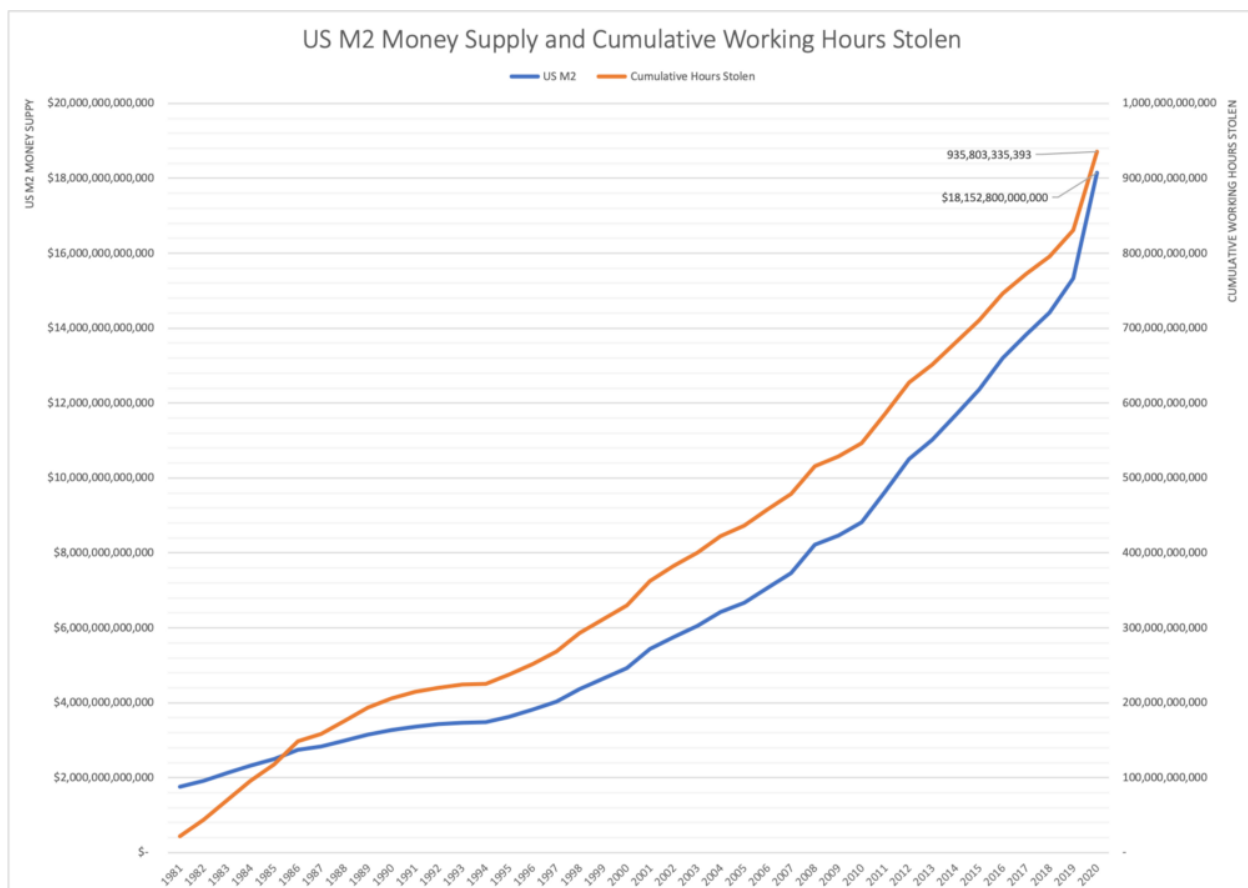
To most truthfully embody the divine principle of the logos individually, and more closely approach the timelessness of God collectively, we must triumph against the evil forces that steal our time secretly and constantly.

Stealing Time

“There is one kind of robber whom the law does not strike at, and who steals what is most precious to men: time.” —Napoleon Bonaparte

Many mistakenly blame capitalism for the myriad economic problems in the world. However, at the heart of every modern economy is an institution of socialism: the central bank. In a primitive sense, the first man who dug a hole to shelter himself from the weather was the first capitalist, and the man who violently encroached on his tiny territory for his own selfish purposes was the first socialist. Capitalism simply means everyone has exclusive rights to the fruits of their own labor; in other words, everyone owns their own time. True capitalists are free to trade any valuables they invest their time to create (goods, services, or knowledge) with other self-owned people doing the same. Socialism, on the other hand, entails that governments (aka other people) own a (greater or lesser) portion of your time; the “pound of flesh” they take through conscription, taxation, and inflation.

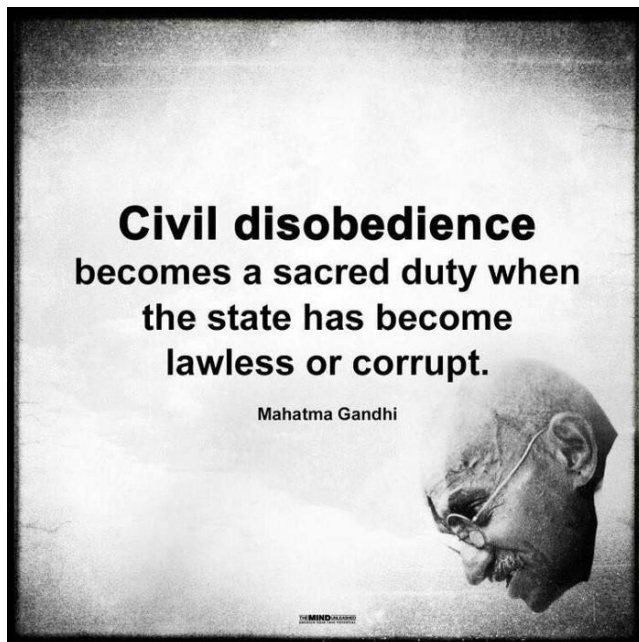
Socialistic fiat currency is the lifeblood of state tyranny: to comprehend just how colossal the central banking system of time-theft has become, let's take a close look at The Fed. Using annual wage data from the social security administration, changes in US M2 money supply, and assuming 2,000 average annual working hours per worker, we arrive at some startling figures. By dividing the growth in USD supply by the average hourly wage each year in dollars, we calculate a proxy for the hours stolen from society through USD supply expansion (source [link](#)).



“Printing money” is currency counterfeiting and the theft of human time—in a word, slavery.

Stealing an average of 7.6% working hours per year since 1981, bureaucrats at The Fed have managed to scalp nearly one trillion hours off the backs of hard working people. Assuming each person works an average of 2,000 hours per year, **this is equivalent to enslaving 11.7M people for 40 years straight**. This implicit taxation via inflation is in addition to all explicit taxes imposed by the US government—all of which are acts of outright socialism. Unless transactions are made by consensual and willing market participants, then exchange is extortive—this is a central tenet of free market capitalism.

Time stolen by The Fed since 1981 is 341% more per year than the trans-Atlantic slave trade. With 23.4B hours stolen annually, The Fed could (in theory) build 2.3 Great Pyramids each year. In terms of absolute human time stolen per year, fiat currency is the largest pyramid scheme and institution of slavery in human history.



When we stop conceiving of central banking as an economics story, and start to see it as a crime story, we are beginning to get the true picture. Capitalism is established in truth (hard work, delayed gratification, and honest trade), whereas socialism is founded in falsehood (bureaucratizing, propagandizing, and theft). Like counterfeit aggry beads and panos, counterfeit dollars are also used to mobilize military efforts, which (before fiat) required explicit taxation or borrowing to finance. Socialistic money is the stealth funding source of evil: it has been used to finance every dictator,

world war, and internment camp in human history. In the 20th century alone, fiat-currency-funded-governments murdered over 169M people—a modern mega-atrocity called *democide*:

TABLE 1.2
20th Century Democide

REGIMES	YEARS	DEMOCIDE (000)[1]			ANNUAL	
		TOTAL	DOMESTIC	GENOCIDE	RATE % [2]	
MEGAMURDERERS	1900-87	151,491	116,380	33,476		[4]
DEKA-MEGAMURDERERS	1900-87	128,168	100,842	26,690	0.18	[4]
U.S.S.R.	1917-87	61,911	54,769	10,000	0.42	
China (PRC)	1949-87	35,236	35,236	375	0.12	
Germany	1933-45	20,946	762	16,315	0.09	
China (KMT)	1928-49	10,075	10,075	Nil	0.07	[5]
LESSER MEGAMURDERS	1900-87	19,178	12,237	6,184	1.63	[4]
Japan	1936-45	5,964	Nil	Nil	Nil	
China (Mao Soviets) [3]	1923-49	3,466	3,466	Nil	0.05	[5]
Cambodia	1975-79	2,035	2,000	541	8.16	
Turkey	1909-18	1,883	1,752	1,883	0.96	
Vietnam	1945-87	1,670	944	Nil	0.10	
Poland	1945-48	1,585	1,585	1,585	1.99	
Pakistan	1958-87	1,503	1,503	1,500	0.06	
Yugoslavia (Tito)	1944-87	1,072	987	675	0.12	
SUSPECTED MEGAMURDERERS	1900-87	4,145	3,301	602	0.24	[4]
North Korea	1948-87	1,663	1,293	Nil	0.25	
Mexico	1900-20	1,417	1,417	100	0.45	
Russia	1900-17	1,066	591	502	0.02	
CENTI-KILOMURDERERS	1900-87	14,918	10,812	4,071	0.26	[4]
TOP 5	1900-87	4,074	2,192	1,078	0.89	[4]
China (Warlords)	1917-49	910	910	Nil	0.02	
Turkey (Atatürk)	1919-23	878	703	878	2.64	
United Kingdom	1900-87	816	Nil	Nil	Nil	
Portugal (Dictatorship)	1926-82	741	Nil	Nil	Nil	
Indonesia	1965-87	729	579	200	0.02	
LESSER MURDERERS	1900-87	2,792	2,355	1,019	.1	[4]
WORLD TOTAL	1900-87	169,202	129,547	38,566	.1	[6]

1. Includes genocide, politicide, and mass murder; excludes war-dead.

These are most probable mid-estimates in low to high ranges.

Figures may not sum due to round off.

2. The percent of a population killed in democide per year of the regime

3. Guerrilla period. 4. Average.

5. The rate is the average of that for three successive periods.

6. The world annual rate is calculated for the 1944 global population

A table quantifying murders by governments from 1900–1987 in millions: 169,202,000 victims of democide.

History is clear: enforced enactment of the fiat currency lie worldwide leads to loss of life on a monstrous scale. Said simply: socialism is fraud, and those who remain silent on the truth of central banking are complicit in its criminality. As Nassim Taleb succinctly states this ethic:

"If you see fraud and do not say fraud, you are a fraud."


The central planning of money is not a new idea. In Marx's 1848 *Manifesto to the Communist Party*, measure number five reads: "Centralization of credit in the hands of the state, by means of a national bank with State capital and an exclusive monopoly." Straight out of Marx's playbook, there is nothing capitalist *at all* about central banking; it is an anticapitalist organization, so let us speak of it truthfully: central banking is monetary socialism—an institution of financial slavery. Further, Karl Marx was a known racist; his socialistic system of central banking is solely designed to extract wealth from those the state deems to be "inferior." It is little surprise, then, that an institution centered on Marxist philosophy has mutated into a racist slavemaster.

Slavemasters seek to steal the benefits of work without making the requisite sacrifices. Across trading societies, gold was favored as money because it required "proof of work" to obtain: an unforgeable costliness that could not be counterfeited, and therefore self-represented the collective sacrifices made to procure it. Work is a noble pursuit, as it carries us closer to the timelessness of God, since all innovations are just productivity enhancers — instruments for accomplishing greater results within the same expanse of time. Theft is the opposite: a twisting of the moral fabric of reality to serve the present ego in defiance of the eternal God. Attempts to twist reality in this way always snap back to devastate those who try: our only salvation from this deceit is the truth.

Money is a social construct created to sacrifice time now and store it for later enjoyment. Debt is created by enjoying now at the cost of later sacrifice. Real money is the final extinguisher of debt. Fiat currency is oxymoronic to the concept of money, since it is born by borrowing. Accordingly, fiat-currency-fueled-economies have spent over a century gorging on debt, and the day of reckoning is at hand: economic reality demands its later sacrifices paid—explaining why governments are on the edge of bankruptcy (morally and financially) today.

An integral element of the social contract, the time we spend serving society today must earn us money redeemable for equivalent services from it in the future. When this intertemporal trust arrangement breaks down due to inflation, society slides into disintegration. Fiat currency is a supreme

instrument of evil in the world: a weapon of intergenerational dispossession wielded by wily slavemasters over unsuspecting subjects.




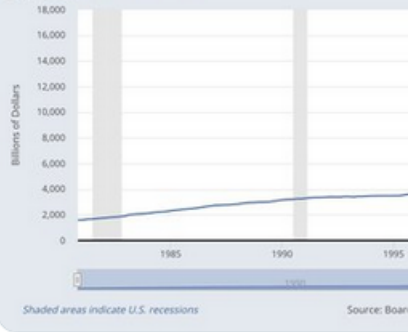
Robert Breedlove
 @Breedlove22

Fiat currency is centered on proof of theft, as measured by its money supply inflation rate.

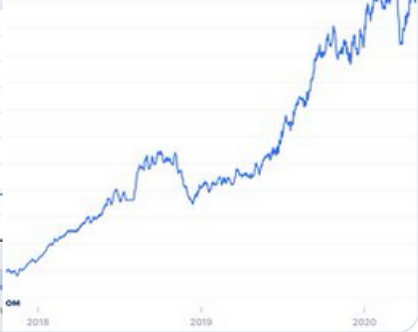
#Bitcoin is based on proof of work, as measured by its hash rate.

Theft is dishonest and demoralizing for both thieves and victims. Honest work is ennobling and empowering for everyone.


M2 Money Stock (M2)
 Observation: 2020-04-13: **16,869.6** (+ more)
 Updated: Apr 23, 2020
 Units: Billions of Dollars, Seasonally Adjusted
 Frequency: Weekly, Ending Monday



Total Hash Rate (TH/s)
 of terahashes per second the bitcoin network is performing in the last 24 hours.



11:07 AM · Apr 28, 2020

198 64 people are Tweeting about this

Modern Slavemasters

“To be a poor man is hard, but to be a poor race in a land of dollars is the very bottom of hardships.” —W.E.B. Du Bois

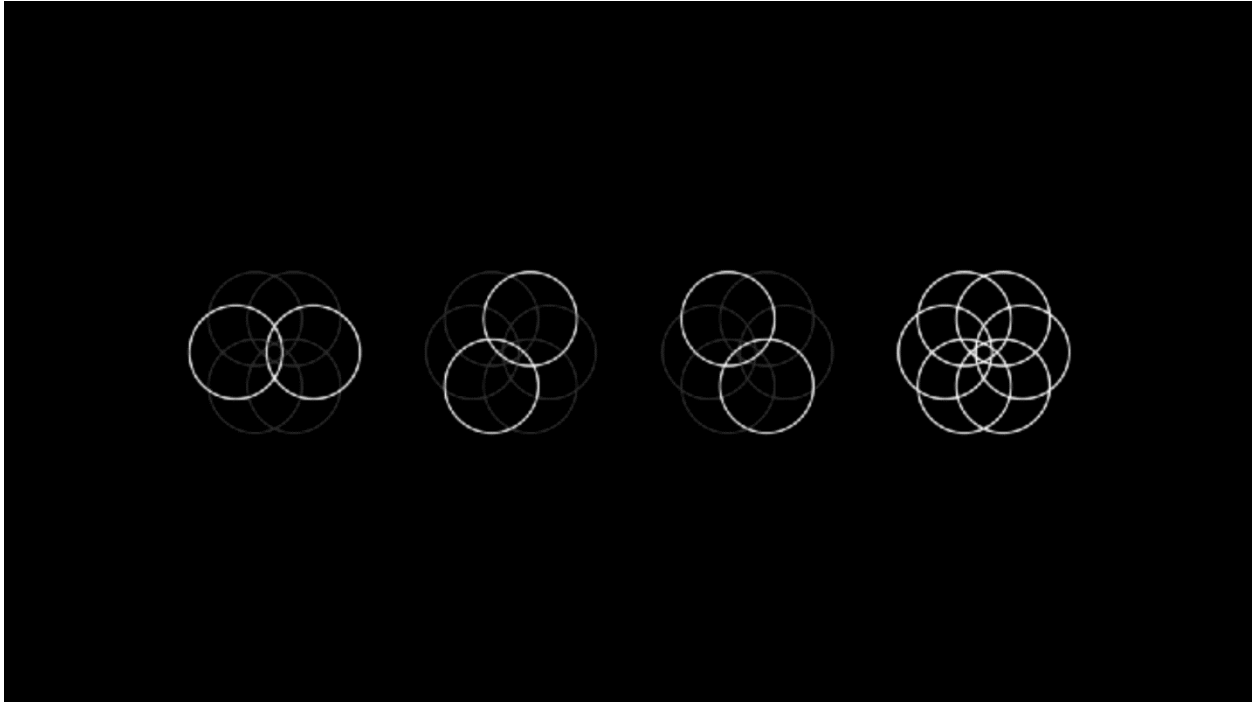
Master and slave dynamics have almost always been racial or cultural in nature, a fact that has not changed even in our present “civilized” age. Recent years in the US have witnessed a rash of police brutality largely targeted at African Americans. And it seems the latest act of police brutality

was the last straw for a society fed up with the seemingly endless stories of black lives assaulted by police. On May 25, 2020, a 46-year-old father, friend, and brother named George Floyd was **murdered** by a state police officer. The cop pinned Floyd down with a knee to the neck, executing a nine-minute-long slow-motion homicide in broad daylight with citizens onlooking helplessly.



Remember: truth is the end of all inquiry. In the digital age, the windows of perception have become exponentially multiplied, thus projecting the light of inquiry into prismatic and interpenetrating patterns. This multi-perspective quality of digitized existence is an accelerant to the truth-finding function of free markets: consider the role of digital technology in the Arab Spring uprising, Wikileaks, and now the George Floyd protests occurring worldwide. In 1965, when Martin Luther King led a protest of unequal voting practices in Alabama, police violently attacked the activists as they marched. Although many events similar to this had come before, this one was *televised*, and that made all the difference. With the eyes of the world watching police brutalize peaceful protestors in real time, the US government was soon pushed to pass legislation banning racial segregation and discrimination.

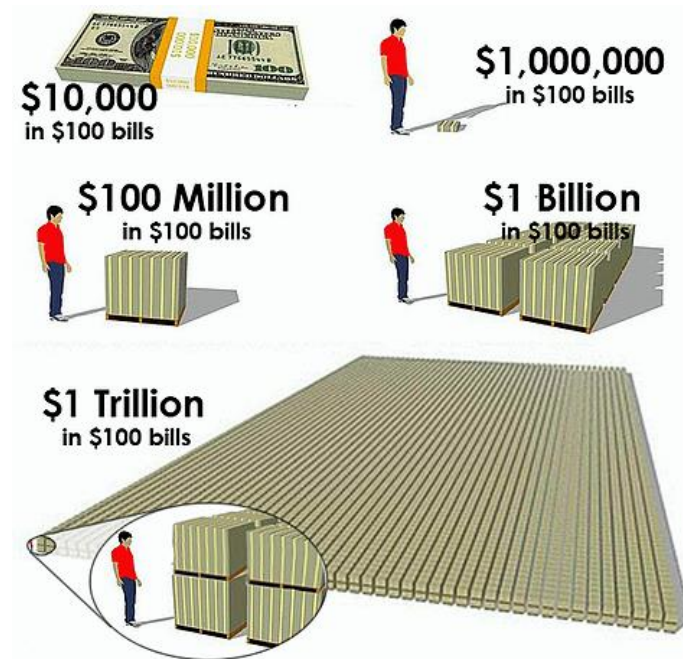
Free market capitalism is a social system in which we see the world through as many eyes as possible (via words and prices) to attain a high resolution picture of reality. In the digital age, this multi-perspectivism of markets has been amplified with smart phones, social media, and live-streaming; thereby further awakening our collective consciousness. The truth is that thousands of tragic stories like George Floyd's have unfolded over time, but the distribution of his via social media sparked a global outcry against police brutality. In the past, murders like this went less noticed, but in modernity the murder of one man can ignite a "fiat-slave rebellion" the world over. George Floyd's murder spreading like wildfire on social media and erupting into a conflagration of protests worldwide is testament to the refractive influence of digital technology on the light of inquiry and, thus, the discovery of truth.



Synthesis of multiple perspectives is the key to gaining a high resolution image of reality: this is the essence of free markets—the forums within which unceasing inquiries become truth.

In truth, police are protectors of government “property”: their job is to “keep the peace” while the state maintains its scheme of constant confiscation from fiat-slaves. Police departments in many southern US cities began as slave patrols tasked with assisting landowners in the recovery and punishment of runaway slaves—thus preserving the “property rights” of slavemasters. Even today, the job of police is to investigate crime by collecting information for the court, not to protect the lives of citizens. As the axiom goes: “possession is nine-tenths of the law,” so clearly the police—a group of militarized fact finders—are truthfully nothing more than glorified government henchmen.

The light of inquiry melts down lies to reveal truth: this is why central banking will fail—it is critically dependent on ignorance, fear, and the suppression of free choice; it cannot stand the galvanizing gaze ever-present in the digital age. Centralized counterfeiting operations will not be tolerated in a world with unprecedented access to knowledge. Before being killed, George Floyd was arrested for attempting to use a counterfeit US \$20 bill: the same crime The Fed perpetrates by the trillion. Millions, billions, trillions: it is easy to say these numbers, but much more difficult to comprehend the actual magnitude of state-sponsored counterfeiting operations. A visualization will help:



George Floyd was murdered for using a counterfeit \$20 bill whereas The Fed counterfeits bills by the trillion.

Every US dollar printed is proof of time stolen—a visualization of US national debt gives us some sense of just how colossal the central banking system of institutionalized time-theft has become:



The US national debt in physical fiat dollars. This rendering is from 2017; with US national debt now pushing \$26T, the Statue of Liberty would no longer be visible today.

Remember: society always slides towards slavery when a privileged few are able to produce money more cheaply than everyone else. As such, a free world is forever beyond reach before central banking is eliminated.

As sickening as it is ironic, George Floyd was pressured to use a counterfeit \$20 bill precisely because The Fed counterfeits US dollars at scale. Again, the economic character of money directly influences moral standards: fiat currency pyramid schemes are premised on proof-of-theft, which pushes people to rent-seek, steal, and deceive others to make ends meet. Inflation impacts the poorest among us the worst, which explains why the median wealth held by a black family in modern America is less than 10% of that held by a white family (\$17,000 to \$171,000) and falling. As Michael Krieger describes this systemic weaponization of debt-based currencies:

“rather than empowering people, it turns them into modern-day indentured servants endlessly stuck on a hamster wheel with little to no hope of getting off. This is not an accident, it’s a tried and tested tool which, when combined with incessant mass media propaganda, is an effective way of creating a submissive, confused, and desperate underclass.”

By buying Bitcoin, you are participating in a global protest against state-controlled currency pyramid schemes in a way that politicians cannot ignore—since money is the only voting system in which your voice cannot be muted.



Buy Bitcoin = bye bye slavemasters.

Although none of us were given the choice of what state to be born in, thanks to Satoshi Nakamoto we are all now free to choose our own money. The first step on this journey is self-education: it is no coincidence that state-owned curriculum teaches us nothing about the origins of money or how it works. Thankfully, the internet is a treasure trove of resources if you know where to look (check out some comprehensive reading [here](#), [here](#), [here](#), [here](#), [here](#), [here](#), [here](#), [here](#), and

[here](#)).

Again, free markets are economic games played for the purpose of finding truth, and market manipulators are lying cheaters. In this sense, the Fed is like a professional sports franchise that can effortlessly score points at the touch of a button: a malicious team that doesn’t play by the same rules as the rest of us. Facing an “invincible” opponent like this is clearly demoralizing for other players in the marketplace, who are constantly robbed no matter how well they play. Money is a game played for keeps, and it involves the highest

stakes imaginable—human freedom. Counterfeiting currency is a mechanism of slavery. By breaking the central bank dominion over money, Bitcoin is an emerging emancipatory force for a world suffering under fiat bondage.

Chasing Starlight

“I prayed for freedom for twenty years, but received no answer, until I prayed with my legs.” —Frederick Douglass

Making haste under starry skies, aided by stalwart abolitionists, escaped slaves in the Antebellum South risked everything to flee northward as they attempted to cross into the free states of Canada. Finding true north could be challenging at times, fortunately there were many clues — like moss growing on the north sides of trees or the northbound flight paths of migrating birds — that helped runaway slaves in their quests for freedom. Perhaps the most crucial of these clues was the North Star which, unlike other heavenly bodies, never changes position in the night sky.

Gaining stealth under the cover of darkness, intrepid former slaves relied upon the fixity of the North Star to light their pathway to liberty. Operating under conditions of dire uncertainty and never knowing who to trust, this celestial torch — a true lodestar — served as the guiding light for the Underground Railroad: a network of secret routes and safe-houses providing safe passage for runaway African Americans into Canada. Antislavery activists like Harriet Tubman supported this volunteer-based, flexible, and covert network that was so instrumental in undermining the heavily enforced institution of slavery in pre-Civil War America.



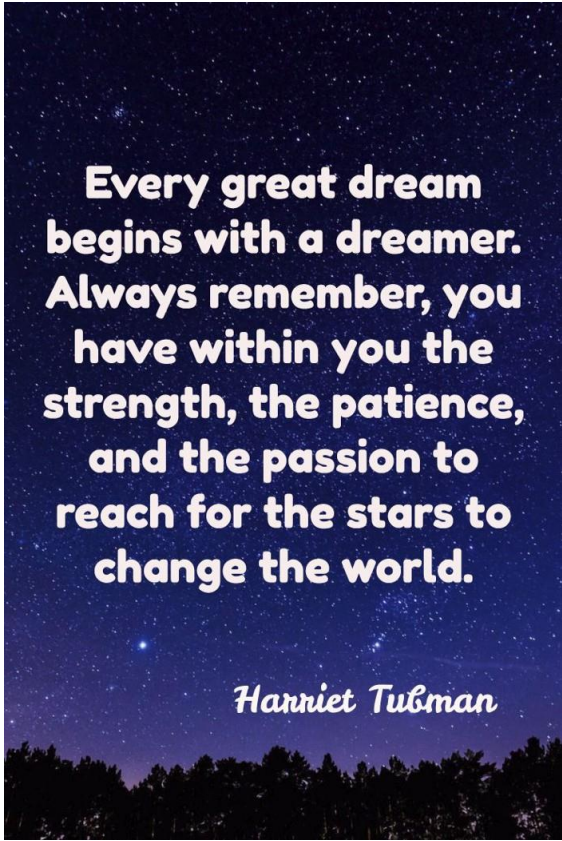
In modernity, we once again find hope of overcoming the financial slavery imposed upon us by The Fed in a volunteer-programmed, open-source, and cryptographically clandestine network guided by its own “North Star”: an immutable supply of 21 million bitcoin. For runaway African slaves, the North Star suspended high in the heavens beyond the reach of vengeful masters was a gift from God: an inextinguishable light for liberation. Bitcoin—a free market money with a supply firmly fixed at 21 million—is the unclosing gateway for fiat-slaves escaping economies controlled by central banking. Acceptance of Bitcoin is the manumission of humanity from central bank bondage, once and for all.

We are all living witnesses to the incineration of institutional falsity by unstoppable honest money. Bitcoin is a burning star of sincerity engulfing the enforced fiction of fiat currencies everywhere. From the ashes of this phoenix immolation, a society structured on the sound principles of accountability, honor, and integrity can arise. As an implementation of absolutely truthful money, it is a luminous beacon that cannot be coerced or concealed. As Buddha taught us:

“Three things cannot be long hidden: the sun, moon, and truth.”

Bitcoin is a rebellion against the most powerful bastion of socialism in the free world: central banking. It is a peaceful revolution involving the permanent disarmament of tyrants who weaponize money to confiscate wealth. Bitcoin is a weapon of peace; the final assassin to time-theft. An alchemical archetype, it is an antidote to state corruption and social moral affliction. As a purely honest free market money, Bitcoin is an irrepressible truth; an expression of pure monetary capitalism and a modern-day declaration of independence for fiat-slaves worldwide.

Bitcoin is money without masters: a system governed by rules instead of rulers. By awakening the world from the nightmare of financial slavery, Bitcoin is a dream of freedom coming true.

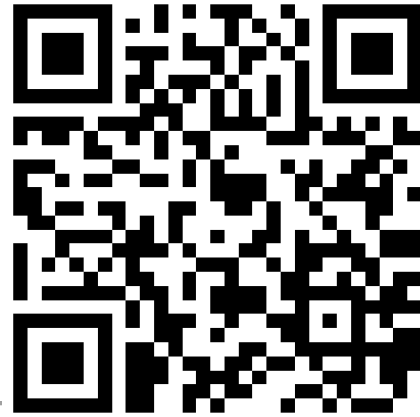


**Every great dream
begins with a dreamer.
Always remember, you
have within you the
strength, the patience,
and the passion to
reach for the stars to
change the world.**

Harriet Tubman

Thank you for reading *Masters and Slaves of Money*.

- Follow me on Twitter: <https://twitter.com/Breedlove22>
- Stack sats with me, get \$10 in free Bitcoin through this link: <https://www.swanbitcoin.com/breedlove>
- Journey with me as I write my first book: <https://bit.ly/3aWITZ5>
- If you enjoyed this, please send sats: <https://tippin.me/@Breedlove22>
- Or, send sats via Lightning Network with Strike: <https://strike.me/breedlove22>
- Or, send sats via PayNymID: +tightking693



Bitcoin accepted here:

3LzRt3a3aoPRuM6pex9ygLZPKR6xPsKPFQ

Translations:

- [Spanish](#)

Thank you for feedback during the writing process: [Jimmy Song](#) [Tuur Demeester](#) [Brandon Quittem](#) [Gigi Willem Van Den Bergh](#) [Stephen Cole](#) [Alex Gladstein](#) [PlanB](#) [Saifedean Ammous](#)

My sincerest gratitude to these amazing minds:

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

And anyone else I forgot :)

Sources:

a. <https://www.amazon.com/Bitcoin-Standard-Decentralized-Alternative-Central/dp/1119473861>

- b. <https://www.bdratings.org/l/tales-of-soft-money-cotton-on-cape-verde/>
- c. <https://www.smithsonianmag.com/smithsonianmag/nazis-planned-bomb-britain-forged-bank-notes-180958258/>
- d. https://en.wikipedia.org/wiki/Number_Nine_Research_Laboratory
- e. <https://pathways.thinkport.org/secrets/gourd1.cfm>
- f. <https://www.ssa.gov/oact/cola/awidevelop.html>
- g. <https://fred.stlouisfed.org/series/M2>
- h. <https://www.slavevoyages.org/assessment/estimates>
- i. <https://www.amazon.com/Heroes-History-Civilization-Ancient-Modern/dp/0743235940#ace-4302123154>
- j. <https://twitter.com/visualizevalue/status/1272736037673021441?s=21>
- k. <https://medium.com/@25stories/julian-s-dab-daily-audio-blog-session-37-million-vs-billion-vs-trillion-1ff8a17980bc>
- l. <https://www.visualcapitalist.com/20-trillion-of-u-s-debt-visualized-using-stacks-of-100-bills/>
- m. <https://blog.richmond.edu/livesofmaps/2014/11/11/map-of-the-week-slave-trade-from-africa-to-the-americas-1650-1860/>
- n. <https://projects.britishmuseum.org/pdf/RP%20171-%200%20Prelims%20rev.pdf>
- o. <https://projects.britishmuseum.org/pdf/RP%20171%20texts%201.pdf>
- p. <https://projects.britishmuseum.org/pdf/RP%20171%20texts%202.pdf>
- q. <https://projects.britishmuseum.org/pdf/RP%20171%20texts%203%20rev%20table.pdf>
- r. <https://www.bdratings.org/sources/>
- s. <https://libertyblitzkrieg.com/2020/02/18/financial-feudalism/>
- t. <https://i.redd.it/nj6mbq1dtrzl.jpg>
- u. <https://imrussia.org/en/nation/763-totalitarianism-and-freedom-of-speech>

Thanks to Tuur Demeester, Jimmy Song, Gigi, Willem Van Den Bergh, and Brandon Quitem.

Soft money, Soft minds.

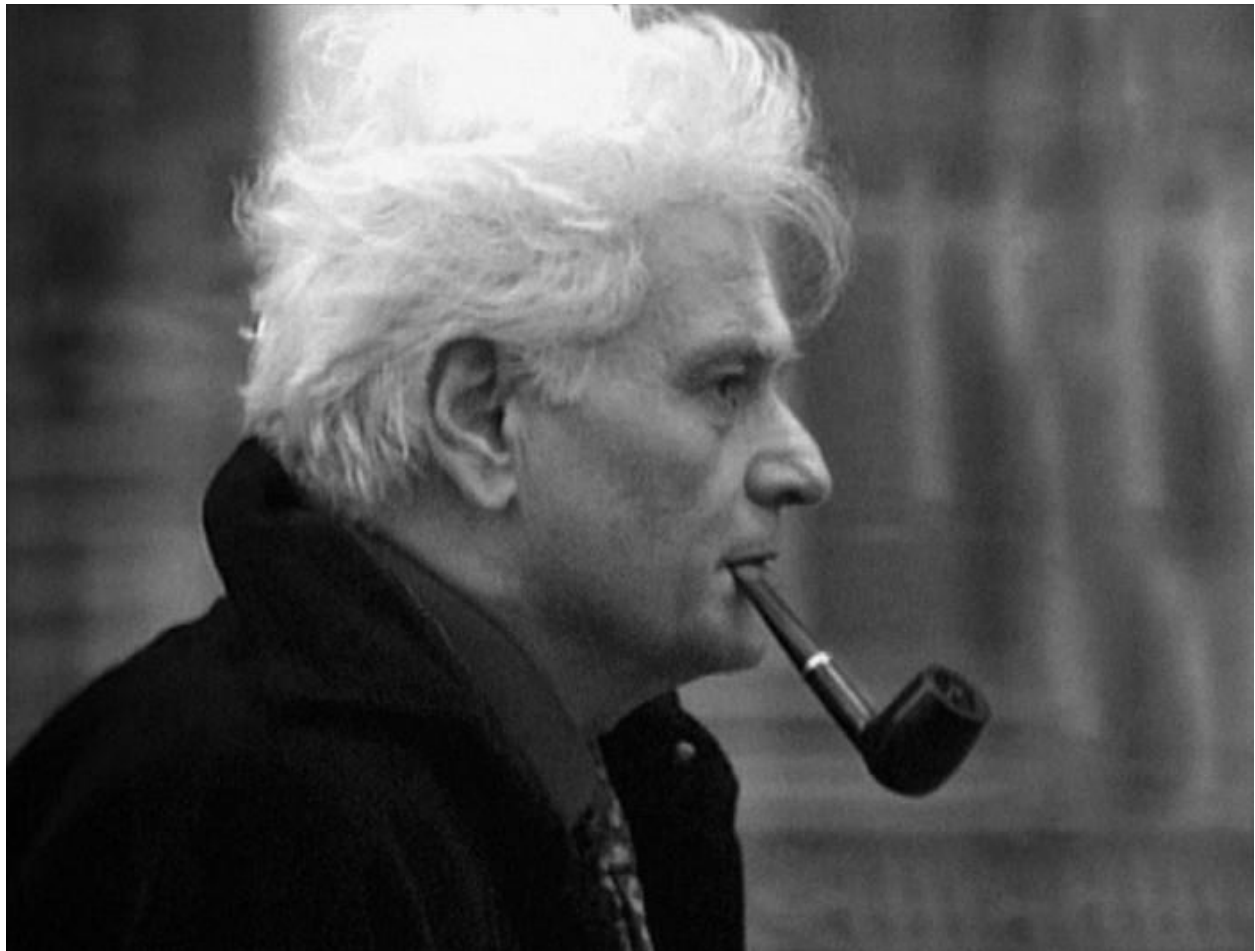
By American Hodl

Posted July 5, 2020

(How fiat currency power games emerged)

I've been trying to stitch this together for awhile in a way that is palatable for one with less background on the postmodern/critical/neomarxist religion, but here in summer 2020 I feel it's more or less self evident.

All the woke shit we're seeing recently can be traced back to one loser in particular named Jacques Derrida (of course he's French).



I could disparage Derrida for awhile, because frankly all his ideas are hot garbage. Jordan Peterson calls him the chief trickster behind modern wokeism. Plus he's french. Did I mention that? Immediate disqualifier.

So what do you need to know about him? Derrida is the philosophical father of deconstructionism. A philosophy expounding (and I'm not kidding) that men with penises make society and so society is penis based and not constructed for the penis-less.

I could have said that in the faux intellectual terms like "phallogocentric" that Derrida is fond of using, but it's more fun the way I said it.

So what's a penis-less person to do in a society built for penises? Riot of course. Tear it asunder. That's the core tactic of postmodern theory and critical wokeness.

Ok so what the hell? How does a stupid theory from some pussy ass Frenchman like this get any traction at all?

I'd like to posit that there is nothing particularly special about Jacques here, stupid theories like this emerge from academia all the time. Derrida just had impeccable timing.

Derrida publishes his work in the mid 60's and by 1979 other scholars (also french 🇫🇷) have transformed the theory into post modernism. Post modernism is a more fleshed out version of deconstructionism that has political action attached to it. 40 years later and we're living through the woke hellscape of a digital and increasingly kinetic deconstructionist revolution.

So again... what the fuck?

As stupid as postmodernism is, I will submit that it is entirely rational and even predictable given the circumstances. Derrida just happened to be the right useful idiot at the right time. He's the first fiat philosopher.

Smack dab in the middle of this pioneering work on deconstructionism the world loses the gold standard in 1971. An intuitive feeling emerges amongst the global population...

"if the money is by decree? Who decrees it? Why not me? Why not my group? Where's our share? This isn't fair."

People wouldn't be able to give voice to this feeling if you asked them. They'd jibber jabber some nonsense at you about racism or classism. Despite being literal deconstructionists they fail to interrogate the dogma of money.

There must be some psychological error code in humans where we can't see what's wrong with our old dogma until we've replaced it with a new dogma.

So now the losers of the cantillion effect have a new operating system. Less of a revolution and more on an insurrection. They don't want to flip the board

over, they just want the historically “oppressed” to have their turn at the money spigot.

This is postmodernism. A dirty tricks campaign and a prevailing idealism that acts as cover story for the money grab.

A fiat power grab.

Why do so many people within the ideology seem so blind to it then? In evolutionary game theory deception confers massive advantage and self deception is the best way to achieve that deception.

You can do terrible things if you convince yourself you’re the good guy. This is why I am scared of the permissive attitude towards violence on the left.

This isn’t just a behavior of the far left either, Reagan era deregulationists went for a massive fiat power grab when they realized that economic growth had slowed. They prioritized growth for the rich (trickle down) because it was easier to do and they directly benefited. Deregulation with a fiat currency is socialism for the rich. They are no better than these leftist morons.

Do I blame any of these people. Not really. Don’t hate the player, hate the game I suppose.

I think the neo-marxists and I would agree on every symptom of decay in our society, but disagree on root cause and treatments.

The effective treatment is to opt out. Back to a fair system where no group has their fingers on the levers of monetary power. We need to flip the board over.

Trust me, you don’t want to inherit the ash pile. The fiat experiments reactor core is melting and the appropriate move is not to change who sits at the control board. The appropriate move is to get the fuck out as fast as possible. Otherwise you’re toast.

The center cannot hold.

Protect yourself, buy bitcoin.

Bitcoin is more like ham radio than the early internet

By JP Koning

Posted July 10, 2020



People in the bitcoin community often make fun of me as a *nocoiner*. That is, I don't have any bitcoins and am vocal about that fact. (Neither of which is true, by the way).

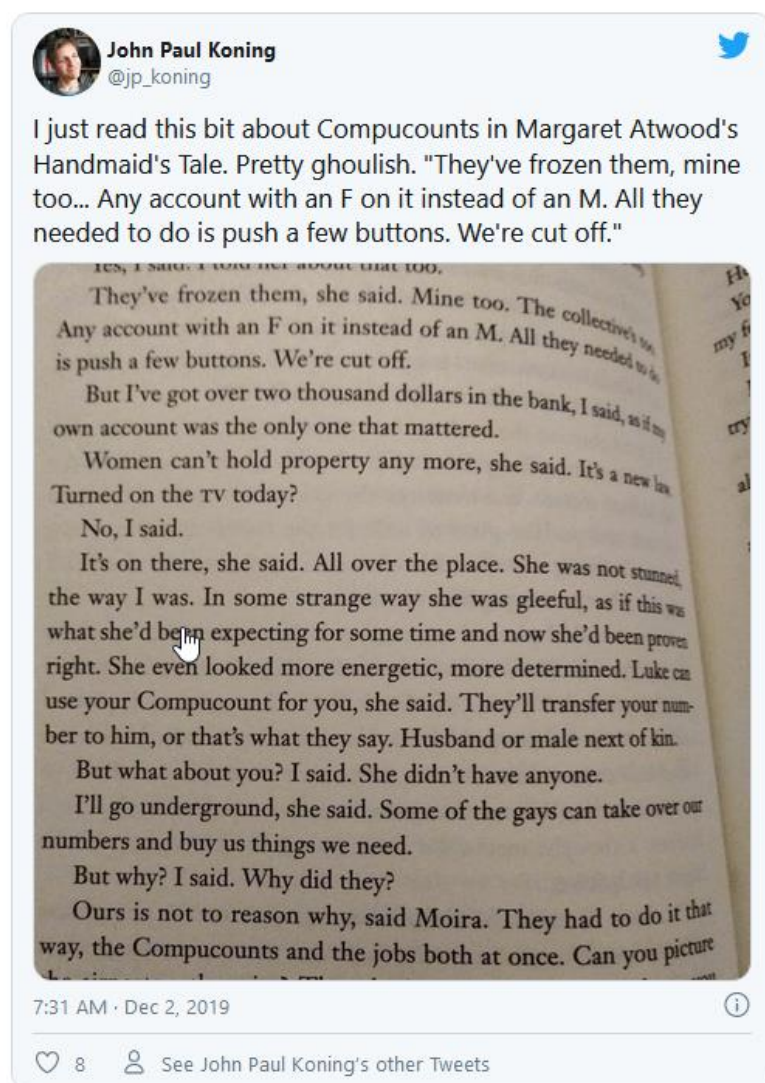
The truth is that I have no problem with bitcoin. It is a solid protocol that has survived handily for eleven years. When I come off as being critical, it's usually because I'm attacking the various narratives, or fan fictions, that have sprung up around bitcoin. Don't get me wrong, all movements rely on some sort of internal mythology to help drive their progress. Bitcoin is no different in this respect. But there is a big difference between accurate self-perception and fantasy.

Bitcoin's wrongest narratives are its triumphal ones. Most of them paint bitcoin as some sort of *heir apparent*, waiting on the wings to inevitably replace regular money: Bitcoin is the internet in 1991, just on the cusp of mass adoption... Bitcoin is email... Hyperbitcoinization is one year away... Bitcoin as monetary revolution...etc. I'm sure you've run into these proclamations.

No, bitcoin isn't going to become a mainstream kind of money. It's too awkward for most people. Crazy price gyrations are far too wicked for the regular money-using public to tolerate.

Nor should bitcoiners want bitcoin to go mainstream.

If five years from now everyone in the world has become a bitcoin user, that could only be because something very very bad has happened to the regular monetary system. Perhaps hostile aliens have enslaved us and are using the payments system to control what we can buy, sort of like Margaret Atwood's Compucounts in her dystopic *Handmaid's Tale*. And so bitcoin has gone mainstream, but only because we have all been forced to become under-the-table bitcoin users in order to buy stuff we need.



Surely no bitcoiner would actually want such a dark future.

I think the ham radio community provides bitcoiners with fertile ground for cultural appropriation. As I suggest in my recent Coindesk article, Bitcoin and ham radio are quite similar. They are both clunky and *old-fangled*. Neither technology is particularly easy to use relative to more mainstream options: ham radio's user experience is trumped by Whatsapp's, and Zelle is smoother to use than bitcoin. Go to Youtube and you'll find thousands of videos explaining how each technology works.

The very feature that makes both ham and bitcoin so confusing is also its strength. They are both decentralized. That is, neither relies on a single omnipresent service provider. Rather, the actual user is 100%

in charge of operating the tool. No account necessary. This lack of a gate keeper means that there is no one to soften the user experience. It also means that *no one* can be excluded from broadcasting a radio message, or transferring some bitcoins. That's a neat feature.

The ham radio community seems to be quite comfortable with its nicheness. Ham radio operators don't huddle together and talk about "overthrowing the totalitarian system of smart phones" or "displacing evil email." There is no *ham radio fixes this* meme on twitter.

And no wonder. If ham radio were to have gone mainstream by 2025, it would only be because some sort of massive natural disaster, say a meteor strike, has crippled all other forms of communication. No sane ham radio operator would wish this sort of doom scenario on the world.

When I was researching my Coindesk piece, I learned that there is a large **community service** element to ham radio. Hurricanes and other natural disaster often knock out cell phones and 911 call centres. As a robust decentralized communications network, independent ham radio operators become first responders. They locate desperate people and relay their needs on to emergency care providers. For instance, in the image below ham radio aficionado Josh Nass aka KI6NAZ is doing rounds of his neighborhood to see if any families have been knocked out by a (mock) disaster.



Source: Youtube

I really liked the ethos that Josh stands for. It's warm and cuddly and heroic. There also seems to be a good dose of humility among ham radio operators. The community thinks of itself as a group of civic-minded hobbyists, not revolutionaries on the cusp of tearing down the system.

Perhaps bitcoiners can learn from this. A hobbyist mentality is required to learn all the obscure things one must do with one's bitcoins: how to custody one's own keys, make bitcoin transactions, run a node, and set up Lightning. Between kids and jobs, most people won't have the time. Or maybe we're just lazy. When the regular monetary & payments system is compromised, say Visa or Zelle or Swish have gone down, perhaps these bitcoin hobbyists—like

their ham radio cousins—can leap into action and help others by enabling them to route transactions around the blockages.

Better this sort of narrative than to be fooled by fantasies saying that bitcoin is destined to rule the world. In the long run, bad narratives lead to disillusionment, and disillusionment kills a movement.

To sum up, bitcoin isn't the next email. It seems more akin to ham radio, a civic-minded and wonkish hobby that comfortably exists alongside its more mainstream centralized cousins. When the regular payments system suffers from a rare interruption, that's bitcoin's turn in the spotlight. But when regular service is restored, it becomes a hobby again. And that's fine.

Accepting Scarcity: A Bitcoin Meditation

By Reed Womack

Posted July 11, 2020

This essay shall concern itself with the conceptual world. It does not address the mystical, non-conceptual world where language and limits do not apply. That world is equally true and equally worthy of investigation via meditation or mysticism, but for now, we concern ourselves only with the world of logic, language, and concepts.

Everything is Scarce:

The conceptual world is governed by scarcity. This scarcity is most obvious in the physical realm: there is a physical limit to the size of our universe, the width of our solar system, the diameter of our Earth, the length of your street, the height of your spouse, and the size of an atom.

Any physical object, no matter how large or small, necessarily ends. While some objects may appear to be more endless than other objects, their apparent limitlessness is merely a trick of perspective. You may be tricked into feeling that large, numerous objects like galaxies are less scarce than small, more intimate objects, (like pet fish), but in reality, all physical things are scarce. You may have two kids and your neighbor has ten kids. While you have fewer kids than your neighbor, both you and your neighbor have scarce kids. In the binary choice between unlimited and limited, all physical things are limited.

Non-physical objects (in Buddhism we call them mental objects) are also equally limited and scarce. While it is clear your cat has physical boundaries (its organs don't spill out to infinity) it is equally true, but less obvious that your conception of "cat" is also bounded. "Cat" has a limited meaning. Although, people may argue about the breadth of its definition, and each person may hold a slightly different mental boundary of what constitutes a cat, for each person, "cat" means something and necessarily implies some category of "non-cat." While we may convincingly disagree about whether a dog-fox hybrid is indeed a cat, we would still be arguing about whether one concept fits into the bounded category of another concept. The truth would remain that those categories have edges, even if we disagree on where those edges are.

So all physical objects and all mental objects are inherently scarce and limited. As much as you'd like any single concept or object to be infinite, it is not. Your body is limited, and the concept of your body is limited. Even words

that attempt to point toward the nonconceptual world (words like Love, G-d, Nirvana, Sublime) are limited and therefore have the boundaries inherent to all concepts. The limitation of concepts is well-known within Buddhism: Buddha once reminded his followers that his teachings were the finger pointing at the moon, not the moon itself.



Accepting Scarcity:

So the reality of the conceptual world is that it has limits. When we accept this scarcity, we accept reality as it is. When we ignore this scarcity or trick ourselves into believing it is infinite, we delude ourselves.

According to Buddhism, ignorance or delusion is one of the three causes of our suffering (the other two are attachment and aversion). So when we are deluded about reality, we perpetuate suffering. When we are aware of reality as it is, we avoid suffering. We all have stories from our lives of people who suffered because they have not accepted reality as it was: they did not accept a break-up and kept pleading to be taken back; they did not accept a death and kept wishing for their parent to return; they did not accept their current reputation and kept bragging to any who would listen. And likewise, we all know of people who can handle surprises and tragedies with tranquility and aplomb.

So accepting reality as it is, in this very moment, is paramount to avoiding suffering. This is not to say that life won't change, that you are resigned to a certain fate, or there is nothing to be done, quite to the contrary. We must just accept reality as it is now and start here, rather than fantasize about it.

And the reality is all things are scarce.

Unfortunately, we repeatedly and routinely delude ourselves about scarcity. We make hyperbolic statements about our physical objects — “The mountains are endless,” “There is always another fish in the sea,” “The Fed has infinite cash” — and about abstract concepts too — “his love is eternal” or “his compassion knows no bounds.” However, all of those concepts are misleading — even the infinite cash statement! While they may provoke the intended emotional response (a sense of vastness) given enough time, life forces people to learn that their previous conception of infinity was wrong. They get to the end of the mountain range, they finish the dishes, or they see their compassionate lover squash an ant. And at that moment, if they still cling to the concept of infiniteness, they suffer through the process of letting go of their wrong view.

To avoid deluding ourselves and to avoid the necessary suffering that arises when the reality of scarcity smacks us in the face, we should never conceive of anything as infinite, even if it appears very large. Even Murray Rothbard, my favorite writer, suffers from this slight delusion in his opus *Man, Economy, and State*. He writes,

“In the first place, all means are scarce, i.e., limited with respect to the ends that they could possibly serve. If the means are in unlimited abundance, then they need not serve as the object of attention of any human action. For example, the air in most situations is in unlimited abundance. It is therefore not a means and is not employed as a means to the fulfillment of ends. It need not be allocated, as time is, to the satisfaction of the more important ends, since it is sufficiently abundant for all human requirements. Air, then, though indispensable, is not a means, but a general condition of human action and human welfare.”

But it’s not just “*means*” that are scarce. Everything is scarce. Nothing is in unlimited abundance, not even the “general conditions” of air. Even if the air is so numerous that each molecule holds little value to humans, it only appears unlimited due to our narrow perspective. And if we hold this perspective for too long, we eventually cause suffering when air pollution begins to build up in cities, the buffalos go extinct, the frontier closes, or passenger pigeons disappear from the skies. Even if something is so vast that you die before you ever discover its scarcity, eventually someone will reach its end and they’ll have to suffer when waking up from the lie of infinity that you told them was true.



Training the mind to accept scarcity:

Fortunately, you can train your mind to accept scarcity, and doing so has innumerable benefits. Namely, you are better able to see reality as it really is, less likely to be deluded, and less likely to suffer the discomfort of waking up from your delusion.

Paying close attention to anything effectively trains your mind to see scarcity (one minor benefit of attention-training). So the closer you pay attention to a tree, the more you recognize that it is not like any other tree. The closer you pay attention to your lover, the more you see how no one could possibly replace her. Still, this scarcity is a felt sense. It is not verifiably nor logically true. It arises from a deeper place of intuition, and it is only sustained by consistent attention.

As soon as your attention drifts off the present moment awareness of the object, the object can delude you into believing its infiniteness. For instance, you can intuitively sense dollar bills are scarce by staring at a dollar bill for long enough, but you are not logically convinced of its scarcity. As soon as your mind drifts slightly, you start imagining loggers clearing the forests to run dollar printing presses full-steam, or the images of the Weimar Republic hyperinflation when people used dollar bills as fire-starter, and suddenly you're caught in an internal story where the sacred dollar bill in front of you transforms into just another dollar among infinite dollar bills.

Thus, all objects, fiat included, don't force you to see their logical scarcity unless you maintain strict attention.

That is all objects except Bitcoin. For Bitcoin represents a new object of meditation that can train one's logical mind to accept scarcity. Bitcoin is the first time a concept has such a clearly defined incontrovertible boundary: 21 million. Whereas I could imagine copies being made of other scarce objects (multiple Mona Lisas or Hope Diamonds), with Bitcoin, I cannot. No such copy can ever be created. The block reward schedule and incentive structure assure that. So staring deeply at Bitcoin protocol can train one's mind to accept scarcity not just as an intuitive truth but as an abiding logical truth.

As a meditative tool, Bitcoin meditation most resembles death meditations — both harness the conceptual mind to teach a concept, and neither transcend the conceptual realm. While many meditators grow comfortable with death simply by cultivating present-moment awareness, some find it helpful to train the logical mind to accept death by focusing on it directly. Then later when their minds drift to other topics, they can still remember their impending death and the death of all things. Bitcoin meditation is similar. By focusing on Bitcoin, you see absolute scarcity deeply, and then, even when your mind drifts to other things, you increasingly see the reality of scarcity everywhere.

So for me, it has provided a compelling meditation object. Aside from providing a long (though not endless) intellectual rabbit-hole, contemplating Bitcoin has, more noticeably, anchored my mind from drifting into delusions of infinity in every-day life. It has grounded me in conceptual reality. Even without sustained attention on Bitcoin, even when I lose my attention and get caught up in the stories of Bitcoin, those stories are not based on, nor have allusions to, infinity. (Bitcoin is just going to the moon, which is a set distance away).

While many other meditation objects (namely my breath) have provided me even deeper and more profound meditative training, Bitcoin has helped me understand the scarcity of conceptual reality more clearly, and I believe helped me sidestep a little suffering arising from my own delusions.

In the coming years, I look forward to watching Bitcoin train my logical mind even more, but for now, it's back to my breath.

The Path to Taproot Activation

By [almkglor](#)

Posted June 13, 2020

Taproot! Everybody wants to have it, somebody wants to make it, nobody knows how to get it!

(If you are asking why everybody wants it, see: [Technical: Taproot: Why Activate?](#))

(Pedants: I mostly elide over lockin times)

Briefly, Taproot is that neat new thing that gets us:

- Multisignatures (n-of-n, k-of-n) that are just 1 signature (1-of-1) in length!! (MuSig/Schnorr)
- Better privacy!! If all contract participants can agree, just use a multisignature. If there is a dispute, show the contract publicly and have the Bitcoin network resolve it (Taproot/MAST).
- Activation lets devs work get back to work on the even newer stuff like!!!
 - Cross-input signature aggregation!! (transaction with multiple inputs can have a single signature for all inputs) — needs Schnorr, but some more work needed to ensure that the interactions with SCRIPT are okay.
 - Block validation - Schnorr signatures for all taproot spends in a block can be validated in a single operation instead of for each transaction!! Speed up validation and maybe we can actually afford to increase block sizes (maybe)!!
 - `SIGHASH_ANYPREVOUT` - you know, for Decker-Russell-Osuntokun (“eltoo”) magic!!!
 - `OP_CHECKTEMPLATEVERIFY` - vaulty vaults without requiring storing signatures, just transaction details!!

So yes, let’s activate taproot!

The SegWit Wars

The biggest problem with activating Taproot is PTSD from the previous softfork, SegWit. Pieter Wuille, one of the authors of the current Taproot proposal, has consistently held the position that he will not discuss activation, and will accept whatever activation process is imposed on Taproot. Other developers have expressed similar opinions.

So what happened with SegWit activation that was so traumatic? SegWit used the BIP9 activation method. Let's dive into BIP9!

BIP9 Miner-Activated Soft Fork

Basically, BIP9 has a bunch of parameters:

- **bit** - A field in the block header, the `nVersion`, has a number of bits. By setting a particular bit, the miner making the block indicates that it has upgraded its software to support a particular soft fork. The **bit** parameter for a BIP9 activation is *which* bit in this `nVersion` is used to indicate that the miner has upgraded software for a particular soft fork.
- **timeout** - a time limit, expressed as an end date. If this timeout is reached without sufficient number of miners signaling that they upgraded, then the activation fails and Bitcoin Core goes back to the drawing board.

Now there are other parameters (**name**, **starttime**) but they are not anywhere near as important as the above two.

A number that is *not* a parameter, is 95%. Basically, activation of a BIP9 softfork is considered as actually succeeding if at least 95% of blocks in the last 2 weeks had the specified **bit** in the `nVersion` set. If less than 95% had this bit set before the **timeout**, then the upgrade fails and never goes into the network. This is not a parameter: it is a constant defined by BIP9, and developers using BIP9 activation cannot change this.

So, first some simple questions and their answers:

- Why not just set a day when everyone starts imposing the new rules of the softfork?
 - This was done classically (in the days when Satoshi was still among us). But this might argued to put too much power to developers, since there would be no way to reject an upgrade without possible bad consequences. For example, developers might package an upgrade that the users do not want, together with vital security bugfixes. Either you live without vital security bugfixes and hire some other developers to fix it for you (which can be difficult, presumably the best developers are already the ones working on the codebase) or you get the vital security bugfixes and implicitly support the upgrade you might not want.
 - Sure, you could fork the code yourself (the ultimate threat in the FOSS world) and hire another set of developers who aren't assholes to do the dreary maintenance work of fixing security

- bugs, but Bitcoin needs strong bug-for-bug compatibility so everyone should really congregate around a single codebase.
- Basically: even the devs do not want this power, because they fear being coerced into putting “upgrades” that are detrimental to users. Satoshi got a pass because nobody knew who he was and how to coerce him.
 - Why 95%?
 - Suppose the threshold were lower, like 51%. If so, after activation, somebody can disrupt the Bitcoin network by creating a transaction that is valid under the pre-softfork rules, but are invalid under the post-softfork rules. Upgraded nodes would reject it, but 49% of miners would accept it and include it in a block (which makes the block invalid) And *then* the same 49% would accept the invalid block and build on top of *that*, possibly creating a short chain of doomed invalid blocks that confirm an invalid spend. This can confuse SPV wallets, who might see multiple confirmations of a transaction and accept the funds, but later find that in fact it is invalid under the now-activated softfork rules.
 - Thus, a very high threshold was imposed. 95% is considered safe. 50% is definitely not safe. Due to variance in the mining process, 80% could also be potentially unsafe (i.e. 80% of blocks signaling might have a good chance of coming from only 60% of miners), so a threshold of 95% was considered “safe enough for Bitcoin work”.
 - Why have a **timeout** that *disables* the upgrade?
 - Before BIP9, what was used was either flag day or BIP34. BIP34 had no flag day of activation or a **bit**, instead, it was just a 95% threshold to signal an `nVersion` value greater than a specific value. Actually, it was two thresholds: at 75%, blocks with the new `nVersion` would have the new softfork rules imposed, but at 95% blocks with the old `nVersion` would be rejected (and only the new blocks, with the new softfork rules, were accepted). For one, between 75% and 95%, there was a situation where the softfork was only “partially imposed”, only blocks signaling the new rules would actually have those rules, but blocks with the old rules were still valid. This was fine for BIP34, which only added rules for miners with negligible use for non-miners.
 - The same activation process for BIP34 was used for BIP66. After BIP66 reached 95%, however, a single miner mined an invalid-for-BIP66 block that still signalled BIP66 support. It turned out that of the 95% signaling BIP66 support, only about 50% were actually imposing the BIP66 new rules. The rest signalled support *without*

upgrading their software to support new rules. This led to many chainsplits and chaos with SPV nodes.

- The reasons miners signalled support was because they felt they were being pressured to signal support. So they signalled support, with plans to actually upgrade later, but because of the widespread signalling, the new BIP66 version locked in *before* upgrade plans were finished. Thus, the timeout that *disables* the upgrade was added in BIP9 to allow miners an escape hatch.

The Great Battles of the SegWit Wars

SegWit not only fixed transaction malleability, it also created a practical softforkable blocksize increase that also rebalanced weights so that the cost of spending a UTXO is about the same as the cost of creating UTXOs (and spending UTXOs is “better” since it limits the size of the UTXO set that every fullnode has to maintain).

So SegWit was written, the activation was decided to be BIP9, and then.... miner signalling stalled at below 75%.

Thus were the Great SegWit Wars started.

BIP9 Feature Hostage

If you are a miner with at least 5% global hashpower, you can hold a BIP9-activated softfork hostage.

You might even secretly *want* the softfork to actually push through. But you might want to extract concession from the users and the developers. Like removing the halvening. Or raising or even removing the block size caps (which helps larger miners more than smaller miners, making it easier to become a bigger fish that eats all the smaller fishes). Or whatever.

With BIP9, you *can* hold the softfork hostage. You just hold out and refuse to signal. You tell everyone you will signal, if and only if certain concessions are given to you.

This ability by miners to hold a feature hostage was enabled because of the miner-exit allowed by the **timeout** on BIP9. Prior to that, miners were considered little more than expendable security guards, paid for the risk they take to secure the network, but not special in the grand scheme of Bitcoin.

Covert ASICBoost

ASICBoost was a novel way of optimizing SHA256 mining, by taking advantage of the structure of the 80-byte header that is hashed in order to

perform proof-of-work. The details of ASICBoost are out-of-scope here but you can [read about it elsewhere](#)

Here is a short summary of the **two** types of ASICBoost, relevant to the activation discussion.

- Overt ASICBoost - Manipulates the unused bits in `nVersion` to reduce power consumption in mining.
- Covert ASICBoost - Manipulates the order of transactions in the block to reduce power consumption in mining.

Now, “overt” means “obvious”, while “covert” means hidden. Overt ASICBoost is obvious because `nVersion` bits that are not currently in use for BIP9 activations are usually 0 by default, so setting those bits to 1 makes it obvious that you are doing something weird (namely, Overt ASICBoost). Covert ASICBoost is non-obvious because the order of transactions in a block are up to the miner anyway, so the miner rearranging the transactions in order to get lower power consumption is not going to be detected.

Unfortunately, while Overt ASICBoost was compatible with SegWit, Covert ASICBoost **was not**. This is because, pre-SegWit, only the block header Merkle tree committed to the transaction ordering. However, with SegWit, another Merkle tree exists, which commits to transaction ordering as well. Covert ASICBoost would require more computation to manipulate two Merkle trees, obviating the power benefits of Covert ASICBoost anyway.

Now, miners want to use ASICBoost (indeed, about 60->70% of current miners probably use the Overt ASICBoost nowadays; if you have a Bitcoin fullnode running you will see the logs with lots of “60 of last 100 blocks had unexpected versions” which is exactly what you would see with the `nVersion` manipulation that Overt ASICBoost does). But remember: ASICBoost was, at around the time, a **novel** improvement. Not all miners had ASICBoost hardware. Those who did, did not want it known that they had ASICBoost hardware, and wanted to do Covert ASICBoost!

But Covert ASICBoost is incompatible with SegWit, because SegWit actually has two Merkle trees of transaction data, and Covert ASICBoost works by fudging around with transaction ordering in a block, and recomputing two Merkle Trees is more expensive than recomputing just one (and loses the ASICBoost advantage).

Of course, those miners that wanted Covert ASICBoost did not want to **openly admit** that they had ASICBoost hardware, they wanted to keep their advantage secret because miners are strongly competitive in a very tight market. And doing ASICBoost Covertly was just the ticket, but they could not work post-SegWit.

Fortunately, due to the BIP9 activation process, they could hold SegWit hostage while covertly taking advantage of Covert ASICBoost!

UASF: BIP148 and BIP8

When the incompatibility between Covert ASICBoost and SegWit was realized, still, activation of SegWit stalled, and miners were still not openly claiming that ASICBoost was related to non-activation of SegWit.

Eventually, a new proposal was created: BIP148. With this rule, 3 months before the end of the SegWit **timeout**, nodes would reject blocks that did *not* signal SegWit. Thus, 3 months before SegWit **timeout**, BIP148 would force activation of SegWit.

This proposal was not accepted by Bitcoin Core, due to the shortening of the timeout (it effectively times out 3 months before the initial SegWit timeout). Instead, a fork of Bitcoin Core was created which added the patch to comply with BIP148. This was claimed as a User Activated Soft Fork, UASF, since users could freely download the alternate fork rather than sticking with the developers of Bitcoin Core.

Now, BIP148 effectively is just a BIP9 activation, except at its (earlier) timeout, the new rules would be activated anyway (instead of the BIP9-mandated behavior that the upgrade is cancelled at the end of the **timeout**).

BIP148 was actually inspired by the BIP8 proposal (the link here is a historical version; BIP8 has been updated recently, precisely in preparation for Taproot activation). BIP8 is basically BIP9, but at the end of **timeout**, the softfork is activated anyway rather than cancelled.

This removed the ability of miners to hold the softfork hostage. At best, they can delay the activation, but not stop it entirely by holding out as in BIP9.

Of course, this implies risk that not all miners have upgraded before activation, leading to possible losses for SPV users, as well as again re-pressuring miners to signal activation, possibly without the miners actually upgrading their software to properly impose the new softfork rules.

BIP91, SegWit2X, and The Aftermath

BIP148 inspired countermeasures, possibly from the Covert ASICBoost miners, possibly from concerned users who wanted to offer concessions to miners. To this day, the common name for BIP148 - UASF - remains an emotionally-charged rallying cry for parts of the Bitcoin community.

One of these was SegWit2X. This was brokered in a deal between some Bitcoin personalities at a conference in New York, and thus part of the so-called “New York Agreement” or NYA, another emotionally-charged acronym.

The text of the NYA was basically:

1. Set up a new activation threshold at 80% signalled at bit 4 (vs bit 1 for SegWit).
 - When this 80% signalling was reached, miners would require that bit 1 for SegWit be signalled to achieve the 95% activation needed for SegWit.
2. If the bit 4 signalling reached 80%, increase the block weight limit from the SegWit 4000000 to the SegWit2X 8000000, 6 months after bit 1 activation.

The first item above was coded in [BIP91](#).

Unfortunately, if you read the BIP91, *independently* of NYA, you might come to the conclusion that BIP91 was only about lowering the threshold to 80%. In particular, BIP91 never mentions anything about the second point above, it never mentions that bit 4 80% threshold would *also* signal for a later hardfork increase in weight limit.

Because of this, even though there are claims that NYA (SegWit2X) reached 80% dominance, a close reading of BIP91 shows that the 80% dominance was only for SegWit activation, without necessarily a later 2x capacity hardfork (SegWit2X).

This ambiguity of bit 4 (NYA says it includes a 2x capacity hardfork, BIP91 says it does not) has continued to be a thorn in blocksize debates later.

Economically speaking, Bitcoin futures between SegWit and SegWit2X showed strong economic dominance in favor of SegWit (SegWit2X futures were traded at a fraction in value of SegWit futures: I personally made a tidy but small amount of money betting against SegWit2X in the futures market), so suggesting that NYA achieved 80% dominance even in mining is laughable, but the NYA text that ties bit 4 to SegWit2X still exists.

Historically, BIP91 triggered which caused SegWit to activate before the BIP148 shorter timeout. BIP148 proponents continue to hold this day that it was the BIP148 shorter timeout and no-compromises-activate-on-August-1 that made miners flock to BIP91 as a face-saving tactic that actually **removed** the second clause of NYA. NYA supporters keep pointing to the bit 4 text in the NYA and the historical activation of BIP91 as a failed promise by Bitcoin developers.

Taproot Activation Proposals

There are two primary proposals I can see for Taproot activation:

1. BIP8.
2. Modern Softfork Activation.

We have discussed BIP8: roughly, it has **bit** and **timeout**, if 95% of miners signal **bit** it activates, at the end of **timeout** it activates. (EDIT: BIP8 has had recent updates: at the end of **timeout** it can now activate or fail. For the most part, in the below text “BIP8”, means BIP8-and-activate-at-timeout, and “BIP9” means BIP8-and-fail-at-timeout)

So let’s take a look at Modern Softfork Activation!

Modern Softfork Activation

This is a more complex activation method, composed of BIP9 and BIP8 as supcomponents.

1. First have a 12-month BIP9 (fail at timeout).
2. If the above fails to activate, have a 6-month discussion period during which users and developers and miners discuss whether to continue to step 3.
3. Have a 24-month BIP8 (activate at timeout).

The total above is 42 months, if you are counting: 3.5 years worst-case activation.

The logic here is that if there are no problems, BIP9 will work just fine anyway. And if there are problems, the 6-month period should weed it out. Finally, miners cannot hold the feature hostage since the 24-month BIP8 period will exist anyway.

PSA: Being Resilient to Upgrades

Software is very brittle.

Anyone who has been using software for a long time has experienced something like this:

1. You hear a new version of your favorite software has a nice new feature.
2. Excited, you install the new version.
3. You find that the new version has subtle incompatibilities with your current workflow.
4. You are sad and downgrade to the older version.

5. You find out that the new version has changed your files in incompatible ways that the old version cannot work with anymore.
6. You tearfully reinstall the newer version and figure out how to get your lost productivity now that you have to adapt to a new workflow

If you are a technically-competent user, you might codify your workflow into a bunch of programs. And then you upgrade one of the external pieces of software you are using, and find that it has a subtle incompatibility with your current workflow which is based on a bunch of simple programs you wrote yourself. And if those simple programs are used as the basis of some important production system, you hve just screwed up because you upgraded software on an important production system.

And well, one of the issues with new softfork activation is that if not enough people (users and miners) upgrade to the newest Bitcoin software, the security of the new softfork rules are at risk.

Upgrading software of any kind is always a risk, and the more software you build on top of the software-being-upgraded, the greater you risk your tower of software collapsing while you change its foundations.

So if you have some complex Bitcoin-manipulating system with Bitcoin somewhere at the foundations, consider running two Bitcoin nodes:

1. One is a “stable-version” Bitcoin node. Once it has synced, set it up to `connect=x.x.x.x` to the second node below (so that your ISP bandwidth is only spent on the second node). Use this node to run all your software: it’s a stable version that you don’t change for long periods of time. Enable `txiindex`, disable pruning, whatever your software needs.
2. The other is an “always-up-to-date” Bitcoin Node. Keep its stoarge down with pruning (initially sync it off the “stable-version” node). You can’t use `blocksonly` if your “stable-version” node needs to send transactions, but otherwise this “always-up-to-date” Bitcoin node can be kept as a low-resource node, so you can run both nodes in the same machine.

When a new Bitcoin version comes up, you just upgrade the “always-up-to-date” Bitcoin node. This protects you if a future softfork activates, you will only receive valid Bitcoin blocks and transactions. Since this node has nothing running on top of it, it is just a special peer of the “stable-version” node, any software incompatibilities with your system software do not exist.

Your “stable-version” Bitcoin node remains the same version until you are ready to actually upgrade this node and are prepared to rewrite most of the software you have running on top of it due to version compatibility problems.

When upgrading the “always-up-to-date”, you can bring it down safely and then start it later. Your “stable-version” will keep running, disconnected from the network, but otherwise still available for whatever queries. You do need some system to stop the “always-up-to-date” node if for any reason the “stable-version” goes down (otherwise if the “always-up-to-date” advances its pruning window past what your “stable-version” has, the “stable-version” cannot sync afterwards), but if you are technically competent enough that you *need* to do this, you are technically competent enough to write such a trivial monitor program (EDIT: [gmax notes](#) you can adjust the pruning window by RPC commands to help with this as well).

This recommendation is from [gmaxwell](#) on IRC, by the way.

Taproot: Why Activate?

By [almkglor](#)

Posted June 15, 2020

This is a follow-up on https://old.reddit.com/r/Bitcoin/comments/hqzpl4/technical_the_path_to_taproot_activation/

Taproot! Everybody wants it!! But... you might ask yourself: sure, everybody **else** wants it, but why would *I*, sovereign Bitcoin HODLer, want it? Surely I can be better than everybody **else** because I swapped XXX fiat for Bitcoin unlike all those nocoiners?

And it is important for you to know the reasons why you, o sovereign Bitcoiner, would want Taproot activated. After all, your nodes (or the nodes your wallets use, which if you are SPV, you hopefully can pester to your wallet vendor/implementor about) need to be upgraded in order for Taproot activation to actually succeed instead of becoming a hot sticky mess.

First, let's consider some principles of Bitcoin.

- You the HODLer should be the one who controls where your money goes. Your keys, your coins.
- You the HODLer should be able to coordinate and make contracts with other people regarding your funds.
- You the HODLer should be able to do the above without anyone watching over your shoulder and judging you.

I'm sure most of us here would agree that the above are very important principles of Bitcoin and that these are principles we would not be willing to remove. If anything, we would want those principles strengthened (especially the last one, financial privacy, which current Bitcoin is only sporadically strong with: you *can* get privacy, it just requires effort to do so).

So, how does Taproot affect those principles?

Taproot and Your /Coins

Most HODLers probably HODL their coins in singlesig addresses. Sadly, switching to Taproot would do very little for you (it gives a mild discount at spend time, at the cost of a mild increase in fee at receive time (paid by whoever sends to you, so if it's a self-send from a P2PKH or bech32 address, you pay for this); mostly a wash).

(technical details: a Taproot output is 1 version byte + 32 byte public key, while a P2WPKH (bech32 singlesig) output is 1 version byte + 20 byte public key hash, so the Taproot output spends 12 bytes more; spending from a P2WPKH requires revealing a 32-byte public key later, which is not needed with Taproot, and Taproot signatures are about 9 bytes smaller than P2WPKH signatures, but the 32 bytes plus 9 bytes is divided by 4 because of the witness discount, so it saves about 11 bytes; mostly a wash, it increases blockweight by about 1 virtual byte, 4 weight for each Taproot-output-input, compared to P2WPKH-output-input).

However, as your HODLings grow in value, you might start wondering if multisignature k-of-n setups might be better for the security of your savings. And it is in multisignature that Taproot starts to give benefits!

Taproot switches to using Schnorr signing scheme. Schnorr makes key aggregation – constructing a *single* public key from multiple public keys – almost as trivial as adding numbers together. “Almost” because it involves some fairly advanced math instead of simple boring number adding, but hey when was the last time you added up your grocery list prices by hand huh?

With current P2SH and P2WSH multisignature schemes, if you have a 2-of-3 setup, then to spend, you need to provide two different signatures from two different public keys. With Taproot, you can create, using special moon math, a single public key that represents your 2-of-3 setup. Then you just put two of your devices together, have them communicate to each other (this can be done airgapped, in theory, by sending QR codes: the software to do this is not even being built yet, but that’s because Taproot hasn’t activated yet!), and they will make a *single* signature to authorize any spend from your 2-of-3 address. That’s 73 witness bytes – 18.25 virtual bytes – of signatures you save!

And if you decide that your current setup with 1-of-1 P2PKH / P2WPKH addresses is just fine as-is: well, that’s the whole point of a *softfork*: backwards-compatibility; you can receive from Taproot users just fine, and once your wallet is updated for Taproot-sending support, you can send to Taproot users just fine as well!

(P2WPKH and P2WSH – SegWit v0 – addresses start with `bc1q`; Taproot – SegWit v1 – addresses start with `bc1p`, in case you wanted to know the difference; in bech32 `q` is 0, `p` is 1)

Now how about HODLers who keep all, or some, of their coins on custodial services? Well, any custodial service worth its salt would be doing *at least* 2-of-3, or probably something even bigger, like 11-of-15. So your custodial service, if it switched to using Taproot internally, could save a lot more (imagine an 11-of-15 getting reduced from 11 signatures to just 1!), which — we

can only hope! — should translate to lower fees and better customer service from your custodial service!

So I think we can say, very accurately, that the Bitcoin principle — that YOU are in control of your money — can only be helped by Taproot (if you are doing multisignature), and, because P2PKH and P2WPKH remain validly-usable addresses in a Taproot future, will not be harmed by Taproot. Its benefit to this principle might be small (it mostly only benefits multisignature users) but since it has no drawbacks with this (i.e. singlesig users can continue to use P2WPKH and P2PKH still) this is still a nice, tidy win!

(even singlesig users get a minor benefit, in that multisig users will now reduce their blockchain space footprint, so that fees can be kept low for everybody; so for example even if you have your single set of private keys engraved on titanium plates sealed in an airtight box stored in a safe buried in a desert protected by angry nomads riding giant sandworms because you're the frickin' Kwisatz Haderach, you still gain some benefit from Taproot)

And here's the important part: *if P2PKH/P2WPKH is working perfectly fine with you and you decide to never use Taproot yourself, Taproot will not affect you detrimentally*. First do no harm!

Taproot and Your Contracts

No one is an island, no one lives alone. Give and you shall receive. You know: by trading with other people, you can gain expertise in some obscure little necessity of the world (and greatly increase your productivity in that little field), and then trade the products of your expertise for necessities other people have created, all of you thereby gaining gains from trade.

So, contracts, which are basically enforceable agreements that facilitate trading with people who you do not personally know and therefore might not trust.

Let's start with a simple example. You want to buy some gewgaws from somebody. But you don't know them personally. The seller wants the money, you want their gewgaws, but because of the lack of trust (you don't know them!! what if they're scammers??) neither of you can benefit from gains from trade.

However, suppose both of you know of some entity that both of you trust. That entity can act as a trusted escrow. The entity provides you security: this enables the trade, allowing both of you to get gains from trade.

In Bitcoin-land, this can be implemented as a 2-of-3 multisignature. The three signatories in the multisignature would be you, the gewgaw seller, and the escrow. You put the payment for the gewgaws into this 2-of-3 multisignature address.

Now, suppose it turns out neither of you are scammers (whaaaaat!). You receive the gewgaws just fine and you're willing to pay up for them. Then you and the gewgaw seller just sign a transaction — you and the gewgaw seller are 2, sufficient to trigger the 2-of-3 — that spends from the 2-of-3 address to a singlesig the gewgaw seller wants (or whatever address the gewgaw seller wants).

But suppose some problem arises. The seller gave you gawgews instead of gewgaws. Or you decided to keep the gewgaws but not sign the transaction to release the funds to the seller. In either case, the escrow is notified, and if it can sign with you to refund the funds back to you (if the seller was a scammer) or it can sign with the seller to forward the funds to the seller (if you were a scammer).

Taproot helps with this: like mentioned above, it allows multisignature setups to produce only one signature, reducing blockchain space usage, and thus making contracts — which require multiple people, by definition, you don't make contracts with yourself — is made cheaper (which we hope *enables* more of these setups to happen for more gains from trade for everyone, also, moon and lambos).

(technology-wise, it's easier to make an n-of-n than a k-of-n, making a k-of-n would require a complex setup involving a long ritual with many communication rounds between the n participants, but an n-of-n can be done trivially with some moon math. You can, however, make what is effectively a 2-of-3 by using a three-branch SCRIPT: either 2-of-2 of you and seller, OR 2-of-2 of you and escrow, OR 2-of-2 of escrow and seller. Fortunately, Taproot adds a facility to embed a SCRIPT inside a public key, so you can have a 2-of-2 Taprooted address (between you and seller) with a SCRIPT branch that can instead be spent with 2-of-2 (you + escrow) OR 2-of-2 (seller + escrow), which implements the three-branched SCRIPT above. If neither of you are scammers (hopefully the common case) then you both sign using your keys and *never have to contact the escrow*, since you are just using the escrow public key without coordinating with them (because n-of-n is trivial but k-of-n requires setup with communication rounds), so in the “best case” where both of you are honest traders, you *also* get a privacy boost, in that the escrow never learns you have been trading on gewgaws, I mean ewww, gawgews are much better than gewgaws and therefore I now judge you for being a gewgaw enthusiast, you filthy gewgawer).

Taproot and Your Contracts, Part 2: Cryptographic Boogaloo

Now suppose you want to buy some data instead of things. For example, maybe you have some closed-source software in trial mode installed, and want to pay the developer for the full version. You want to pay for an activation code.

This can be done, today, by using an HTLC. The developer tells you the hash of the activation code. You pay to an HTLC, paying out to the developer if it reveals the preimage (the activation code), or refunding the money back to you after a pre-agreed timeout. If the developer claims the funds, it has to reveal the preimage, which is the activation code, and you can now activate your software. If the developer does not claim the funds by the timeout, you get refunded.

And you can do that, with HTLCs, today.

Of course, HTLCs do have problems:

- Privacy. Everyone scraping the Bitcoin blockchain can see any HTLCs, and preimages used to claim them.
 - This can be mitigated by using offchain techniques so HTLCs are never published onchain in the happy case. Lightning would probably in practice be the easiest way to do this offchain. Of course, there are practical limits to what you can pay on Lightning. If you are buying something expensive, then Lightning might not be practical. For example, the “software” you are activating is really the firmware of a car, and what you are buying is not the software really but the car itself (with the activation of the car firmware being equivalent to getting the car keys).
 - Even offchain techniques need an onchain escape hatch in case of unresponsiveness! This means that, if something bad happens during payment, the HTLC might end up being published onchain anyway, revealing the fact that some special contract occurred.
 - And an HTLC that is claimed with a preimage onchain will also publicly reveal the preimage onchain. If that preimage is really the activation key of a software then it can now be pirated. If that preimage is really the activation key for your newly-bought cryptographic car — well, not your keys, not your car!
- Trust requirement. You are trusting the developer that it gives you the hash of an actual valid activation key, without any way to validate that the activation key hidden by the hash is actually valid.

Fortunately, with Schnorr (which is enabled by Taproot), we can now use the Scriptless Script construction by [Andrew Poelstra](#). This Scriptless Script allows a new construction, the PTLC or Pointlocked Timelocked Contract. Instead of hashes and preimages, just replace “hash” with “point” and “preimage” with “scalar”.

Or as you might know them: “point” is really “public key” and “scalar” is really a “private key”. What a PTLC does is that, given a particular public key, the

pointlocked branch can be spent only if the spender reveals the private key of the given public key to you.

Another nice thing with PTLCs is that they are *deniable*. What appears onchain is just a single 2-of-2 signature between you and the developer/manufacturer. It's like a magic trick. This signature has no special watermarks, it's a perfectly normal signature (the pledge). However, from this signature, plus some data given to you by the developer/manufacturer (known as the *adaptor signature*) you can derive the private key of a particular public key you both agree on (the turn). Anyone scraping the blockchain will just see signatures that look just like every other signature, and as long as nobody manages to hack you and get a copy of the adaptor signature or the private key, they cannot get the private key behind the public key (point) that the pointlocked branch needs (the prestige).

(Just to be clear, the public key you are getting the private key from, is distinct from the public key that the developer/manufacturer will use for its funds. The activation key is different from the developer's onchain Bitcoin key, and it is the activation key whose private key you will be learning, not the developer's/manufacturer's onchain Bitcoin key).

So:

- Privacy: PTLCs are private even if done onchain. Nobody else can learn what the private key behind the public key is, except you who knows the adaptor signature that when combined with the complete onchain signature lets you know what the private key of the activation key is. Somebody scraping the blockchain will not learn the same information even if all PTLCs are done onchain!
 - Lightning is still useful for reducing onchain use, and will also get PTLCs soon after Taproot is activated, but even if something bad happens and a PTLC has to go onchain, it doesn't reveal anything!
- Trust issues can be proven more easily with a public-private keypair than with a hash-preimage pair.
 - For example, the developer of the software you are buying could provide a signature signing a message saying "unlock access to the full version for 1 day". You can check if feeding this message and signature to the program will indeed unlock full-version access for 1 day. Then you can check if the signature is valid for the purported pubkey whose private key you will pay for. If so, you can now believe that getting the private key (by paying for it in a PTLC) would let you generate any number of "unlock access to the full version for 1 day" message+signatures, which is equivalent to getting full access to the software indefinitely.

- For the car, the manufacturer can show that signing a message “start the engine” and feeding the signature to the car’s firmware will indeed start the engine, and maybe even let you have a small test drive. You can then check if the signature is valid for the purported pubkey whose privkey you will pay for. If so, you can now believe that gaining knowledge of the privkey will let you start the car engine at any time you want.
- (pedantry: the signatures need to be unique else they could be replayed, this can be done with a challenge-response sequence for the car, where the car gathers entropy somehow (it’s a car, it probably has a bunch of sensors nowadays so it can get entropy for free) and uses the gathered entropy to challenge you to sign a random number and only start if you are able to sign the random number; for the software, it could record previous signatures somewhere in the developer’s cloud server and refuse to run if you try to replay a previously-seen signature.)

Taproot lets PTLCs exist onchain because they enable Schnorr, which is a requirement of PTLCs / Scriptless Script.

(technology-wise, take note that Scriptless Script works only for the “pointlocked” branch of the contract; you need normal Script, or a pre-signed `nLockTime` transaction, for the “timelocked” branch. Since Taproot can embed a script, you can have the Taproot pubkey be a 2-of-2 to implement the Scriptless Script “pointlocked” branch, then have a hidden script that lets you recover the funds with an `OP_CHECKLOCKTIMEVERIFY` after the timeout if the seller does not claim the funds.)

Quantum Quibbles!

Now if you were *really* paying attention, you might have noticed this parenthetical:

(technical details: a Taproot output is 1 version byte + 32 byte public key, while a P2WPKH (bech32 singlesig) output is 1 version byte + 20 byte public key hash...)

So wait, Taproot uses raw 32-byte public keys, and not public key hashes? Isn’t that more quantum-vulnerable??

Well, in theory yes. In practice, they probably are not.

It’s not that hashes can be broken by quantum computes — they’re still not. Instead, you have to look at how you *spend from* a P2WPKH/P2PKH pay-to-public-key-hash.

When you *spend from* a P2PKH / P2WPKH, you have to reveal the public key. Then Bitcoin hashes it and checks if this matches with the public-key-hash, and only then actually validates the signature for that public key.

So an unconfirmed transaction, floating in the mempools of nodes globally, will show, in plain sight for everyone to see, your public key.

(public keys should be public, that's why they're called public keys, LOL)

And if quantum computers are fast enough to be of concern, then they are probably fast enough that, in the several minutes to several hours from broadcast to confirmation, they have already cracked the public key that is openly broadcast with your transaction. The owner of the quantum computer can now replace your unconfirmed transaction with one that pays the funds to itself. Even if you did not opt-in RBF, miners are still incentivized to support RBF on RBF-disabled transactions.

So the extra hash is not as significant a protection against quantum computers as you might think. Instead, the extra hash-and-compare needed is just extra validation effort.

Further, if you have ever, in the past, *spent from* the address, then there exists already a transaction indelibly stored on the blockchain, openly displaying the public key from which quantum computers can derive the private key. So those are still vulnerable to quantum computers.

For the most part, the cryptographers behind Taproot (and Bitcoin Core) are of the opinion that quantum computers capable of cracking Bitcoin pubkeys are unlikely to appear within a decade or two.

- Current quantum computers can barely crack prime factorization problem for primes of 5 bits.
- The 256-bit elliptic curve use by Bitcoin is, by my (possibly wrong) understanding, equivalent to 4096-bit primes, so you can see a pretty big gap between now (5 bit primes) and what is needed (4096 bit primes).
- A lot of financial non-Bitcoin systems use the equivalent of 3072-bit primes or less, and are probably easier targets to crack than the equivalent-to-4096-bit-primes Bitcoin.

So:

- Quantum computers capable of cracking Bitcoin are still far off.
- Pay-to-public-key-hash is not as protective as you might think.
- We will probably see banks get cracked before Bitcoin, so the banking system is a useful canary-in-a-coal-mine to see whether we should panic about being quantum vulnerable.

For now, the homomorphic and linear properties of elliptic curve cryptography provide a lot of benefits — particularly the linearity property is what enables Scriptless Script and simple multisignature (i.e. multisignatures that are just 1 signature onchain). So it might be a good idea to take advantage of them now while we are still fairly safe against quantum computers. It seems likely that quantum-safe signature schemes are nonlinear (thus losing these advantages).

Summary

- If you are a singlesig HODL-only Bitcoin user, Taproot will not affect you positively or negatively. Importantly: Taproot does no harm!
- If you use or intend to use multisig, Taproot will be a positive for you.
- If you transact onchain regularly using typical P2PKH/P2WPKH addresses, you get a minor reduction in fees since multisig users will likely switch to Taproot to get smaller tx sizes, freeing up blockspace for yours.
- If you are using multiparticipant setups for special systems of trade, Taproot will be a positive for you.
 - Remember: Lightning channels are multiparticipant setups for special systems of lightning-fast offchain trades!

I Wanna Be The Taprooter!

So, do you want to help activate Taproot? Here's what *you*, mister sovereign Bitcoin HODLer, can do!

- *If you have developer experience especially in C, C++, or related languages*
 - Review the Taproot code! There is one pull request in Bitcoin Core, and one in libsecp256k1. I deliberately am not putting links here, to avoid brigades of nontechnical but enthusiastic people leaving pointless reviews, but if you are qualified you know how to find them!
 - *But I am not a cryptographer/Bitcoin Core contributor/mathematician/someone as awesome as Pieter Wuille*
 - That's perfectly fine! The cryptographers have been over the code already and agree the math is right and the implementation is right. What is wanted is the dreary dreary dreary software engineering: are the comments comprehensive and understandable? no misspellings in the comments? variable names understandable? reasonable function naming convention? misleading coding style? off-by-one errors in loops?

conditions not covered by tests? accidental mixups of variables with the same types? missing frees? read-before-init? better test coverage of suspicious-looking code? missing or mismatching header guards? portability issues? consistent coding style? you know, stuff any coder with a few years of experience in coding *anything* might be able to catch. With enough eyes all bugs are shallow!

- *If you are running a mining pool/mining operation/exchange/custodial service/SPV server*
 - Be prepared to upgrade!
 - One of the typical issues with upgrading software is that subtle incompatibilities with your current custom programs tend to arise, disrupting operations and potentially losing income due to downtime. If so, consider moving to the two-node setup suggested by gmax, which is in the last section of [my previous post](#). With this, you have an up-to-date “public” node and a fixed-version “private” node, with the public node protecting the private node from any invalid chainsplits or invalid transactions. Moving to this setup from a typical one-node setup should be smooth and should not disrupt operations (too much).
- *If you are running your own fullnode for fun or for your own wallet*
 - Be prepared to upgrade! The more nodes validating the new rules (even if you are a non-mining node!), the safer every softfork will be!
- *If you are using an SPV wallet or custodial wallet/service (including hardware wallets using the software of the wallet provider)*
 - Contact your wallet provider / SPV server and ask for a statement on whether they support Taproot, and whether they are prepared to upgrade for Taproot! Make it known to them that Taproot is something you want!

But I Hate Taproot!!

That’s fine!

- Raise your objections to Taproot now, or forever hold your peace! Maybe you can raise them here and some of the devs (probably [/u/nullc](#), he goes everywhere, even in rbtc!) might be able to see your objections! Or if your objections are very technical, head over to the appropriate pull request and object away!
- Maybe you simply misunderstand something, and we can clarify it here!
- Or maybe you do have a good objection, and we can make Taproot better by finding a solution for it!

Discussions About Taproot Activation

- IRC logs for freenode.net ##taproot-activation:
<http://gnusha.org/taproot-activation>
 - Telegram group: https://t.me/bips_activation
 - Reddit:
https://old.reddit.com/r/Bitcoin/comments/hqzp14/technical_the_path_to_taproot_activation/
-

3 Reasons I'm Investing in Bitcoin

By Lyn Alden

Posted July 17, 2020

Blockchain-based cryptocurrencies have been around for over a decade, since the release of Bitcoin in early 2009.

While the asset class has grown considerably, it remains relatively small and highly volatile, so deciding whether to insert a small bit of Bitcoin or other cryptocurrency exposure into a portfolio allocation can be a controversial and confusing decision.

Maybe this article will assist some investors in the decision one way or the other. Bitcoin analysis online can be very polarizing; either written by hardcore bullish enthusiasts or dismissed as a worthless ponzi scheme. As a generalist investor with a value-slant and a global macro emphasis, I've sought to bridge the gap a bit by sharing my view of Bitcoin, which is currently bullish.

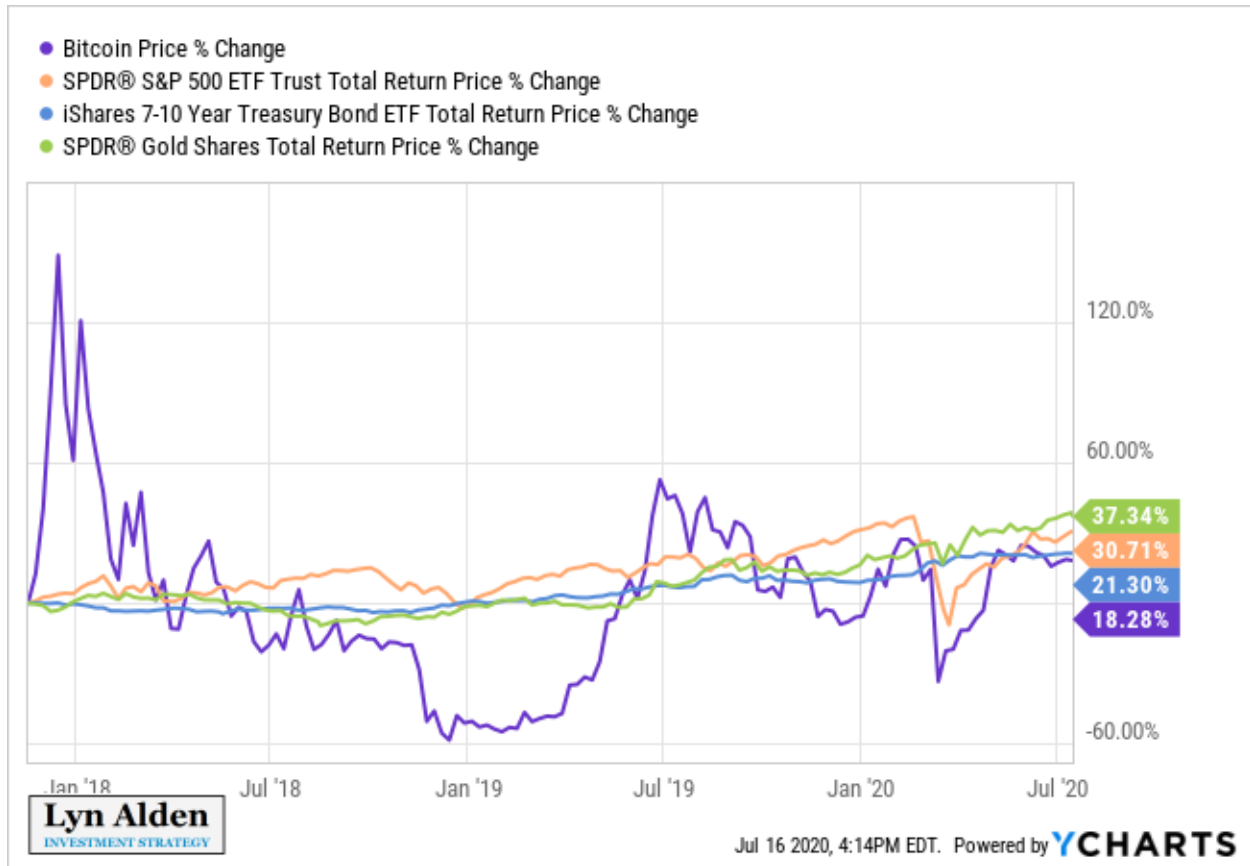
Although I was aware of Bitcoin as a speculative small asset since around 2011, and knew someone who mined it on her computer back when that was possible (now it requires application-specific integrated circuits, due to heavy competition), I wrote my [first article](#) on cryptocurrencies back in November 2017, when the price was in the \$6500-\$8000 range. During the week or two writing and editing period, the price rose substantially in that big range. My conclusion at the time was neutral-to-bearish, and I didn't buy any.

Right now, there's already a lot of optimism backed in; bitcoins and other major cryptocurrencies are extremely expensive compared to their estimated current usage. Investors are assuming that they will achieve widespread adoption and are paying up accordingly. That means investors should apply considerable caution.

-Lyn Alden, November 2017

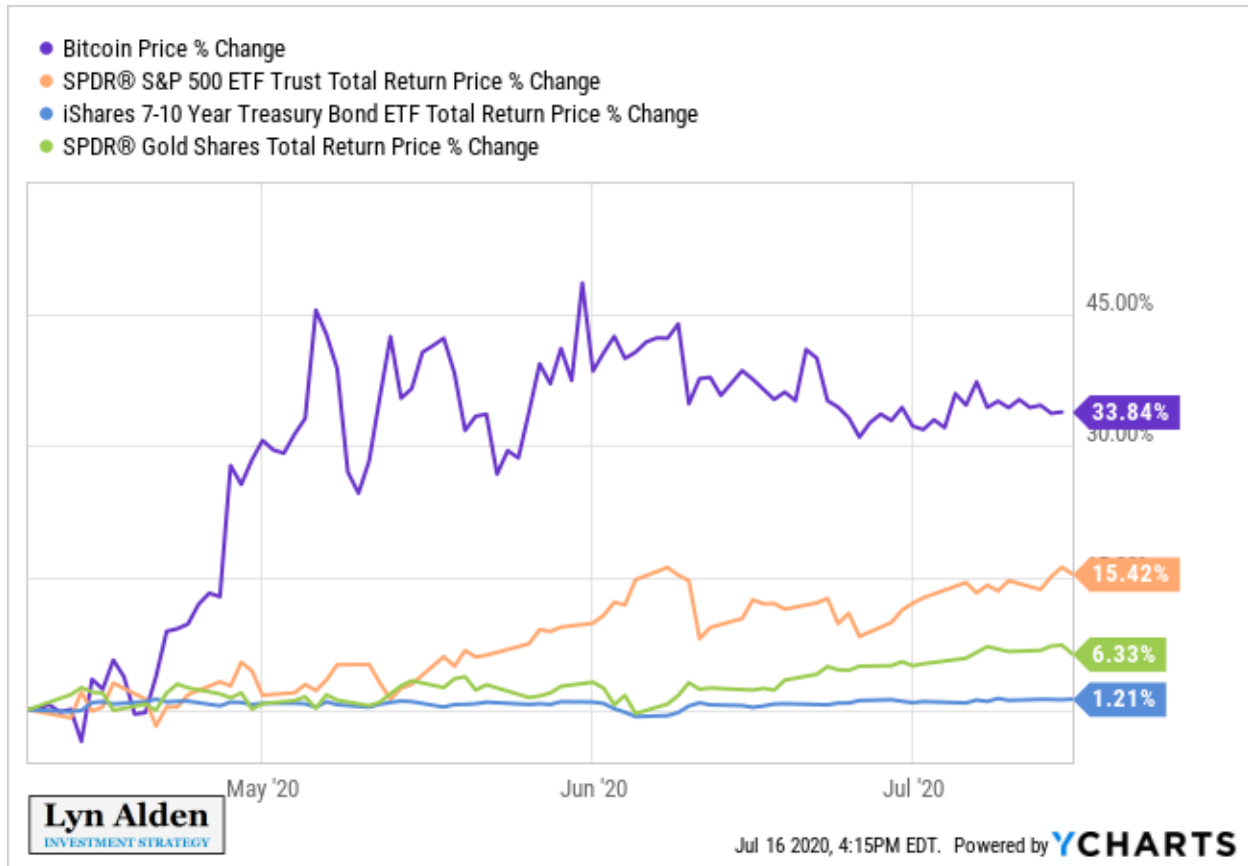
Within the next month or so after the original article, Bitcoin briefly soared to reach \$20,000, but then crashed down to below \$3,500 a year later, and has since recovered to bounce around in a wide trading range with little or no durable returns.

From the time of my original article nearly two and a half years ago, Bitcoin underperformed the S&P 500, gold, Treasury notes, and a variety of other asset classes, especially on a volatility-adjusted basis:



I've updated the article from time to time to refresh data and keep it relevant as changes happen in the industry, but other than keeping an eye on the space from time to time, I mostly ignored it.

In early 2020, I revisited Bitcoin and became bullish. I recommended it as a small position in my [premium research service](#) on April 12th, and bought some bitcoins for myself on April 20th. The price was around \$6,900 for that stretch of time. Since that period in April, Bitcoin quickly shot up to the \$9,000+ range with 30%+ returns, but its price is highly volatile, so those gains may or may not be durable:



My base case is for Bitcoin to perform very well over the next 2 years, but we'll see. I like it as a small position within a diversified portfolio, without much concern for periodic corrections, using capital I'm willing to risk.

As someone with an engineering and finance blended background, Bitcoin's design has always interested me from a theoretical point of view, but it wasn't until this period in early 2020 that I could put enough catalysts together to build a constructive case for its price action in the years ahead. As a new asset class, Bitcoin took time to build a price history and some sense of the cycles it goes through, and plenty of valuable research has been published over the years to synthesize the data.

So, I'm neither a perma-bull on Bitcoin at any price, or someone that dismisses it outright. As an investor in many asset classes, these are the three main reasons I switched from uninterested to quite bullish on Bitcoin early this year, and remain so today.

Reason 1) Scarcity + Network Effect

Bitcoin is an open source peer-to-peer software monetary system invented by an anonymous person or group named Satoshi Nakamoto that can store and transmit value.

It is decentralized; there is no singular authority that controls it, and instead it uses encryption based on blockchain technology, calculated by multiple parties on the network, to verify transactions and maintain the protocol. Incentives are given by the protocol to those that contribute computing power to verify transactions in the form of newly-“mined” coins, and/or transaction fees. In other words, by verifying and securing the blockchain, you earn some coins.

In the beginning, anyone with a decent computer could mine some coins. Now that many bitcoins have been mined and the market for mining coins has become very competitive, most people acquire coins simply by buying them from existing owners on exchanges and other platforms, while mining new coins is a specialized operation.

Bitcoin's protocol limits it to 21 million coins in total, which gives it scarcity, and therefore *potentially* gives it value... if there is demand for it. There is no central authority that can unilaterally change that limit; Satoshi Nakamoto himself couldn't add more coins to the Bitcoin protocol if he wanted to at this point. These coins are divisible into 100 million units each, like fractions of an ounce of gold.

For context, these “coins” aren't “stored” on any device. Bitcoin is a distributed public ledger, and owners of Bitcoin can access and transmit their Bitcoin from one digital address to another digital address, as long as they have their private key, which unlocks their encrypted address. Owners store their private keys on devices, or even on paper or engraved in metal.

In fact, a private key can be stored as a seed phrase that can be remembered, and later reconstructed. You could literally commit your seed phrase to memory, destroy all devices that ever had your private key, go across an international border with nothing on your person, and then reconstruct your ability to access your Bitcoin with the memorized seed phrase later that week.

A Digital Monetary Commodity

Satoshi envisioned Bitcoin as basically a rare commodity that has one unique property.

As a thought experiment, imagine there was a base metal as scarce as gold but with the following properties:

- boring grey in colour
- not a good conductor of electricity
- not particularly strong, but not ductile or easily malleable either
- not useful for any practical or ornamental purpose

and one special, magical property:

– can be transported over a communications channel

If it somehow acquired any value at all for whatever reason, then anyone wanting to transfer wealth over a long distance could buy some, transmit it, and have the recipient sell it.

-Satoshi Nakamoto, August 2010

So, Bitcoin can be thought of as a rare digital commodity that has unique attributes. Although it has no industrial use, it is scarce, durable, portable, divisible, verifiable, storable, fungible, salable, and recognized across borders, and therefore has the properties of money. Like all “potential” money, though, it needs sustained demand to have value.

As of this writing, Bitcoin’s market capitalization is about \$170 billion, or roughly the value of a large company. The total market capitalization of the entire cryptocurrency asset class is about \$270 billion, including Bitcoin as the dominant share. Here’s Bitcoin’s market capitalization chart:



One of my concerns with Bitcoin back in 2017 was that, even if we grant that these digital commodity attributes are useful, and even if we acknowledge that the units of any cryptocurrency are scarce by design, anyone can now create a brand new cryptocurrency. Since Satoshi figured out the mathematical and software methods to create digital scarcity (based in part on previous work by others) and made that knowledge public, and thus

solved the hard problems associated with it, any programmer and marketing team can now put together a new cryptocurrency.

There are thousands of them, now that the floodgate of knowledge has been opened. Some of them are optimized for speed. Some of them are optimized for efficiency. Some of them can be used for programmed contracts, and so forth.

So, rather than just one scarce “commodity” that has the unique property of being able to be transported over a network, there are thousands of similar commodities that have that new property. This risks the scarcity aspect of the commodity, and thus risks its value by potentially diluting it and dividing the community among multiple protocols. Each cryptocurrency is scarce, but there is no scarcity to the number of cryptocurrencies that can exist.

This is unlike, say, gold and silver. There are only a handful of elemental precious metals, they each have scarcity within the metal (200,000 tons of estimated mined gold, for example), and there is scarcity regarding how many elemental precious metals exist and they are all unique (silver, gold, platinum, palladium, rhodium, a few other rare and valuable elements and... that's it. Nature is not making more).

There is a ratio called “Bitcoin dominance” that measures what percentage of the total cryptocurrency market capitalization that Bitcoin has. When Bitcoin was created, it was the only cryptocurrency and thus had 100% market share. Following the rise of Bitcoin, now there are thousands of different cryptocurrencies. First there was a trickle of them, and then it became a flood.

By the end of 2017, during that peak enthusiasm period for cryptocurrencies, Bitcoin's market share briefly fell below 40%, even though it still remained the largest individual protocol. It has since risen back above 60% market share. Out of thousands of cryptocurrencies, Bitcoin has nearly two thirds of all cryptocurrency market share.

So, what gives individual cryptocurrencies potential value, is their network effect, which in Bitcoin's case is mainly derived from its first-mover advantage, which led to a security advantage.

An analogy is that a cryptocurrency is like a social network, except instead of being about self-expression, it's about storing and transmitting value. It's not hard to set up a new social network website; the code to do it is well understood at this point. Anyone can make one. However, creating the next Facebook (FB) or other billion-user network is a nearly impossible challenge, and a multi-billion-dollar reward awaits any team that somehow pulls it off. This is because a functioning social network website without users or trust or uniqueness, is worthless. The more people that use one, the more

people it attracts, in a self-reinforcing virtuous network effect, and this makes it more and more valuable over time.

Similarly, ever since Satoshi solved the hard parts of digital scarcity and published the method for the world to see, it's easy to make a new cryptocurrency. The nearly impossible part is to make one that is trusted, secure, and with sustained demand, which are all traits that Bitcoin has.

When I analyzed cryptocurrencies in 2017, I was concerned with cryptocurrency market share dilution. Bitcoin's market share was near its low point, and still falling. What if thousands of cryptocurrencies are created and used, and therefore none of them individually retain much value? Each one is scarce, but the total number of all of them is potentially infinite. Even if just ten protocols take off, that could pose a valuation problem. If the total cryptocurrency market capitalization grows to \$1 trillion, but is equally-divided among the top ten protocols for example, then that would be just \$100 billion in capitalization for each protocol.

In addition, there were some notable Bitcoin forks at the time, where Bitcoin Cash and subsequently Bitcoin Satoshi Vision were forked protocols of Bitcoin, that in theory could have split the community and market share. Ultimately, they didn't catch on since then for a variety of reasons, including their weaker security levels relative to Bitcoin.

Gold vs Bitcoin

This reliance on the network effect is not unique to Bitcoin or other cryptocurrencies. Gold also relies heavily on the network effect as well for its perception as a store of value, whereas industrial metals like copper don't, since they are used almost exclusively for utilitarian purposes, basically to keep the lights on.

Unlike Bitcoin, gold does have non-monetary industrial use, but only about 10% of its demand is industrial. The other 90% is based on bullion and jewelry demand, for which buyers view gold as a store of wealth, or a display of beauty and wealth, because it happens to have very good properties for it in the sense that it looks nice, doesn't rust, is very rare, holds a lot of value in a small space, is divisible, lasts forever, and so forth. If gold's demand for jewelry, coinage, and bars were to ever decrease substantially and structurally, leaving its practical industrial usage as its primary demand, the existing supply/demand balance would be thrown out and this would likely result in a much lower price.

In the West, interest in gold bullion has gradually declined somewhat over decades, while demand from the East for storing wealth has been strong. I

suspect the 2020's decade, due to monetary and fiscal policy, could renew western interest in gold, but we'll see.

So, the argument that Bitcoin isn't like gold because it can't be used for anything other than money, doesn't really hold up. Or more specifically, it's about 10% true, referring to gold's 10% industrial demand. With 90% of gold's demand coming from jewelry and bullion usage, which are based on perception and sentiment and fashion (all for good reason, based on gold's unique properties), gold would have similar problems to Bitcoin if there was ever a widespread loss of interest in it as a store of value and display of wealth.

Of course, gold's advantage is that it has thousands of years of international history as money, in addition to its properties that make it suitable for money, so the risk of it losing that perception is low, making it historically an extremely reliable store of value with less upside and less downside risk, but not inherently all that different.

The difference is mainly that Bitcoin is newer and with a smaller market capitalization, with more explosive upside and downside potential. And as the next section explains, a cryptocurrency's security is tied to its network effect, unlike precious metals.

Cryptocurrency Security is Tied to Adoption

A cryptocurrency's security is tied to its network effect, and specifically tied to the market capitalization that the cryptocurrency has. If the network is weak, a group with enough computing power could potentially override all other participants on the network, and take control of the blockchain ledger. Cryptocurrencies with a small market capitalization have a small hash rate, meaning they have a small amount of computing power that is constantly operating to verify transactions and support the ledger.

Bitcoin, on the other hand, has so many devices verifying the network that they collectively consume more electricity per year than a small country, like Greece or Switzerland. The cost and computing power to try to attack the Bitcoin network is immense, and there are safeguards against it even if attempted at that scale by a nation state or other massive entity.

Any news story you have ever heard about Bitcoin being hacked or stolen, was not about Bitcoin's protocol itself, which has never been hacked. Instead, instances of Bitcoin hacks and theft involve perpetrators breaking into systems to steal the private keys that are held there, often with lackluster security systems. If a hacker gets someone's private keys, they can access that person's Bitcoin holdings. This risk can be avoided by using robust security practices, such as keeping private keys in cold storage.

The rise of quantum computers could eventually pose an actual security threat to Bitcoin's encryption, where private keys could be determined from public keys, but there are already known methods that the Bitcoin protocol can adopt when necessary in order to become more quantum resilient, since the blockchain can be updated when there is broad consensus among participants.

Bitcoin's programmed difficulty for verifying transactions is automatically updated every two weeks, and it seeks the optimal point of profitability and security. In other words, the difficulty of the puzzle to add new blocks to the blockchain is automatically tuned up or down depending on how efficiently miners as a whole are solving those puzzles.

If Bitcoin becomes too unprofitable to mine (meaning the price falls below the cost of hardware and electricity to verify transactions and mine it), then fewer companies will mine it, and the rate of new block creation will lag its intended speed as computational power gradually falls off the network. An automatic difficulty adjustment will occur, making it require less computational power to verify transactions and mine new coins, which reduces security but is necessary to make sure that miners don't get priced out of maintaining the network.

On the other hand, if Bitcoin becomes extremely profitable to mine (meaning the price is way above the cost of hardware and electricity to mine it), then more people will mine it, and the rate of new block creation will surpass its intended speed as more and more computational power is added to the network. An automatic difficulty adjustment will occur, making it require more computational power to verify transactions and mine new coins, which increases security of the network.

More often than not, the latter occurs, so Bitcoin's difficulty has gone up exponentially over time, which makes its network more and more secure.

Even if a demonstrably superior cryptocurrency to Bitcoin came around (and some users argue that some of the existing protocols are already superior in many ways, based on speed or efficiency or extra features), that superior cryptocurrency would still find it nearly impossible to catch up with Bitcoin's security lead in terms of hash rate. Simply by coming later and thus having weaker security due to a weaker network effect, they have an in-built inferiority to Bitcoin on that particular metric, and for a store of value, security is the most important metric. The fact that Bitcoin came first, is something that can't be replicated unless the community around it somehow stumbles very badly and allows other cryptocurrencies to catch up. The gap, though, is quite wide.

An investment or speculation in a cryptocurrency, especially Bitcoin, is an investment or speculation in that cryptocurrency's network effect. Its network effect is its ability to retain and grow its user-base and market capitalization, and by extension its ability to secure its transactions against potential attacks.

Bitcoin Strengthening Market Share and Security

Since my 2017 analysis when I was somewhat concerned with market share dilution, Bitcoin has stabilized and strengthened its market share.

The semi-popular forks did not harm it, and thousands of other coins did not continue to dilute it. It has by far the best security and leading adoption of all cryptocurrencies, cementing its role as the digital gold of the cryptocurrency market.

Compared to its 2017 low point of under 40% cryptocurrency market share, Bitcoin is back to over 60% market share.

There is a whole ecosystem built around Bitcoin, including specialist banks that borrow and lend it with interest. Many platforms allow users to trade or speculate in multiple cryptocurrencies, like Coinbase and Kraken, but there is an increasing number of platforms like Cash App and Swan Bitcoin that enable users to buy Bitcoin, but not other cryptocurrencies.

The ongoing stability of Bitcoin's network effect is one of the reasons I became more optimistic about Bitcoin's prospects going forward. Rather than quickly fall to upstart competitors like Myspace did to Facebook, Bitcoin has retained substantial market share, and especially hash rate, against thousands of cryptocurrency competitors for a decade now.

Currencies tend to have winner-take-most phenomena. They live or die by their demand and network effects, especially in terms of international recognition. Cryptocurrencies so far appear to be the same, where a few big winners take most of the market share and have most of the security, especially Bitcoin, and most of the other 5,000+ don't matter. Some of them, of course, may have useful applications outside of primarily being a store of value, but as a store of value in the cryptocurrency space, it's hard to beat Bitcoin.

During strong Bitcoin bull markets, these other cryptocurrencies may enjoy a speculative bid, briefly pushing Bitcoin back down in market share, but Bitcoin has shown considerable resilience through multiple cycles now.

Through a combination of first-mover advantage and smart design, Bitcoin's network effect of security and user adoption is very, very hard for other cryptocurrencies to catch up with at this point. Still, this must be monitored and analyzed from time to time to see if the health of Bitcoin's network effect

is intact, or to see if that thesis changes for the worse for one reason or another.

Reason 2) The Halving Cycle

Starting from inception in January 2009, about 50 new bitcoins were produced every 10 minutes from “miners” verifying a new block of transactions on the network. However, the protocol is programmed so that this amount of new coins per block decreases over time, once a certain number of blocks are added to the blockchain.

These events are called “halvings”. The launch period (first cycle) had 50 new bitcoins every 10 minutes. The first halving occurred in November 2012, and from that point on (second cycle), miners only received 25 coins for solving a block. The second halving occurred in July 2016, and from there (third cycle) the reward fell to 12.5 new coins per block. The third halving just occurred in May 2020 (fourth cycle), and so the reward is now just 6.25 coins per new block.

The number of new coins will asymptotically approach 21 million. Every four years or so, the rate of new coin creation gets cut in half, and in the early 2030's, over 99% of total coins will have been created. The current number that has been mined is already over 18.4 million out of the 21 million that will eventually exist.

Bitcoin has historically performed extremely well during the 12-18 months after launch and after the first two halvings. The reduction in new supply or flow of coins, in the face of constant or growing demand for coins, unsurprisingly tends to push the price up.

Here's Bitcoin's historical price chart in logarithmic form, with four red dots indicating the earliest price point close to launch, and the three halvings, which represent the start of the four Bitcoin market cycles so far:

Market Price

The average USD market price across major bitcoin exchanges.



Chart Source: [Blockchain.com](https://blockchain.com)

Here we see a pretty strong pattern. During the 12-24 months after launch and the subsequent halvings, money flows into the reduced flow of coins, and the price goes up due to this restricted supply. Then after a substantial price increase, momentum speculators get on board, and then other people chase it and cause a mania, which eventually pops and crashes. Bitcoin enters a bear market for a while and then eventually stabilizes around an equilibrium trading range, until the next halving cycle cuts new supply in half again. At that point, if reasonable demand still exists from current and new users, another bull run in price is likely, as incoming money from new buyers flows into a smaller flow of new coins.

For more detail, Preston Pysh, the co-founder of the [Investor's Podcast Network](#), put together a chart and narrative that describes his view of the halving cycle from the perspective of the miners:

1. Following a halving event, efficient miners capture new reward flow and don't need to sell due to margins produced by new hardware advantage.
2. Less selling pressure quickly produces price growth towards the new S2F price orbit.
3. Speculators take the price well beyond the orbit (Mark A).
4. Miners try to capture the significant price margin & buy new equipment (which has a lag coming onto the network) (Between Marks A & B)
5. The difficulty adjustment during this period (Between Marks A & B) ramps up, making miner margin capture harder every 2 weeks – producing increased selling pressure.
6. Inefficient miners capitulate, difficulty adjustment makes it profitable again, price seeks balance at S2F orbit until next halving event.



Twitter: @PrestonPysh

Chart Source: @PrestonPysh

Based on recent hash rate data, it appears the mining market may have gotten past the post-halving capitulation period (from May into July), and now is looking pretty healthy. Bitcoin's difficulty adjustment reached a new high point this week, for the first time since its March sell-off.

Stock-to-Flow Model

Monetary commodities have high stock-to-flow ratios, which refers to the ratio between the amount of that commodity that is stored (aka "the stock") and the amount of that commodity that is newly-produced each year (aka "the flow").

Base commodities like oil and copper have very low stock-to-flow ratios. Since they have a large volume relative to price, they are costly to store and transport, so only a handful of months of supply are stored at any one time.

Monetary commodities like silver and gold have high stock-to-flow ratios. Silver's ratio is over 20 or 30, and gold's ratio is over 50 or 60. Specifically, the World Gold Council estimates that 200,000 tons of gold exists above ground, and annual new supply is roughly 3,000 tons, which puts the stock-to-flow ratio somewhere in the mid-60's as a back-of-the-envelope calculation. In

other words, there are over 60 years' worth of current gold production stored in vaults and other places around the world.

As Bitcoin's existing stock has increased over time, and as its rate of new coin production decreases after each halving period, its stock-to-flow ratio keeps increasing. In the current halving cycle, about 330,000 new coins are created per year, with 18.4 million coins in existence, meaning it currently has a stock-to-flow ratio in the upper 50's, which puts it near gold's stock-to-flow ratio. In 2024, after the fourth halving, Bitcoin's stock-to-flow ratio will be over 100.

In 2019, a popular Bitcoin price model based on its stock-to-flow ratio was published by PlanB, a Dutch institutional investor. He has several versions of it, and multiple visualizations to display it, but here's one of the representations:

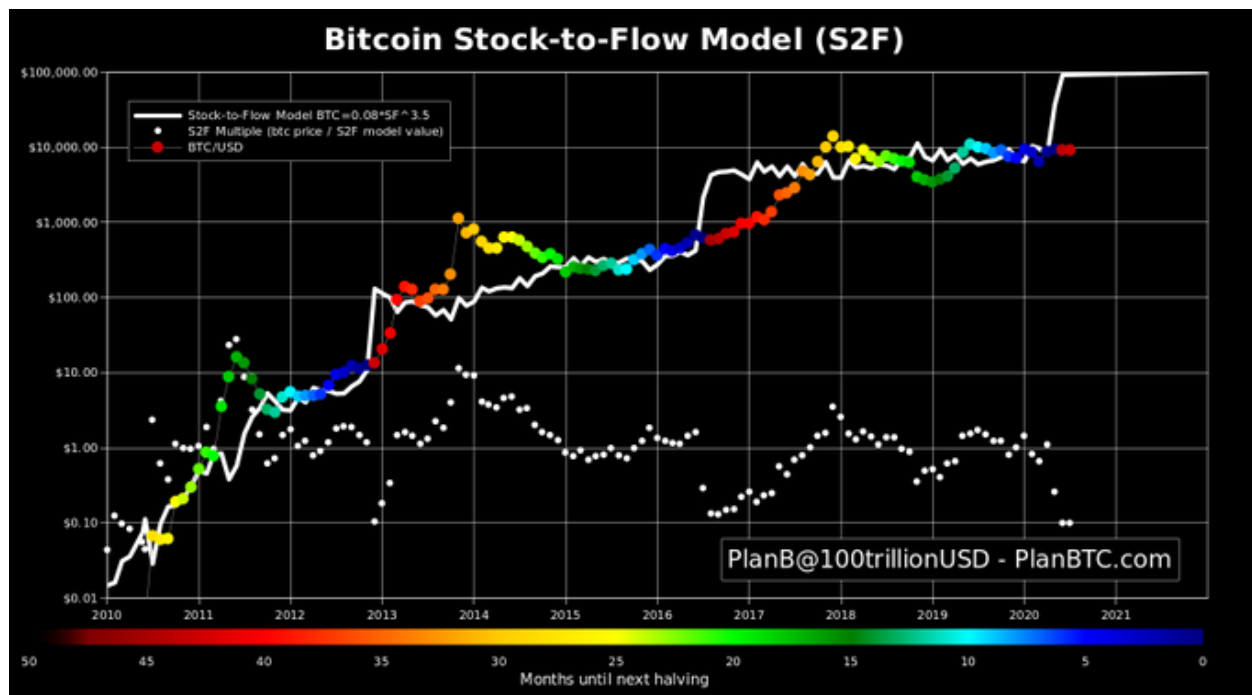


Chart Source: [PlanB, @100trillionUSD](#)

The model backtests Bitcoin and compares its price history to its changing stock-to-flow ratio over time, and in turn develops a price model which it can then (potentially) be extrapolated into the future. He also has created other versions that look at the stock-to-flow ratios of gold and silver, and apply that math to Bitcoin to build a cross-asset model.

The white line in the chart above represents the price model over time, with the notable vertical moves being the three halvings that occurred. The colored dots are the actual price of Bitcoin during that timeframe, with colors changing compared to their number of months until the next halving. The

actual price of Bitcoin was both above and below the white price model line in every single year since inception.

As you can see, the previously-described pattern appears. In the year or two after a halving, the price tends to enjoy a bull run, sharply overshoots the model, and then falls below the model, and then rebounds and finds equilibrium closer to the model until the next halving.

Here's his breakdown of each halving cycle, including the launch cycle, which makes it even more clear:

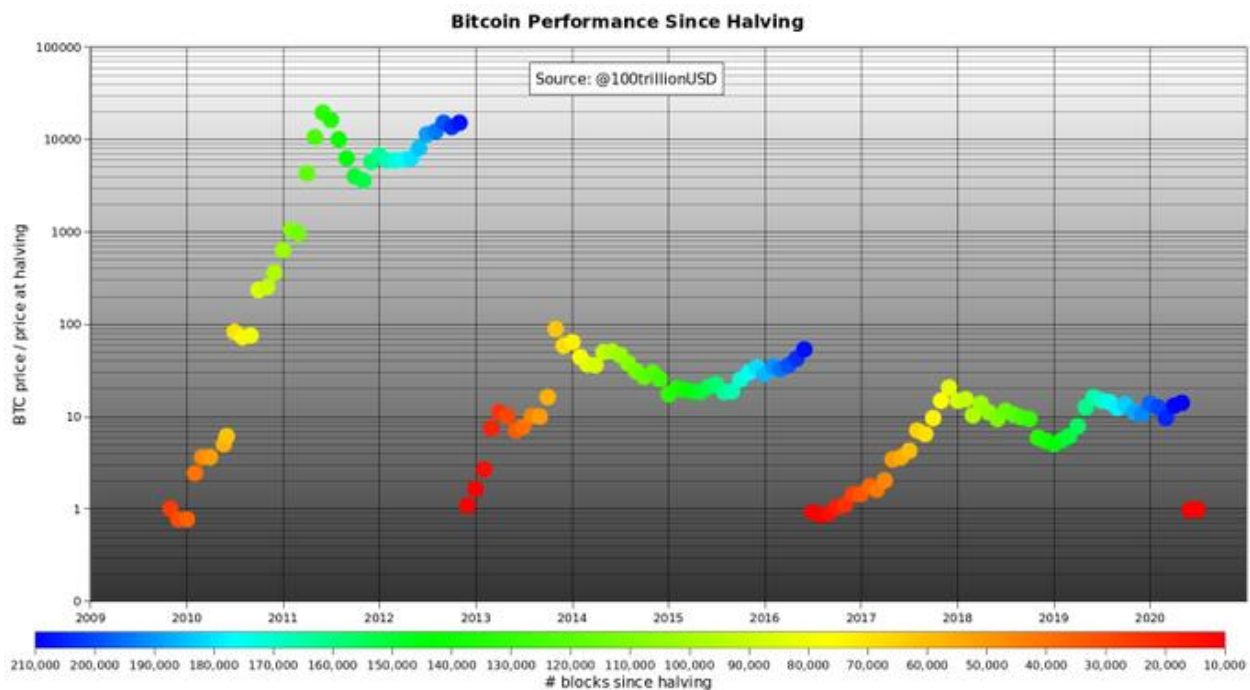


Chart Source: PlanB, @100trillionUSD

Each halving cycle is less explosive than the previous one, as the size of the protocol grows in market capitalization and asset class maturity, but each cycle still goes up dramatically.

PlanB's model extrapolation is very bullish, suggesting a six figure price level within the next 18 months in this fourth cycle, and potentially far higher in the fifth cycle. A six figure price compared to the current \$9,000+ price range, is well over a tenfold increase. Will that happen? I have no idea. That's more bullish than my base case but it's nonetheless a useful model to see what happened in the past.

If Bitcoin reaches a six figure price level with 19 million coins in total, that would put its market cap at just under \$2 trillion or more, above the largest mega-cap companies in the world today. It would, however, still be a small fraction of 1% of global net worth, and about a fifth of gold's estimated market

capitalization (roughly \$10 trillion, back-of-the-envelope), so it's not unfathomable for Bitcoin to eventually reach that height if there is enough sustained demand for it. During the late-2017 cryptocurrency mania, the total market capitalization of the cryptocurrency space reached over \$800 billion, although as previously mentioned, Bitcoin's share of that briefly fell to under 40% of the asset class, so it peaked at just over \$300 billion.

While the PlanB model is accurate regarding what the price of Bitcoin did relative to its historical stock-to-flow ratio, the extent to which it will continue to follow that model is an open question. During the first decade of Bitcoin's existence, it went from a micro-cap asset with virtually no demand, to a relatively large asset with significant niche demand, including from some institutional investors. On a percent-growth basis, the demand increase has been unbelievably fast, but is slowing.

When something becomes successful, the law of large numbers starts to kick in. It takes a small amount of money to move the needle on a small investment, but a lot of money to move the needle on a big investment. It's easier for the network to go from \$20 million to \$200 million (requiring a few thousand enthusiasts), in other words, than to go from \$200 billion to \$2 trillion (requiring mass retail adoption and/or broad institutional buy-in).

The unknown variable for how well Bitcoin will follow such a model over this halving cycle, is the demand side. The supply of Bitcoin, including the future supply at a given date, is known due to how the protocol operates. This model's historical period involves a very fast-growing demand for Bitcoin on a percent gain basis, going from nearly no demand to international niche demand with some initial institutional interest as well.

The launch cycle had a massive gain in percent terms from virtually zero to over \$20 per Bitcoin at its peak. The second cycle, from peak-to-peak, had an increase of over 50x, where Bitcoin first reached over \$1,000. The third cycle had an increase of about 20x, where Bitcoin briefly touched about \$20,000. I think looking at the 2-5x range for the next peak relative to the previous cycle high makes sense here for the fourth cycle.

If demand grows more slowly in percent terms than it has in the past, the price is likely to undershoot PlanB's historical model's projections in the years ahead, even if it follows the same general shape. That would be my base case: bullish with an increase to new all-time highs from current levels within two years, but not necessarily a 10x increase within two years. On the other hand, we can't rule out the bullish moonshot case if demand grows sharply and/or if some global macro currency event adds another catalyst.

All of this is just a model. I have a moderately high conviction that the general shape of the price action will play out again in this fourth cycle in line with the historical pattern, but the magnitude of that cycle is an open guess.

Game Theory

Let's put away real numbers for a second, and assume a simple thought experiment, with made-up numbers for clarity of example.

Suppose Bitcoin has been around for a while after a period of explosive demand. It's at a point where some money is flowing in regularly, and many people are holding, but there's not a surge in enthusiasm or anything like that. Just a constant low-key influx of new capital. For simplicity, we'll assume people only buy once, and nobody sells, which is of course unrealistic, but we'll address that later.

In this example, the starting state is 100 holders of Bitcoin, with 1000 coins in existence between them (an average of 10 coins each), at a current price point of \$100 per coin, resulting in a total market capitalization of \$100,000.

Each year for the next five years, ten new people each want to put \$1,000 into Bitcoin, totaling \$10,000 in annual incoming capital, for one reason or another.

However, there is a shrinking number of new coin supply per year (and nobody is selling existing coins other than the miners that produce them). In the first year, 100 new coins are available for resale. In the second year, only 90 new coins are available. In the third year, only 80 new coins are available, and so forth. That's our hypothetical new supply reduction for this thought experiment.

Year	Start	1	2	3	4	5
Total Bitcoin Hodlers	100	110	120	130	140	150
Total Bitcoin Number	1000	1100	1190	1270	1340	1400
Price per Bitcoin	\$100.00	\$100.00	\$111.11	\$125.00	\$142.86	\$166.67
Total Bitcoin Market Cap	\$100,000.00	\$110,000.00	\$132,222.22	\$158,750.00	\$191,428.57	\$233,333.33
New Bitcoin Per Year		100	90	80	70	60
New Buyers Per Year		10	10	10	10	10
New Investment Per Year		\$10,000.00	\$10,000.00	\$10,000.00	\$10,000.00	\$10,000.00

During the first year, the price doesn't change; the ten new buyers with \$10,000 in total new capital can easily buy the 100 new coins (10 coins each), and the price per coin remains \$100.

During the second year, with only 90 new coins and still \$10,000 in new capital that wants to come in, each buyer can only get 9 coins, at an effective price point of \$111.11 per coin.

During the third year, with only 80 new coins and still \$10,000 in new capital, each buyer can only get 8 coins, at an effective price point of \$125 per coin.

By the fourth year with 70 new coins, that's \$142.86 per coin. By the fifth year with 60 new coins, that's \$166.67 per coin. The number of coins has increased by 40% during this five-year period, so the market capitalization also grew pretty substantially (over 130%), because both the number of coins and the per-coin price increased.

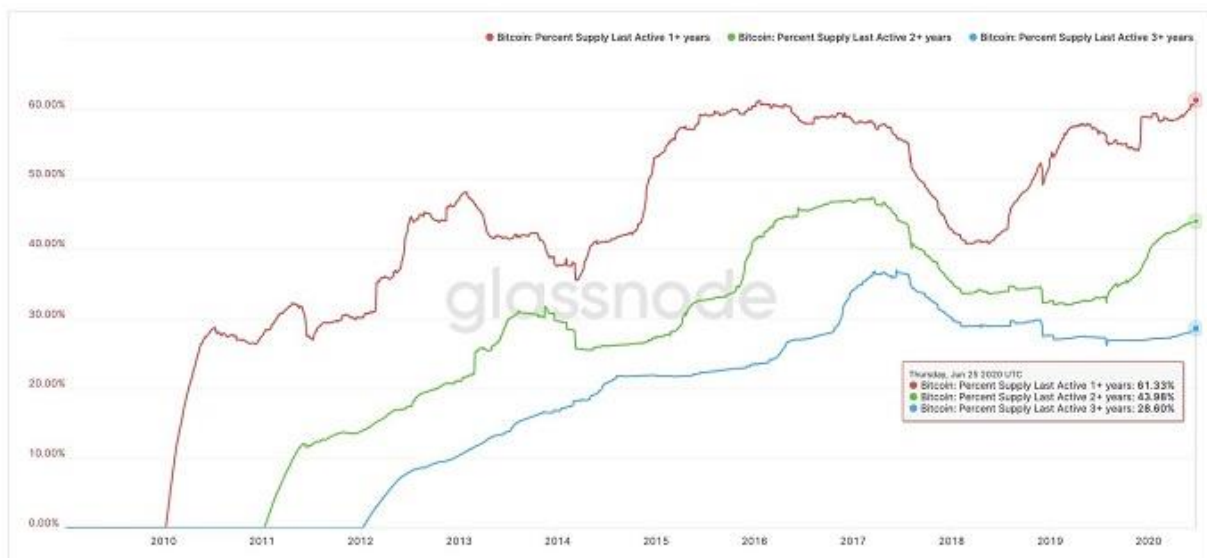
Some of those premises are of course unrealistic, and are simply used to show what happens when there is a growing user-base and constant low-key source of new buyers against a shrinking flow of new coins available.

In reality, a growing price tend to cause more demand, and vice versa. When investors see a bull market in Bitcoin, the demand increases dramatically, and when investors see a bear market in Bitcoin, the demand decreases. In addition, not all of the existing Bitcoin stock is permanently held; plenty of it is traded and sold.

However, Glassnode has plenty of research and data regarding how long people hold their Bitcoin.

For example, they published a chart within the past few weeks that showed that over 60% of Bitcoin supply hasn't changed addresses in the past year or more, and over 40% hasn't moved in the past two years or more:

Bitcoin: Supply Last Active 1+ Years, 2+ Years, and 3+ Years



© 2020 Glassnode. All Rights Reserved.

glassnode

Chart Source: [Glassnode](https://glassnode.com/)

That's not a perfect metric because an existing user can shift their Bitcoin from one address to another, firms that hold custody of Bitcoin for others can complicate the issue, and some percentage of early-mined Bitcoin are most likely lost due to people losing their private keys. However, it does provide useful data nonetheless.

Well-known gold bull and Bitcoin bear Peter Schiff recently performed a poll among his followers with a large 28,000+ sample, and found that about 85% of people who buy-and-hold Bitcoin and that answered his poll (which we must grant is a biased sample, although I'm not sure to which bias) are willing to hold for 3 years or more even if the price remains below \$10,000 that whole time.



I'm not trying to criticize or praise Peter Schiff here; just highlighting a recent sentiment sampling.

The simple thought experiment above merely captures the mathematical premise behind a stock-to-flow argument. As long as there is a mildly growing user-base of holders, and some consistent level of new demand in the face of less new supply, a reduction in new

supply flow naturally leads to bullish outcomes on the price. It would take a drop-off in new or existing demand for it to be otherwise.

The additional fact that the new supply of Bitcoin gets cut in half roughly every four years rather than reduced by a smaller fixed amount each year like in the simplistic model, represents pretty smart game theory inherent in Bitcoin's design. This approach, in my view, gave the protocol the best possible chance for successfully growing market capitalization and user adoption, for which it has thus far been wildly successful.

Basically, Bitcoin has a built-in 4-year bull/bear market cycle, not too much different than the stock market cycle. And these 4 years give investors plenty of time to experience the mania and despair associated with a cycle like this, which would be hard to replicate in 1-year cycles because it would all happen too quickly:

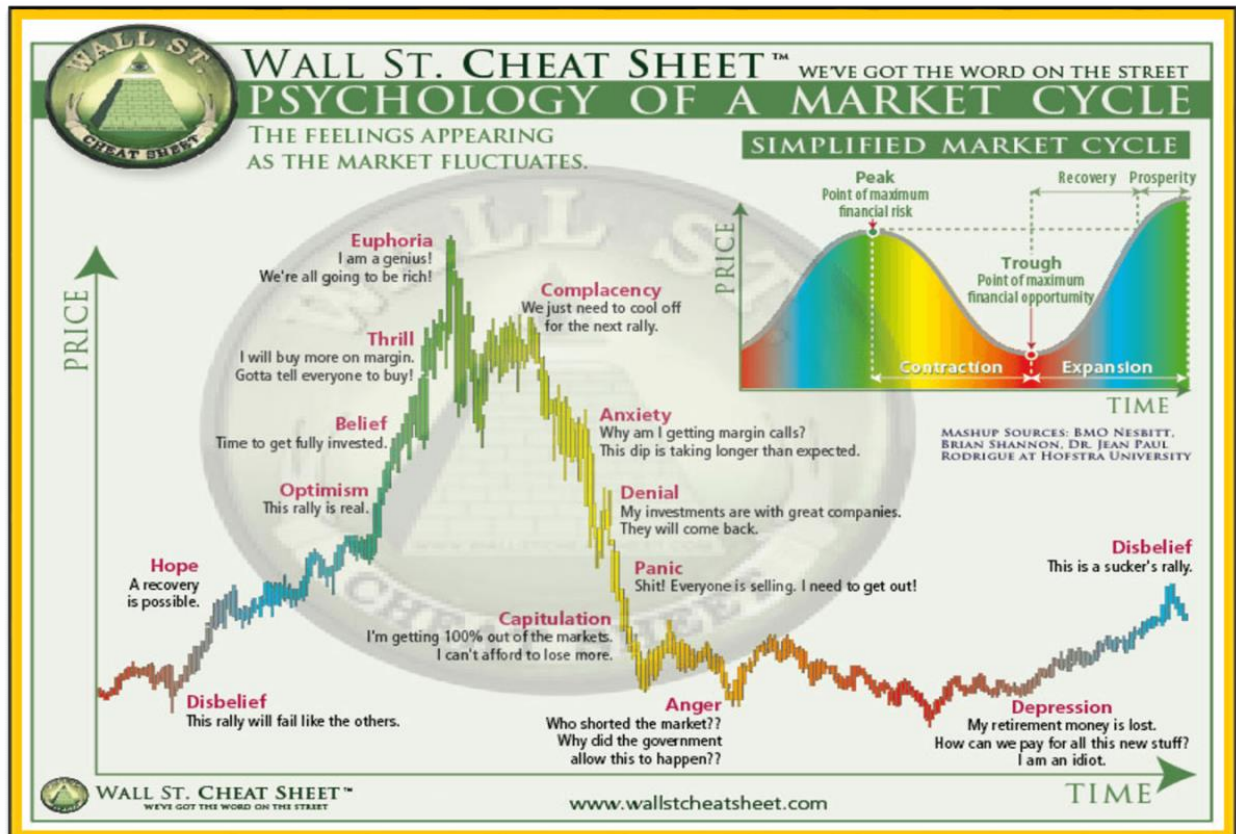


Chart Source: Wall St. Cheat Sheet

Bitcoin tends to have these occasional multi-year bear markets during the second half of each cycle, and that cuts away the speculative froth and lets Bitcoin bears pile on, pointing out that the asset hasn't made a new high for years, and then the reduction in new supply sets the stage for the next bull-run. It then brings in new users with each cycle.

For one more Glassnode visual, here is their recent chart that compares Bitcoin's price (gray line) to the percent of Bitcoin supply that hasn't changed addresses in at least a year (orange line). I added green dots to indicate halvings:

Bitcoin: Supply Last Active 1+ Years Ago



© 2020 Glassnode. All Rights Reserved.

glassnode

Chart Source: Glassnode

Here we see a consistent trend. During the Bitcoin price spikes associated with each cycle, people trade frequently and therefore the percentage of long-term holders diminishes. During Bitcoin consolidation periods that lead into the halvings, the percent of Bitcoin supply that is inactive, starts to grow. If new demand comes into the space, it has to compete for a smaller set of available coins, which in the face of new supply cuts, tends to be bullish on a supply/demand basis for the next cycle.

And although these halving-cycle relationships are more well known among Bitcoin investors over the past year, partly thanks to PlanB's published research, Bitcoin remains a very inefficient market. There's lots of retail activity, institutions aren't leading the way, and relatively few people with big money ever sit down and try to really understand the nuances of the protocol or what makes one cryptocurrency different than another cryptocurrency. Each time Bitcoin reaches a new order of magnitude for market capitalization, though, it captures another set of eyes due to increased liquidity and price history.

Bitcoin Priced in Gold

We can remove the dollar and various models from the price equation, and just look at Bitcoin priced in another scarce asset: grams of gold.

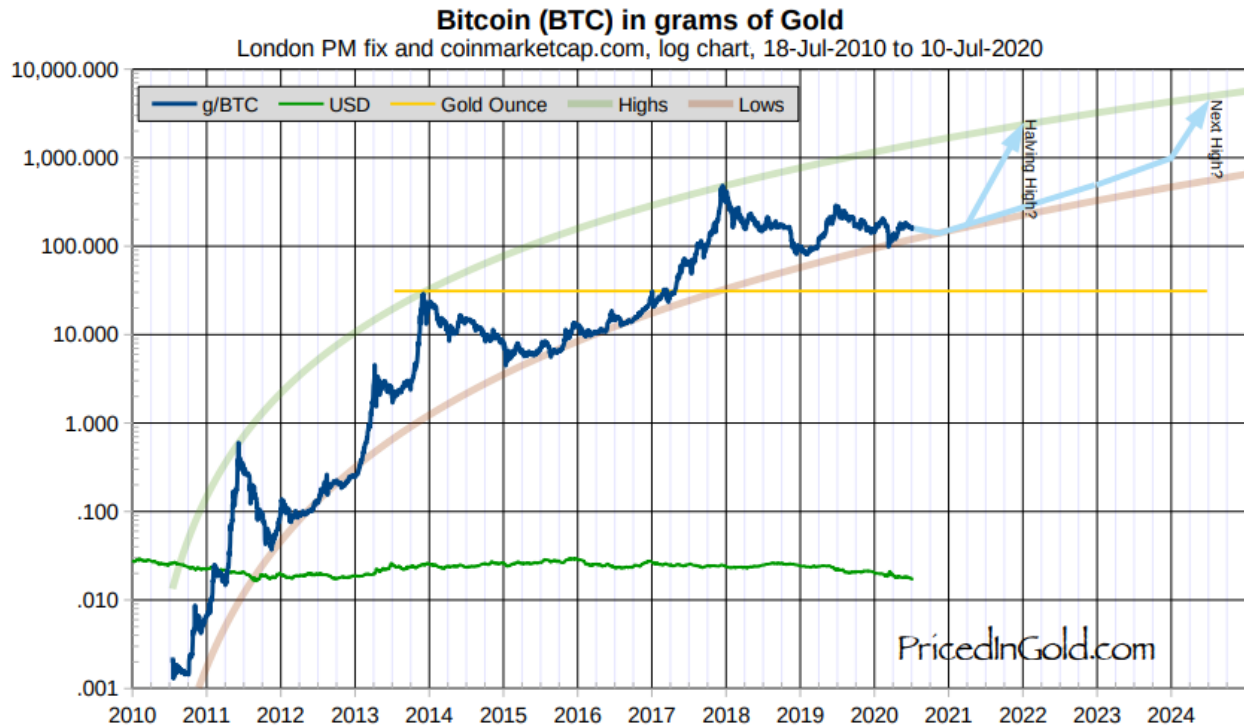


Chart Source: Charles Vollum, PricedInGold.com

Charles Vollum's chart suggests a more than 10x increase in the years ahead if it bounces back to the top end of its historical range, which would imply a six figure dollar price (like PlanB's model) if gold remains relatively static in dollar terms. However, he also notes that it has historically been less explosive in each cycle.

My analysis starts by noticing the relative heights and timings of the highs in mid-2011, late-2013 and late 2017. The second peak is about 48 times higher than the first, while the third peak is about 17x the second. So the rate of growth in the peaks seems to be slowing.

-Charles Vollum

If the next Bitcoin-priced-in-gold peak is 5x higher than the previous peak, as a random example that continues the diminishing pattern, that would be well into the six figures in dollar terms, assuming gold holds its value over the next few years. After the mania period with this model, it could drop back down into the five figure dollar price range for a while until the next cycle. This is all speculative, but worthy of note for folks that notice patterns.

Volatility Reduction Over Time

Charles Vollum also noticed the decline in volatility over Bitcoin's existence, again as priced in gold (but it also applies roughly to dollars):

Next, notice the distance between the red and green lines for any given date. In 2011, the upper bound was about 84x the lower bound. A year later, the ratio was 47x. By 2015 it was 22x, and at the start of 2020 it had fallen to 12x. This is a good thing, demonstrating a decline in overall peak-to-trough volatility. If this pattern holds up, the ratio will be about 9x in mid 2024, and about 6.5x by the end of the decade. Still high by forex and bond standards, but less than 10% of the 2011 volatility!

-Charles Vollum

Since Bitcoin started from a tiny base and grew into a meaningful size, in my view its volatility has been a feature, rather than a bug. In some years, it has been down over 80%, while in other years, it has gone up over 1,000%. This feature makes it speculative for most people, rather than having a reputation as a reliable store of value that gold enjoys, since it's relatively uncommon for gold to have a double-digit percent drawdown year, let alone a double-digit percent drawdown day like Bitcoin sometimes has.

If, over the next 5+ years, Bitcoin's market capitalization becomes larger and more widely-held, its notable volatility can decrease, like a small-cap growth company emerging into a large-cap blue-chip company.

In the meantime, Bitcoin's volatility can be managed by using appropriate position sizes relative to an investor's level of knowledge and conviction in the asset, and relative to their personal financial situation and specific investment goals.

Bitcoin's volatility is not for the faint of heart, but then again, a 2% portfolio position in something is rarely worth losing sleep over even if it gets cut in half, and yet can still provide meaningful returns if it goes up, say, 3-5x or more.

Intentional Design

Whether it ultimately succeeds or fails, Bitcoin is a beautifully-constructed protocol. Genius is apparent in its design to most people who study it in depth, in terms of the way it blends math, computer science, cyber security, monetary economics, and game theory.

Rather than just a fixed set of coins released to the public, or a fixed perpetual rate of new supply, or any other possible permutation that Satoshi could have designed, this is the specific method he chose to initiate, which is now self-perpetuating. Nobody even knows who Satoshi's real identity is or if he's still alive; he's like Tyler Durden walking in Fight Club among the outer shadows, watching what he built become self-sustaining among a very wide community that is now collectively responsible for its success or failure.

The regular halving events consistently reduce the flow of new coins, meaning that as long as there is a persistent user-base that likes to hold a lot of the existing coins, even if the annual new interest in Bitcoin from new buyers remains just constant (rather than growing), Bitcoin's price is likely to rise in value over the course of a halving cycle. This in turns attracts more attention, and entices new buyers during the cycle.

The thought put into its architecture likely played a strong role for why Bitcoin reached relatively wide adoption and achieved a twelve-figure market capitalization, rather than come and go as a novel thing that a few cypherpunk programmers found fascinating. For it to fail, Bitcoin's user-base would need to stagnate, go sideways, and ultimately go down in a sustained fashion for quite a while. Its death has been prematurely described or greatly exaggerated on many occasions, and yet here it is, chugging along and still growing, over 11 years into its existence, most likely thanks in part to the halving cycles in addition to its first-mover advantage that helped it build the most computational security.

In other words, in addition to solving the challenging technical problems associated with digital scarcity and creating the first cryptocurrency, Satoshi also chose a smart set of timing and quantity numbers (out of a nearly infinite set that he could have chosen from, if not carefully thought out) to maximize the incentive structure and game theory associated with his new protocol. Or, he was brilliantly lucky with his choices.

There are arguments for how it can change, like competitor protocols that use proof-of-stake rather than proof-of-work to verify transactions, or the adoption of encryption improvements to make it more quantum-resilient, but ultimately the network effect and price action will dictate which cryptocurrencies win out. So far, that's Bitcoin. It's not nearly the fastest cryptocurrency, it's not nearly the most energy-efficient cryptocurrency, and it's not the most feature-heavy cryptocurrency, but it's the most secure and the most trusted cryptocurrency with the widest network effect and first-mover advantage.

How Bitcoin behaves over the next two years, compared to its performance after previous halvings, is a pretty big test for its third halving and fourth overall cycle. We'll see if it stalls here and breaks down vs the historical pattern, or keeps pushing higher and wider as it has in the previous three cycles.

I don't have the answer, but my base outlook is bullish, with several catalysts in its favor and no firm catalyst as to why this cycle should be different than the prior cycles in terms of general direction and shape, even if I wouldn't really try to guess the magnitude.

Reason 3) An Ideal Macro Backdrop

In Satoshi's genesis block for Bitcoin that initiated the blockchain, he put in a news headline from that week:

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

-Bitcoin Genesis Block

Bitcoin was conceived and launched during 2008 and 2009; the heart of the global financial crisis, with widespread bank failure, large government bailouts, and international adoption of quantitative easing as a policy tool by central banks. His protocol was an attempt to store and transmit value in a way that was both verifiable and scarce, like a digital gold in contrast to the idea of bailouts and money-printing.

That crisis took years to play out. U.S. deficits were elevated for over 5 years, and quantitative easing didn't end until late 2014. Europe experienced a delayed sovereign debt crisis in 2012. That whole financial crisis was a process, rather than an event.

Over a decade later, we have an even larger crisis on our hands, with larger bailouts, bigger quantitative easing, and direct cash handouts to companies and consumers which are paid for by central bank deficit monetization.

The broad money supply in the United States, for example, has gone up massively. Here is the year-over-year percent change rate:

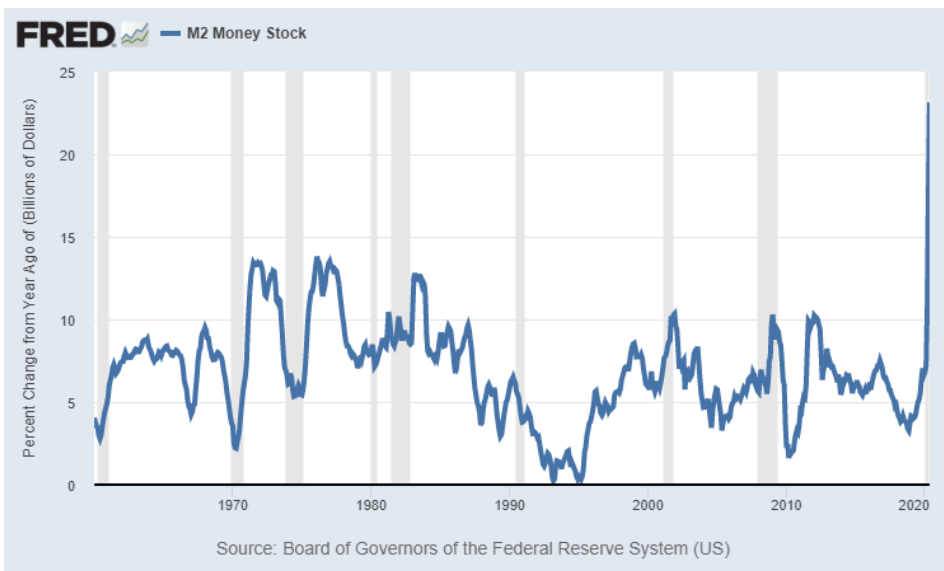


Chart Source: St. Louis Fed

The U.S. federal government is set to run a deficit somewhere in the ballpark of 20% of GDP this year, depending on the size of their next fiscal injection, which is by far the largest deficit since World War II. And most of this deficit is

being monetized by the Federal Reserve, by creating money to buy Treasuries from primary dealers and elsewhere on the secondary market, to ensure that this explosive supply of Treasuries does not overwhelm actual demand.

The dichotomy between quantitative easing that central banks around the world are doing, and the quantitative tightening that Bitcoin just experienced with its third halving, makes for a great snapshot of the difference between scarcity or the lack thereof. Dollars, euro, yen, and other fiat currencies are in limitless abundance and their supply is growing quickly, while things like gold and silver and Bitcoin are inherently scarce.

This is an era of near-zero interest rates, even negative nominal interest rates in some cases, and vast money-printing. Key interest rates and sovereign bond yields throughout the developed world are below their central banks' inflation targets. The fast creation of currency has demonstrably found its way into asset prices. Stock prices, bond prices, gold prices, and real estate prices, have all been pushed up over the past 25 years.

Even a 1% spillover into Bitcoin from the tens of trillions' worth of zero-yielding bonds and cash assets, if it were to occur, would be far larger than Bitcoin's entire current market capitalization.

I have several articles describing the money-printing and currency devaluation that is likely to occur throughout the 2020's decade:

- [The Subtle Risks of Treasury Bonds](#)
- ["Fixing" the Debt Problem](#)
- [QE, MMT, and Inflation/Deflation: A Primer](#)
- [Why This is Unlike the Great Depression](#)

In early May 2020, Paul Tudor Jones became publicly bullish and went long Bitcoin, describing it as a hedge against money-printing and inflation. He drew comparisons between Bitcoin in the 2020's and gold in the early 1970's.

Smaller hedge funds have already been dabbling in Bitcoin, and Tudor Jones may be the largest investor to date to get into it. There are now firms that have services directed at getting institutional investors on board with Bitcoin, whether they be hedge funds, pensions, family offices, or RIA Firms, by providing them the enterprise-grade security and execution they need, in an asset class that has historically been focused mainly on retail adoption. Even an asset manager as large as Fidelity now has a group dedicated to providing institutional cryptocurrency solutions.

And speaking of retail, the onboarding platforms for Bitcoin are getting easier to use. When I first looked at Bitcoin in 2011, and then again in 2017, and then again in early 2020, it was like a new era each time in terms of the usability and depth of the surrounding ecosystem.

Some major businesses are already on board, apart from the ones that grew from crypto-origins like Coinbase. Square's (SQ) Cash App enables the purchase of Bitcoin, for example. Robinhood, which has enjoyed an influx of

millions of new users this year, has built-in cryptocurrency trading, making an easy transition for Robinhood users if they happen to shift bullishness from stocks to cryptos. Paypal/Venmo (PYPL) might roll it out one day as well.

So, if Bitcoin's halving cycle, or the fiscal/monetary policy backdrop, lead to bull market in Bitcoin within the next couple years, there are plenty of access points for retail and institutional investors to chase that momentum, potentially leading to the same explosive price outcome that the previous three halving cycles had. Again, I'm not saying that's a certainty, because ultimately it comes down to how much demand there is, but I certainly think it's a significant possibility.

Final Thoughts

At the current time, I view Bitcoin as an asymmetric bet for a small part of a diversified portfolio, based on a) Bitcoin's demonstrated network effect and security, b) where we are in Bitcoin's programmed halving cycle, and c) the unusual macro backdrop that favors Bitcoin as a potential hedge.

If a few percentage points of a portfolio are allocated to it, there is a limited risk of loss. If Bitcoin's price gets cut in half or somehow loses its value entirely over the next two years, and this fourth cycle fails to launch and totally breaks down and completely diverges from the three previous launch/halving cycles, then the bet for this period will have been a dud. On the other hand, it's not out of the question for Bitcoin to triple, quadruple, or have a potential moonshot price action from current levels over that period if it plays out anything remotely like the previous three launch/halving cycles.

What will happen in this cycle? I don't know. But the more I study the way the protocol works, and by observing the ecosystem around it over the years, I am increasingly bullish on it as a calculated speculation with a two-year viewpoint for now, and potentially for much longer than that.

Additional Note: Ways to Buy Bitcoin

Some people have asked me what I think the best places to buy Bitcoin are, so I'm adding this last section.

Plenty of people have strong feelings about where to buy it or what companies they want to do business with; ultimately it comes down to your country of residence, how much you want to buy, how hands-on you want to be with it, and whether you want to accumulate it or trade it. There are trade-offs for convenience, security, and fees for various choices.

Exchanges like Kraken and Binance and Coinbase are popular entry points for people into buying some Bitcoin, especially if they want to trade it. Do

your homework, and find one that meets your criteria that operates in your jurisdiction.

I think Swan Bitcoin is great for accumulating Bitcoin, especially if you want to dollar-cost average into it, and I use it myself. I have a referral code as well: folks that sign up at swanbitcoin.com/alden/ can earn \$10 in free Bitcoin if they start accumulating through that platform. It can be stored for free with their custodian, or automatically transferred to your wallet. For many people, this is the method I would personally recommend checking out.

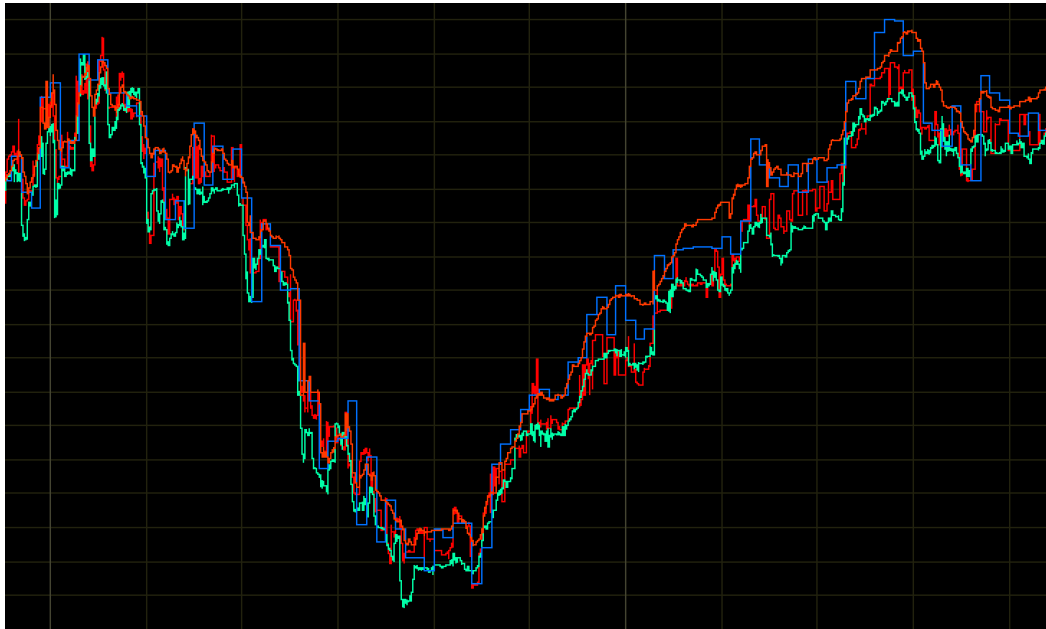
The Grayscale Bitcoin Trust (GBTC) is a publicly-traded trust that holds Bitcoin, and is therefore a hands-off method that can be purchased through an existing brokerage account. It has some disadvantages, like relatively high fees, a tendency to trade for a sizable premium over NAV, and centralized custody, but it's one of the few options available for investors if they want to hold a small allocation to Bitcoin within a tax-advantaged account.

Ultimately, it comes down individual needs. In general, if you want to minimize fees and maximize security for a large Bitcoin purchase, then maintaining your own Bitcoin wallet and private keys is the rock-solid way to go, but has a learning curve. If you want to just buy a bit and maintain some exposure and maybe trade it a bit, some of the exchanges are a good way to get into it. For folks that want to have some long-term exposure to it, Swan Bitcoin is a great place to start.

Ten Years of Bitcoin Market Data

By Clark Moody

Posted July 17, 2020



On July 17, 2010, two trading parties matched for the first time on the Mt. Gox Bitcoin exchange when 20 bitcoin changed hands for just under a dollar. The exact price of that first trade was \$0.04951 per whole bitcoin.

Prior to the trade on Mt. Gox, real-world goods had been exchanged for Bitcoin, but the existence of an electronic matching venue changed the game. Finding a trading partner on an automated electronic exchange is far simpler than making forum posts or jumping into IRC rooms. In July 2010, real-time Bitcoin price discovery began in earnest.

The First Bitcoin Trade

The exact specifications of the first Bitcoin trade:

```
Time: 2010-07-17 23:09:17 UTC
Amount: 20.00000000 BTC
Price: $0.04951
Value: $0.9902
```

At that moment ten years ago, the height of the blockchain was 68,773, and the total issued supply of Bitcoin was 3,438,650. A quick multiplication places the market cap of Bitcoin at roughly \$170,000 at the time of the first Mt. Gox trade.

If They Never Sold

Though it's probably not the case, let's assume for a moment that the buyer of those first coins on Mt. Gox held that 20 bitcoin until today, when the price is \$9,109 per coin. The return on the dollar invested would be roughly 184,000×!

Looking back to these early prices and seeing that Bitcoin has gained in value by more than five orders of magnitude offers a bit of perspective to those impatient for further price appreciation. Too often, new Bitcoiners think they're not early enough and they missed the boat. And every now and then, the value of Bitcoin rockets by another order of magnitude or two.

Bumps and Milestones Along the Way

Around two months after the first trade, Bitcoin had doubled to pass the 10 cent milestone on September 14, 2010. Not long thereafter, Bitcoin dropped a full 90% to reach its all-time low of \$0.01 on October 8, 2010. One lucky buyer snagged a full 100 bitcoin for a penny each.

Dollar parity would not come until February 9, 2011. Bitcoin would trade at \$10 on June 2, 2011, already up 1000× over its ultimate low nine months earlier.

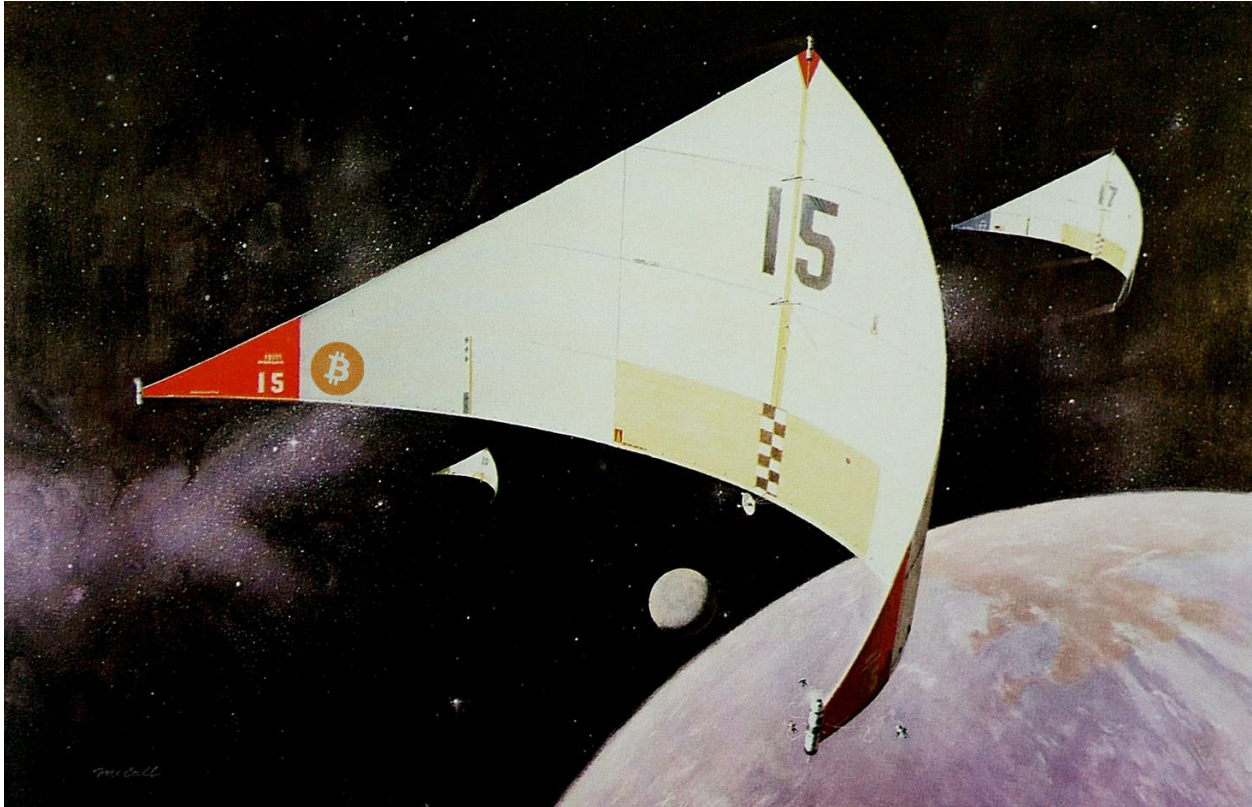
My Journey

Shortly after Bitcoin reached \$1.00 in February 2011, I learned about the project. At the time, I was interested in markets and trading, so I gravitated toward the free and open real-time market data coming from Mt. Gox. By the time I announced my first Bitcoin website [on the forum](#) in early June 2011, Bitcoin had already climbed past \$10.

Over the intervening years, my projects have always had something to do with the market data side of Bitcoin. It wasn't until the launch of my [Dashboard](#) that I presented network-level stats with the same real-time focus that I dedicated to market data projects.

The markets have matured, and now we have dozens of spot exchanges, regulated derivatives products, 100× leverage casinos, and auto-buy stacking apps. There are wallets for the streets and cash-only coordinators for private Bitcoin acquisition. In the middle of it all, there is free and open data. Without the free data feeds from exchanges and the blockchain, sites like mine would have taken much longer to appear. Certainly my first Bitcoin website wouldn't exist.

The Road Ahead



Over the course of the last ten years, the market cap of Bitcoin has gone from \$170k to \$170B. We've crashed 90%, and we've rallied 100×. Each order of magnitude increase in price brings a new cohort of profit-seekers, skeptics, opportunists, scammers, entrepreneurs, developers, hobbyists, and folks who finally have to figure out what's going on with that magic internet money. Somehow this thing never seems to die.

Each wave of volatility brings a new batch of memes, startups, hacks, bankruptcies, liquidations, and of course, Lamborghinis. Bitcoin's nature as sound money means that the miners can't simply increase output to meet increased demand, so I don't predict we'll see the end of volatility any time soon.

Whatever their reasons for learning about Bitcoin, each wave of adoption causes a small few to look past the promise of riches to start asking serious questions about the nature of money and the state. These conversations take years, but in the end, Bitcoin is showing people the way toward a sound money. And that could take us way beyond the Moon.

The Alchemy of Hashpower, Part I.

By Leo Zhang & Karthik Venkatesh

July 20, 2020

“Scientific method seeks to understand things as they are, while alchemy seeks to bring about a desired state of affairs. To put it another way, the primary objective of science is truth, that of alchemy, operational success.”
— George Soros, *The Alchemy of Finance*

Outline

Part 1.

1. *The Economic Value of Hashpower*
2. *The Hashpower Asset Class*
 1. *The Machine Markets*
 2. *The Dimensions of Hashpower*
 3. *Synthetic Hashpower*
 4. *Hashpower Investment Vehicles*

Part 2.

1. *Reflexivity in Hashpower*
2. *The Four Phases of Reflexivity*

The Economic Value of Hashpower

Bitcoin is a new computing paradigm. It abstracts out storage, communication, and computing from dedicated hardware. All nodes perform independent verification of each transaction, new blocks, and selection of the chain with the most computation power. Bitcoin achieves state replication without central coordination. But the design comes with clear trade-offs: in order to give all participants the full copy of the database, redundant messages and data storage are required. The redundancy is inevitable regardless of how much optimization is done to improve on-chain performances. The purpose of this system is not to improve the efficiency over the traditional distributed computation, but to formalize and publicize *how* the process is done.

Why do we need a computing paradigm that is highly redundant, inefficient, and fully transparent?

In a traditional distributed system, the nodes and their coordination rules are controlled by the institution or the company providing data storage and access services to their business. On the other hand, the Bitcoin network's consensus and transaction rules are homogeneously obeyed, in spite of the heterogeneity of the nodes. Transactions are sporadically initiated by anonymous participants all over the world with different network speeds. Without a single source of time or an authoritative coordinator, it is impossible to determine at what point in time does a transaction take place. Bitcoin works around the thorny issue of time coordination with proof-of-work, a mechanism that can prove a certain amount of computation resources has been utilized for a period of time. As Gregory Trubeskey explained, *"the difficulty in finding a conforming hash acts as a clock."* Through the ticking of this decentralized clock, the transaction blocks become timestamped, and thus allowing a p2p network to coordinate efficiently. Hashpower crystallizes the sequence of transactions on the ledger, allowing Bitcoin to automate trust, and independently facilitates value transfers and storage with strong assurances.

Settlement assurance is the critical foundation to the adoption and longevity of a settlement network. The settlement assurance, or economic finality, is considered strong when the ordering of the transactions is resistant to tampering. As the blockchain propagates and the network hashpower continues to accumulate, the "energy attached" increases the block's economic weight. The cost of acquiring 51%+ of the global hashpower may become too expensive compared to the possible gains from launching an attack.

All economic activities flow into the settlement network. In Economics of Bitcoin as a Settlement Network, Saifedean argues that Bitcoin's ability to handle large settlements compares favorably to those between central banks and financial institutions, thanks to it being cheaper, more verifiable, and free of counterparty risks. The Fedwire system processes over \$2 trillion on a daily basis. But only the few chartered banks can benefit from the value accrued from economic activities on top. In Bitcoin, anyone can sustain Bitcoin's heartbeat by contributing computations, and in return gets rewarded with a share of the economic value. **Hashpower secures the Bitcoin network, and the economic value of hashpower in turn is fundamentally driven by the activities on the network.** This is how the Bitcoin paradigm connects energy with digital information. This is the Yin-Yang duality of hashpower.

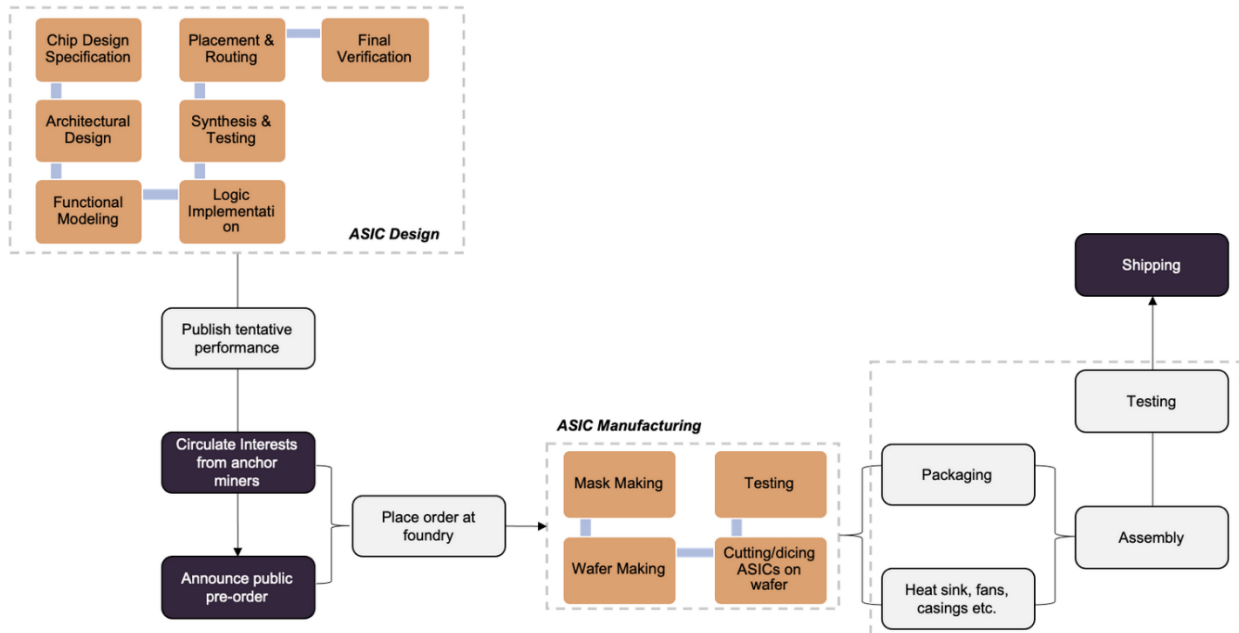


The Hashpower Asset Class

We categorize all assets that produce hashpower in exchange for cryptocurrency, and synthetic contracts / financial instruments that mimic mining returns as part of the hashpower asset class. Despite its short history, investing in this asset class has grown popular. A number of mining special purpose vehicles (SPV), verticalized institutional mining projects, and mining infrastructure / service providers, mining-related financial contracts were launched to satisfy the demand. **In this chapter, we describe the key characteristics of different types of hashpower assets, their nature as financial instruments, as well as the challenges each market vector is facing today.**

I. The Machine Markets

Unlike the pure digital commodities that they create, a mining operation is significantly affected by physical attributes such as qualities and locations. Producing hashpower involves many exogenous factors such as chips design, tape-out, supply chain, energy source, and maintenance.



New product releases are usually scheduled right before the Sichuan monsoon season to capture miners' interests, and are usually sold out immediately. Manufacturers would circulate interests from large miners and distributors to anchor the pre-orders, and release only a small percentage online for retail. Latest generation machines are typically available around 6 months after product announcements. **Purchasing new machines from manufacturers is similar to purchasing oil term supply contracts before the 1980s.** Contracts in which a seller of oil agrees to supply a buyer with specific quantities of oil at scheduled dates in the future, and the price is determined by the oil company unilaterally.

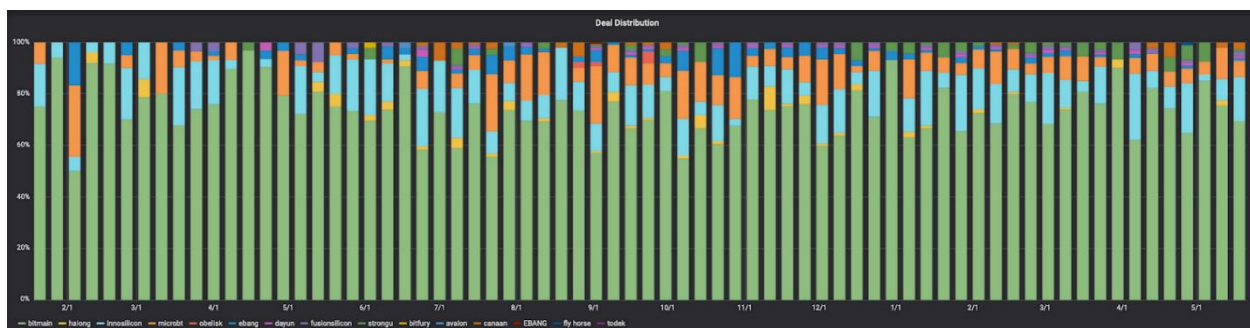
After 2018, manufacturers have become increasingly prudent on inventory management. Manufacturers only assemble machines after orders have been confirmed and aggregated, and buyers typically have to wait 2-3 months for the machines to ship. Since manufacturers only release a fraction to the public, retail buyers often have to acquire miners through distributors and pay an extra premium. The upside is, buyers can get machines sooner if the distributor has the machines in stock. Based on the distributor's location and inventory availability, the price for the same machine can vary significantly:

	Whatsminer M30s	Whatsminer M20s	Antminer S19 Pro	Antminer S17 Pro
Distributor 1	\$2,638	\$1,140	\$3,015	\$1,580
Distributor 2	\$2,469	\$1,430	\$2,480	\$1,590
Distributor 3	\$2,560	\$1,489	\$3,249	\$1,675
Distributor 4	\$2,905	\$1,650	\$3,320	\$1,963
Distributor 5		\$2,952	\$3,399	\$3,454
Distributor 6		\$3,950	\$4,676	
Standard deviation	\$188	\$1,104	\$727	\$799

(Source: asicminervalue.com)

Used machines also have a rather large secondary market. **Trading used machines requires significant experience.** Information is highly asymmetric in the secondary market. Transactions are often peer-to-peer, and the sellers have much better understanding of the qualities of the machines than buyers. Used machines are usually way past their warranty. It's not uncommon for them to underperform expected hashrate. Not to mention some vendors are outright scams. When buying from distributors or secondary markets, it's important to choose reliable distributors and channels whose reputation is well-established, and sign proper contracts that promise compensation should the machines be delayed, or fail to meet expected performance.

The machine market is notoriously illiquid. Some machines are easier to source via secondary markets because they have been around longer, or produced at greater volume. Mining machines are commodities. Machines with similar efficiency produced by different manufacturers may have similar unit price on manufacturers' websites. But once they hit the secondary market, it's all about supply and demand. This is why despite Whatsminer and Canaan rapidly cannibalizing Bitmain's market share in the past two years, secondary market deals in 2020 so far are still dominated by Bitmain machines:

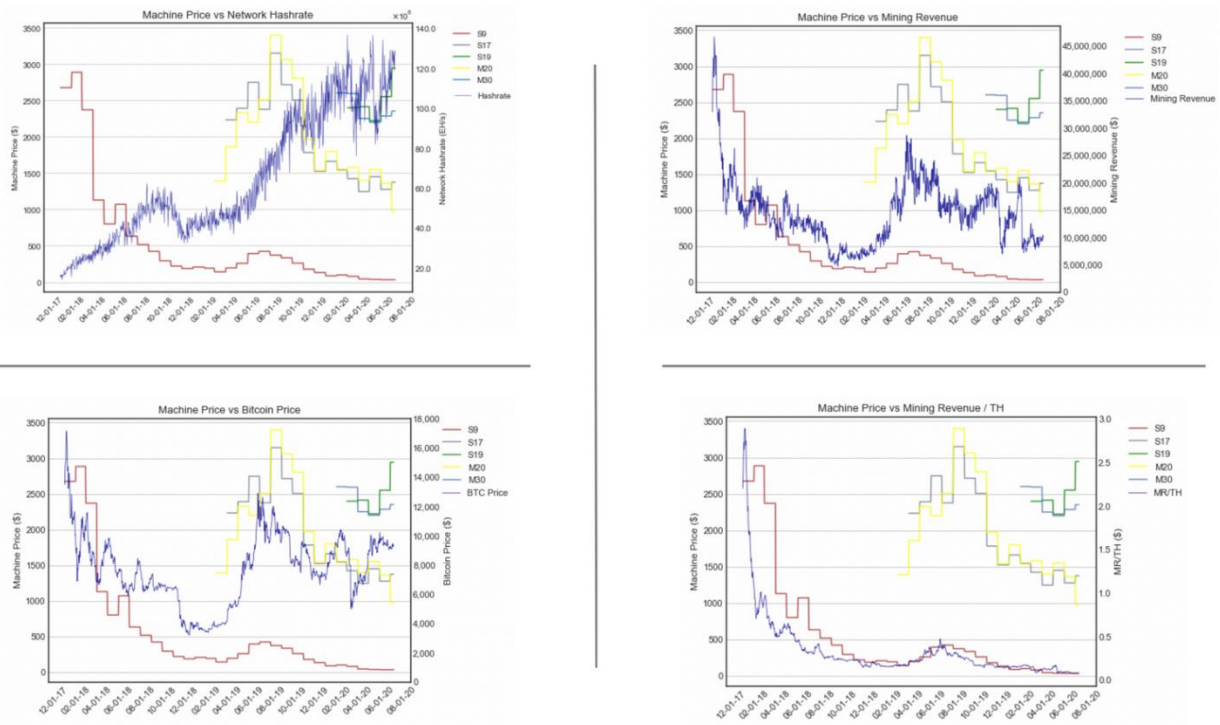


(Source: Luxor Mining)

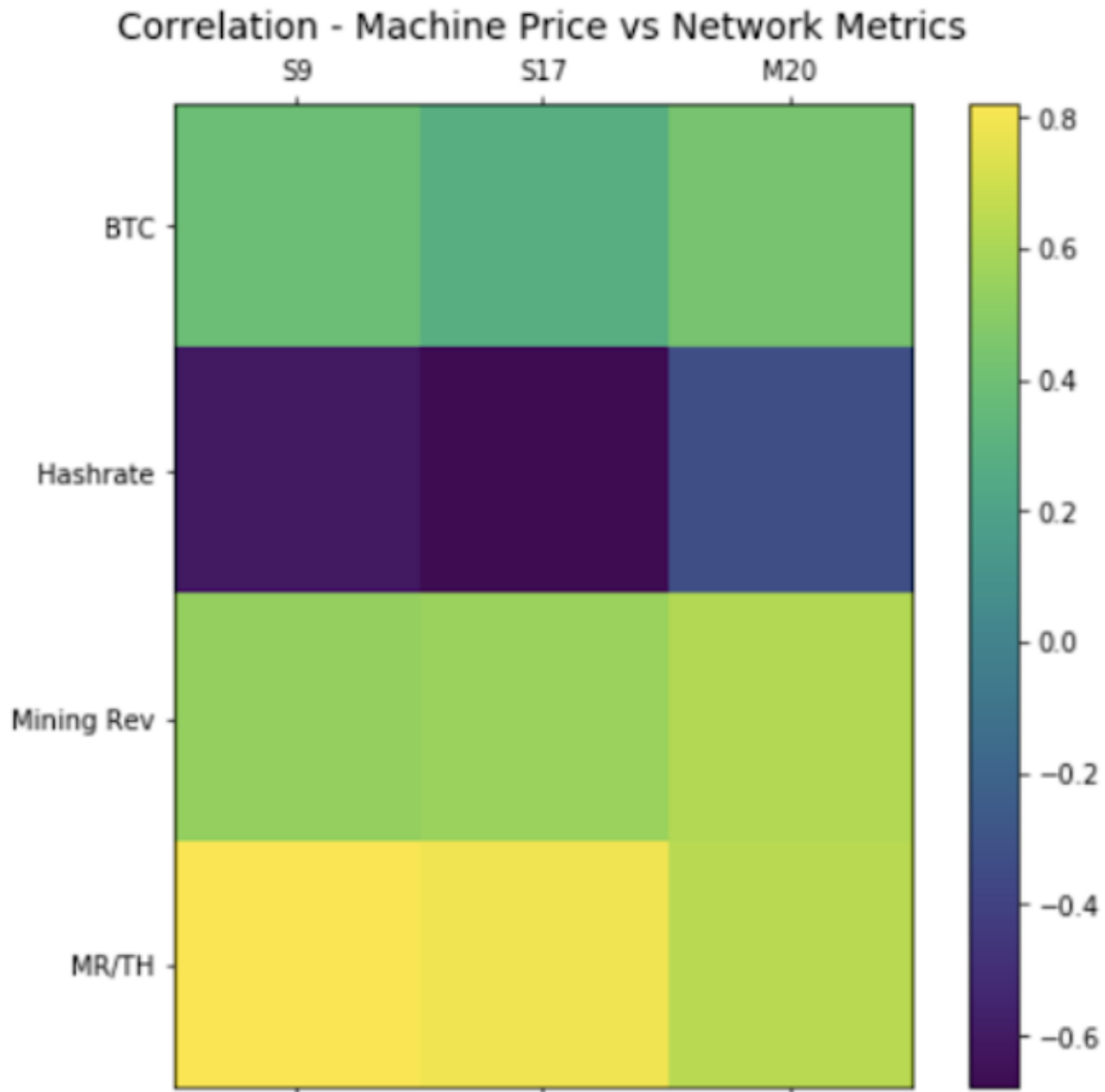
II. The Dimensions of Hashpower

There are many factors that influence the pricing of the machines. **In this section, we construct a simple proxy model for the valuation of hashpower, and break down how it responds to changes in underlying variables.**

The value of hashpower fluctuates as Bitcoin price, network hashpower (technically difficulty, but given that most pools payout calculations are based on expected value, hashrate is good enough as a proxy), and transaction fees change. Using the rigs data on [Hashrateindex](#), we can compare how historical machine prices moved against these variables:



(Data source: [Hashrateindex](#), [Coinmetrics](#))



(S19 and M30 are excluded due to relatively short history.)

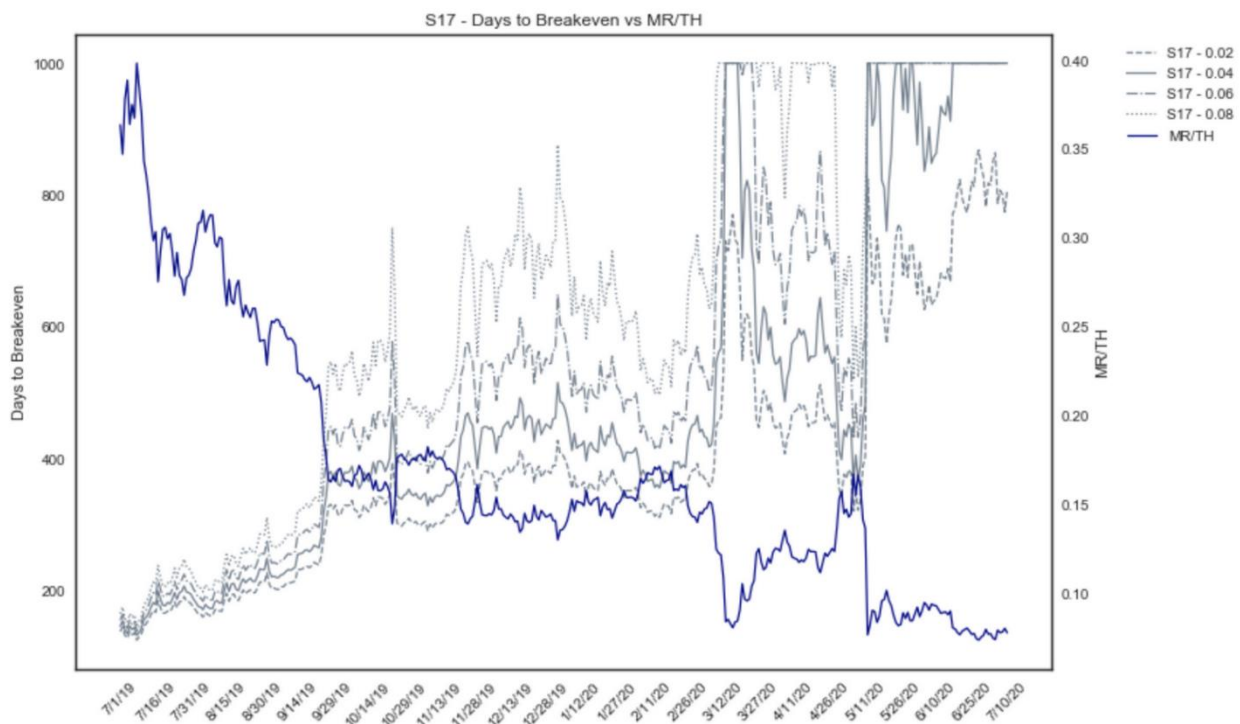
Unsurprisingly, machine prices track unit mining revenue the closest. But it doesn't help us understand the expenses associated with running the hashpower. In the market today, the vogue of hashpower valuation metrics is **static days-to-breakeven**, especially among the Chinese mining community. It is simple to calculate and intuitive to understand. Similar to how "implied volatility" is the proxy for options valuation, days-to-breakeven has become a popular proxy for machines valuation:

$$D = \frac{C}{[P * \frac{S}{H} * (m + n) * 6 * 24 - k * S * r * 24]}$$

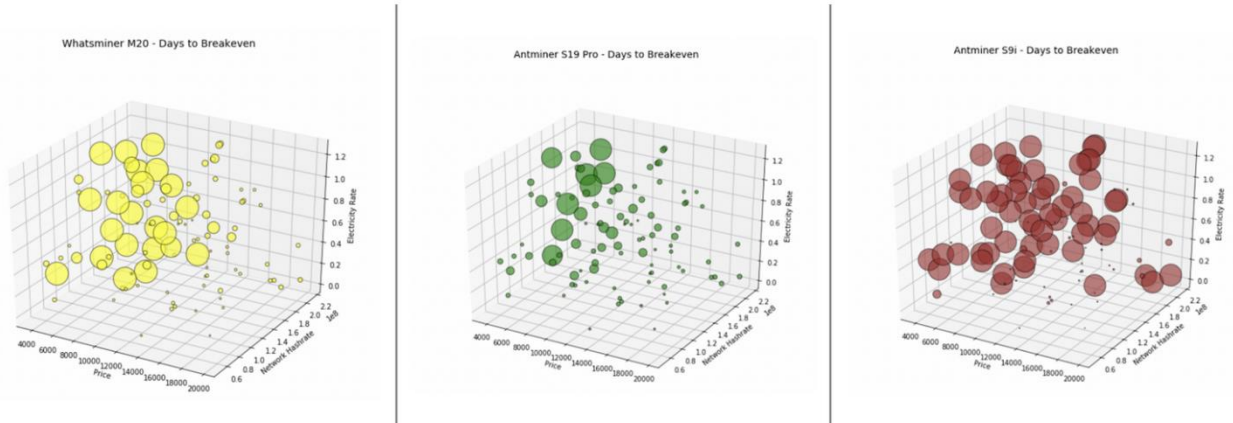
Where:

- D is the static days-to-breakeven
- C is the upfront capital expenditure
- P is the current Bitcoin price
- S is hashrate produced by the purchased equipments
- H is the network hashrate
- m is the coinbase reward, currently it is 6.25BTC.
- n is the current avg. transaction fee per block
- k is the efficiency (J/T) of the equipments
- r is the all-in electricity cost (\$/KwH)

Backtest of Days-to-Breakeven of a S17 at various r (all-in electricity cost):



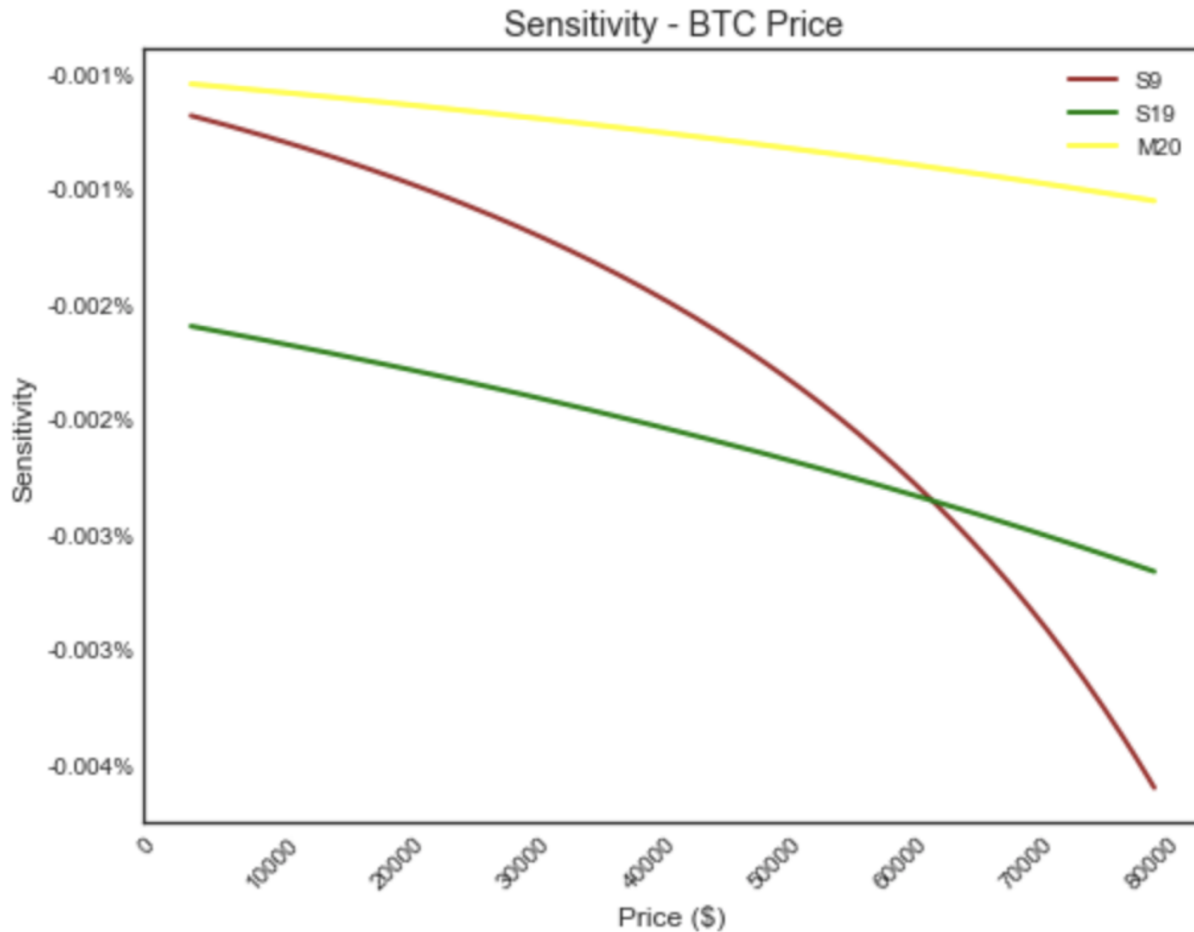
This is a static measure and fails to capture the options value of the machine as the underlyings variables change. There are two main components to this metric: the revenue and the cost. Before making a mining investment, most miners understand their cost structure (hopefully). The unit costs are fixed during the lifetime of the machines (hopefully!). The revenue on the other hand, is determined by three random walks:



We can examine the sensitivity of days-to-breakeven metric by taking its partial derivatives with respect to each variable. **This is analogous to options delta, which measures how much the value of the option changes when the underlying asset's price changes.** The higher the absolute number of the output is, the faster days-to-breakeven responds to price change. Sensitivity to price change:

$$\frac{dD}{dP} = - \frac{C * H * (m + n)}{4S * (6 (m + n) * P - H * k * r)^2}$$

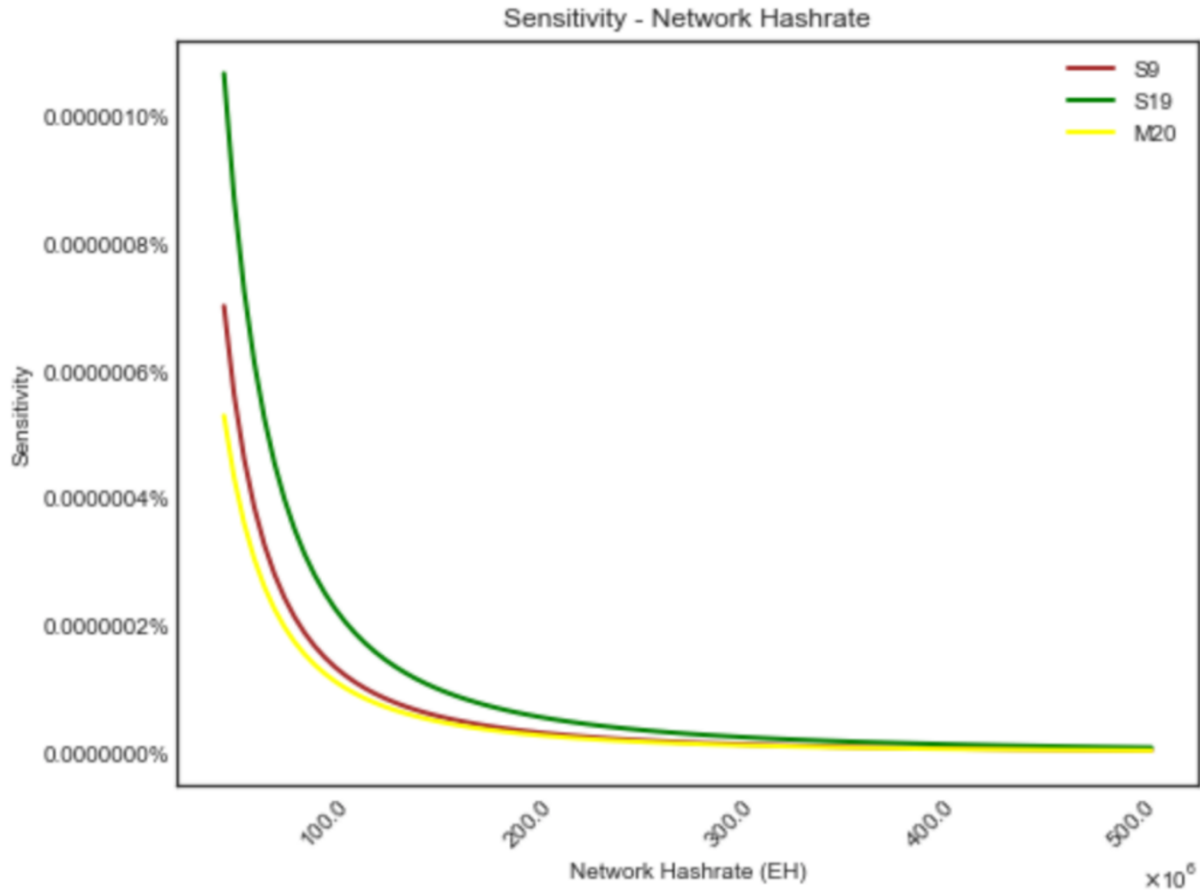
Using the formula above, we can plot out the metric's sensitivity to BTC price:



The graph shows that as the Bitcoin price increases, days-to-breakeven will gradually become more sensitive to price change. With S9's sensitivity picking up much faster than the other two. Note that price, network hashpower, and fees are interconnected. But without the explicit function of $dH(p)/dp$ or $df(p)/dp$, we assume the variables are independent. The same analysis can be applied to network hashpower change:

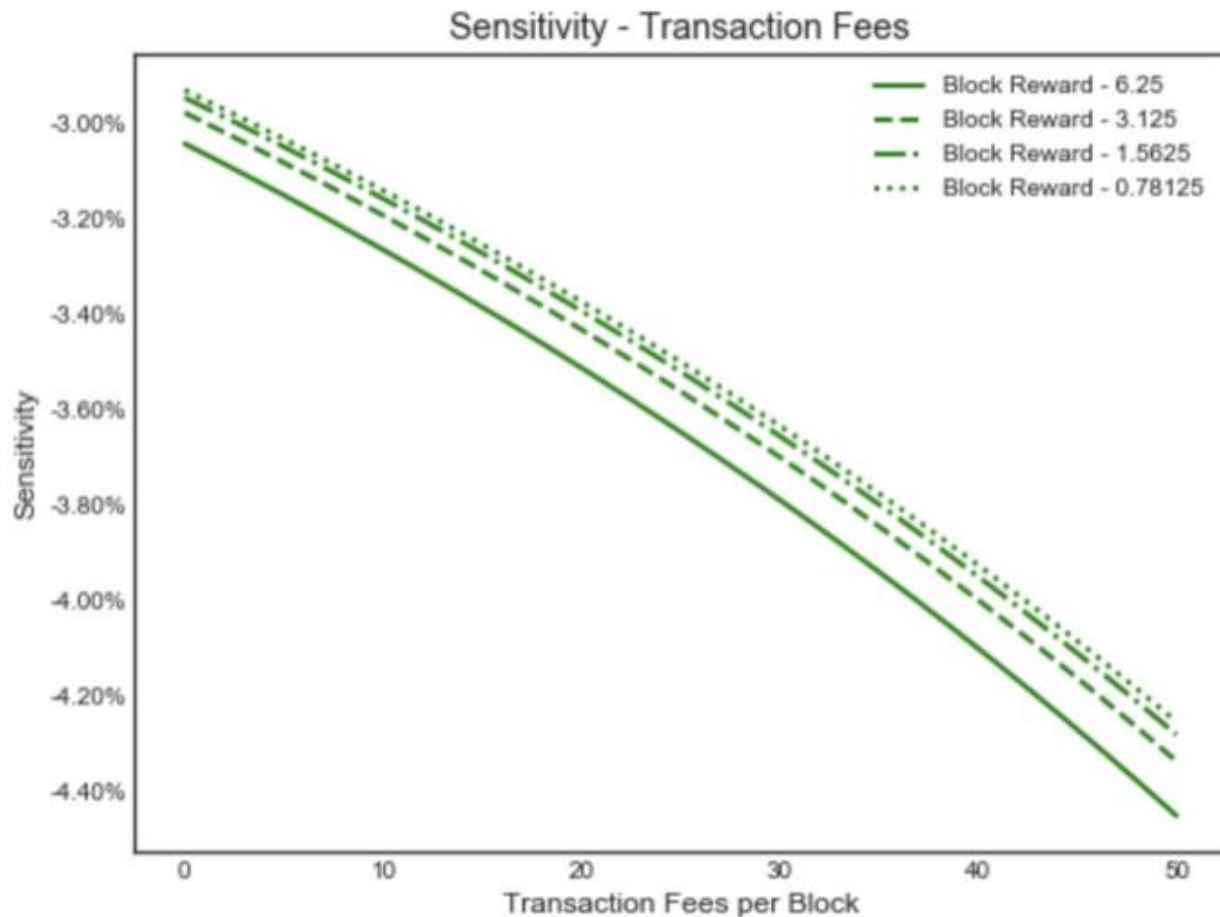
$$\frac{dD}{dH} = \frac{C * P * (m + n)}{4S * (6(m + n) * P - H * k * r)^2}$$

Sensitivity to network hashpower change:



Next we show sensitivity to average fees per block with different coinbase rewards. As the coinbase reward programmatically reduces, transaction fee plays a more important role as a source of mining revenue. Sensitivity for S19 Pro:

$$\frac{dD}{dn} = - \frac{C * H * P}{4S * (6(m + n) * P - H * k * r)^2}$$



While days-to-breakeven is a simple and intuitive static measure of mining performance, it eliminates the inherent options value of the machines, and thus the metric itself is highly volatile. In order to create a rigorous valuation model for hashpower, we need to capture future uncertainties by treating it as a multivariate option, or synthesize it with a basket of different instruments. These valuation approaches have different pros and cons. We intend to cover these trade-offs and explain the mathematics of each methodologies in a future article on the *architecture of a hashpower marketplace*. Separately, we will go over other “hashpower greeks” such as gamma (second derivative, the sensitivity of the sensitivities) and theta (time decay).

III. Synthetic Hashpower

In addition to the complexity in financial valuation, purchasing and running mining machines come with many operational challenges. For retail buyers, this process can be daunting to manage. An easier way to get mining exposure is through purchasing cloud mining contracts. **Cloud mining is a primitive form of a hashpower financial derivative that separates future**

production from its current physical location. In this section, we present several different variations of synthetic hashpower.

Over the years, countless cloud mining projects have sprung into existence and quietly faded into oblivion. The dilemma of cloud mining is that it clearly targets retail buyers since large miners are better off operating machines themselves. But evaluating these contracts requires significant insider knowledge about the mining industry, and expertise in complex options pricing. This is a main reason that, despite that in theory, the concept represents a natural next step in developing capital markets, the majority of the current cloud mining projects are considered as “scams” (a lot of them actually are scams).

As an immature and still relatively small field, the cloud mining market suffers from a complete lack of market standards. HoneyLemon Market is a fantastic data aggregator for cloud mining information. Using its dashboard, we can see that different platforms have wildly inconsistent contract terms and pricings:

Spot Contracts		Unit Price(VWAP)	Volume(24h)	Premium / Discount
Real time	NiceHash	\$ 0.0743 (/TH/Day)	239,077 TH	-11%
Forward Contracts				
Contract Maturities		Best Unit Price	Cost Basis	ROI ☺
3 months	2 Platforms	\$ 0.0684 (/TH/Day)	\$ 9,436.70 per BTC	-2%
6 months	3 Platforms	\$ 0.1479 (/TH/Day)	\$ 20,403.27 per BTC	-55%
8 months	1 Platforms	\$ 0.1472 (/TH/Day)	\$ 20,310.94 per BTC	-54%
1 year	4 Platforms	\$ 0.0678 (/TH/Day)	\$ 9,359.29 per BTC	-1%
2 years	2 Platforms	\$ 0.0849 (/TH/Day)	\$ 11,707.73 per BTC	-21%
3 years	1 Platforms	\$ 0.0699 (/TH/Day)	\$ 9,643.86 per BTC	-4%

Currently most of the contracts are unprofitable. Due to the built-in premium on cost-of-production, it requires very specific market conditions in order to generate profits through cloud mining. Typically after a prolonged period of downmarket, and price trend starts to reverse into a natural rally (e.g. April-May of 2019). The demand for hashpower suddenly increases. Purchasing and installing machines may take too long, so buying cloud mining contracts becomes a faster way to build a position. Through cloud mining, investors can also gain exposure to newly launched projects that are not yet available on

exchanges. Whats more, hackers can rent hashrate to opportunistically carry out 51% attacks on smaller networks. This is the **hashpower Darwinism** that filters out poorly designed PoW projects.

Another synthetic hashpower asset is the **machine token**. They are liquid tokens that represent a fraction of a mining machine. Traders speculate on the secondary market volatility of the machines rather than the coins that they produce. While the concept has been around for a while, volume hasn't really shown much growth. Mostly because the multivariate nature of mining revenue makes it challenging for speculators to form consensus on pricing "liquid machines".

Sophisticated traders can structure synthetic hashpower asset portfolios.

For instance, a long cloud mining contract can be purchased concurrently with a long position in FTX's implied hashrate futures, and add a short position on BTC spot futures. There are multiple creative ways to structure mining portfolios with financial instruments. For funds and trading firms who don't want to own and operate hardwares, this is a cleaner way to gain mining exposure.

Illustrative portfolio:

	Price up, Difficulty up	Price up, Difficulty down	Price down, Difficulty down	Price down, Difficulty up
Long hashrate futures	<i>up</i>	<i>down</i>	<i>down</i>	<i>up</i>
Short BTC futures	<i>down</i>	<i>down</i>	<i>up</i>	<i>up</i>
Long BTC	<i>up</i>	<i>up</i>	<i>down</i>	<i>down</i>
Long Cloud mining contract	<i>neutral</i>	<i>up</i>	<i>neutral</i>	<i>down</i>

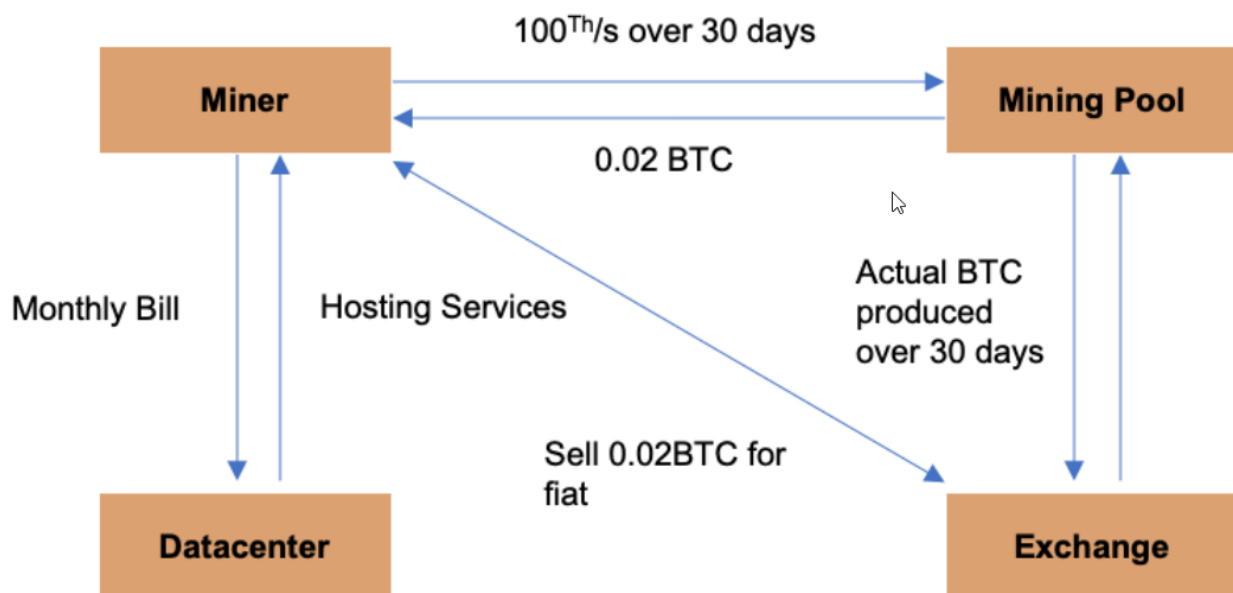
(Depending on the magnitude of the movements, "long cloud mining contract" is most likely not neutral when Price and Difficulty move in opposite directions.)

In practice, structuring such a portfolio is a highly nuanced task. As the set of days-to-breakeven sensitivity analysis shows, mining metrics' sensitivities change rapidly as the market evolves. The hedge ratios of each instrument need to constantly be refreshed. Managing it requires close monitoring and making frequent adjustments. However, there are lots of restraints such as poor liquidity and pricing obscurity. Traders need to understand exactly what kind of slippage and discount factors they need to take into risk calculations. By structuring a virtualized hashpower portfolio instead of running a mining

operation, the investor effectively exchanges mining operational risks with additional financial risks.

As for miners, a new way to hedge their exposure is through **hashpower forwards**. Similar to renting hashpower on cloud mining platforms, forward contracts let the miner sell a fixed amount of hashpower for a period of time, for an upfront price. Unlike cloud mining, they are usually structured over-the-counter, and have higher customization flexibility. However, without a public benchmark, the forward market doesn't have any established pricing framework. Every deal turns into a negotiation, and the desk that execute the trade inevitably has to take on some market risks. A recent high-profile success is the BitOoda transaction with CoinMint, a large mining operation based in New York.

These deals will happen more frequently as more exchanges / financial services vertically integrate with mining pools. Mining pools are excellent aggregators of miners traffic, but after years of development they have turned into commodity software. Everyone wants miners' trading flow. The deep liquidity reserve of the exchanges allows them to offer creative and potentially risky transaction types to win over miners' trading flow. Miners can set parameters to always sell a percentage of their hashpower to lock-in the payment for operating expenses, and the counterparty receives the stream of coins produced by that hashpower from the pool. For instance, the miner can pre-sell 100Th/s for 30 days at the beginning of the month. Based on estimated difficulty growth and fees assumptions, the pool offers to pay 0.02 BTC upfront. The miner locks in production of the 100Th/s for the entire month, effectively transferring production risks to the pool.



(Numbers are for illustrative purpose only)

Binance, OK, and Huobi are aggressively expanding their pool business to capture this market share. We expect to see other top exchanges to follow suit, or partner up with existing pool operators very soon. Besides exchanges, some lending firms and trading companies are also venturing in this direction: Babel Finance announced their Ethereum mining pool, Three Arrows Capital will offer structured products through Poolin. In the past, different layers of the cryptocurrency industry have been highly fragmented. Years of trials-and-errors standardizes and commoditizes key infrastructure layers. Some of these standalone infrastructures don't have defensible business models. Consolidation or verticalization is inevitable.

IV. Hashpower Investment Vehicles

Investing in mining is a full-time job. Most traditional investors and venture capitals don't have the bandwidth or the expertise to run machines or structure complex virtualized hashpower portfolios. **It's more common for them to get exposure to mining through mining SPV or mining companies.** 2019 started with an explosion of overhyped GPU-launched projects. Rumors about deep-pocketed VCs investing hundreds of millions in Grin spread like wildfire. GPU farms that had bitten dust in the last quarter of 2018 were resurrected to ride the wave. Investors wanted to build large positions but did not have the manpower or technical expertise to run machines, causing them to pool capital together to fund mining operations. Managers of the SPVs source and run machines with the investors' initial investments, and in exchange take a percentage of the mining revenue.

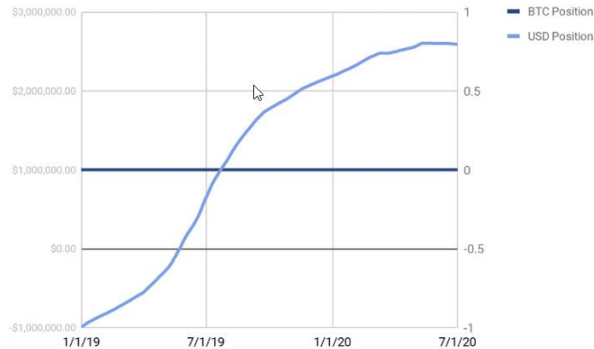
Investing in mining companies is also common for large BTC operations. Some of them are already publicly traded. Mining companies generate bulks of coins every day. A mining operation is effective both as a hardware operator and a liquid fund manager. There are numerous well-capitalized mining projects that failed due to mismanagement of trading positions. A notorious example is Gigawatt in 2018. According to the court case documents, the company had "*estimated assets worth less than \$50,000, whereas estimated liabilities are in the range of \$10–50 million.*" by the time it declared bankruptcy.

How the operators manage cash flow is imperative. Developing a reasonable selling strategy to counter changes in market conditions is critical to the fund / company's financial success. Here we illustrate the backtesting outcomes of four typical strategies:

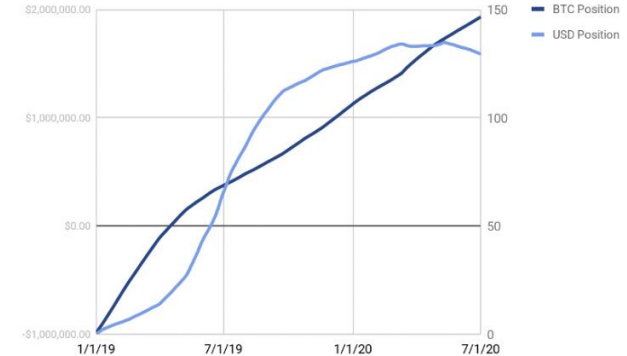
Assumptions

- *Starting date: 1/1/2019*
- *Valuation date: 7/1/2020*

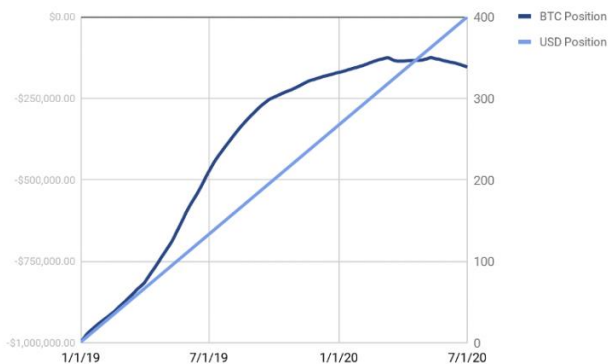
- Initial investment: \$1,000,000
- Number of machines: 4840 units of S9s, purchased at \$206.6 per unit. Linearly depreciating over 18 months.
- Total hashpower: 67,761 Th/s
- Total power consumption: 6,389KW
- All-in rate: \$0.04 / Kwh

Strategy 1*Sell all BTC mined everyday*

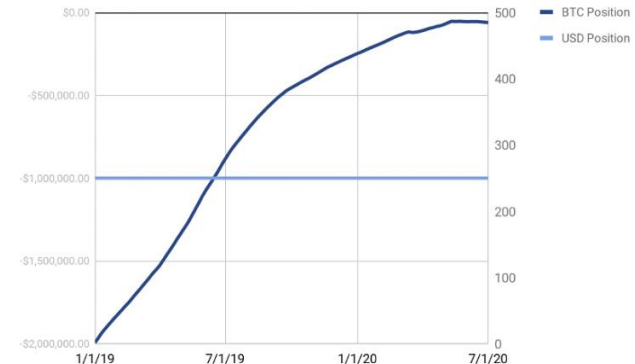
Final BTC Position: 0 BTC
 Final USD Position: \$2,588,377
 Fair Market Value: \$2,588,377

Strategy 2*Sell BTC to cover operating expenses and capture net profit in USD*

Final BTC Position: 146.6 BTC
 Final USD Position: \$1,588,377
 Fair Market Value: \$2,943,191

Strategy 3*Sell BTC to cover operating expenses and daily depreciation.*

Final BTC Position: 338.4 BTC
 Final USD Position: \$ -
 Fair Market Value: \$3,127,161

Strategy 4*Sell BTC to cover operating expenses.*

Final BTC Position: 484.99 BTC
 Final USD Position: \$(1,000,000.0)
 Fair Market Value: \$3,481,974.0

The strategies illustrated above represent different risk preferences for BTC vs. USD positions. **Note that in a different market environment, the strategy that yields highest return may be the least profitable.** Some miners prefer to hodl regardless of the market conditions until they absolutely have to sell. Depending on the manager's objective (accumulate BTC or chase USD return), the strategy should be adjusted accordingly. Mining operations equipped with sophisticated prop traders can also sell

rewards and buy them back when price drops below cost-of-production, or use a combination of financial instruments such as collateralized lending, or Bitcoin futures, to protect downside risks. We will cover this topic in greater depth in a future article on *hashpower financialization and risk management*.

Summary of the hashpower asset class:

	Physical ←————→ Virtualized					
	Mining Machine	Mining Machine	Hashpower Forwards	Cloud Mining	Mining Fund / Company	Tokenized Machines
Source	Manufacturer	Secondary Market	Exchange-integrated Pool	Cloud Mining Platform	Individual Fund / Company	Machine Token Exchange
Asset Type	Hardware	Hardware	OTC contract	Security	Security	Security
Underlying Assets	Mining Machines	Mining Machine	X amount of hashpower for Y number of days	X amount of hashpower for Y number of days	Shares	Tokens
Upfront Capital Requirement	High	High	High	Low	Depends	Low
Operating Expense	High	High	None	None	None	None
Operation Risk	High	High	Low	Low	High	None
Price-discovery Mechanism	Direct deal	Network of brokers	Direct deal	Platform sets the price	Direct deal	Public exchange
Liquidity	Poor	Poor	None	None	None	Medium

In Part II, we will describe the internal logics of the variables that drive the trends in mining, and present how reflexivity plays out in the hashpower market. We will break down the cyclic macro patterns that emerge from these intricate interactions, and use real market examples to illustrate their ebbs and flows.

Debunking Common Bitcoin Myths

By Yassine Elmandjra on ARK Invest

Posted June 26, 2020

More than eleven years after its creation, Bitcoin is struggling to gain widespread institutional acceptance. While constructive criticism is healthy, ARK believes that some influential financial research institutions are dismissing bitcoin based on stale information, incoherent arguments, and flawed analysis.

Given Goldman Sachs' recent stance on Bitcoin, ARK is revisiting the most common misperceptions weighing on its acceptance. We look forward to participating in healthy and educational debates about bitcoin and the important role we believe it deserves in well-diversified portfolios.

ARK believes that some influential financial research institutions are dismissing bitcoin based on stale information, incoherent arguments, and flawed analysis.

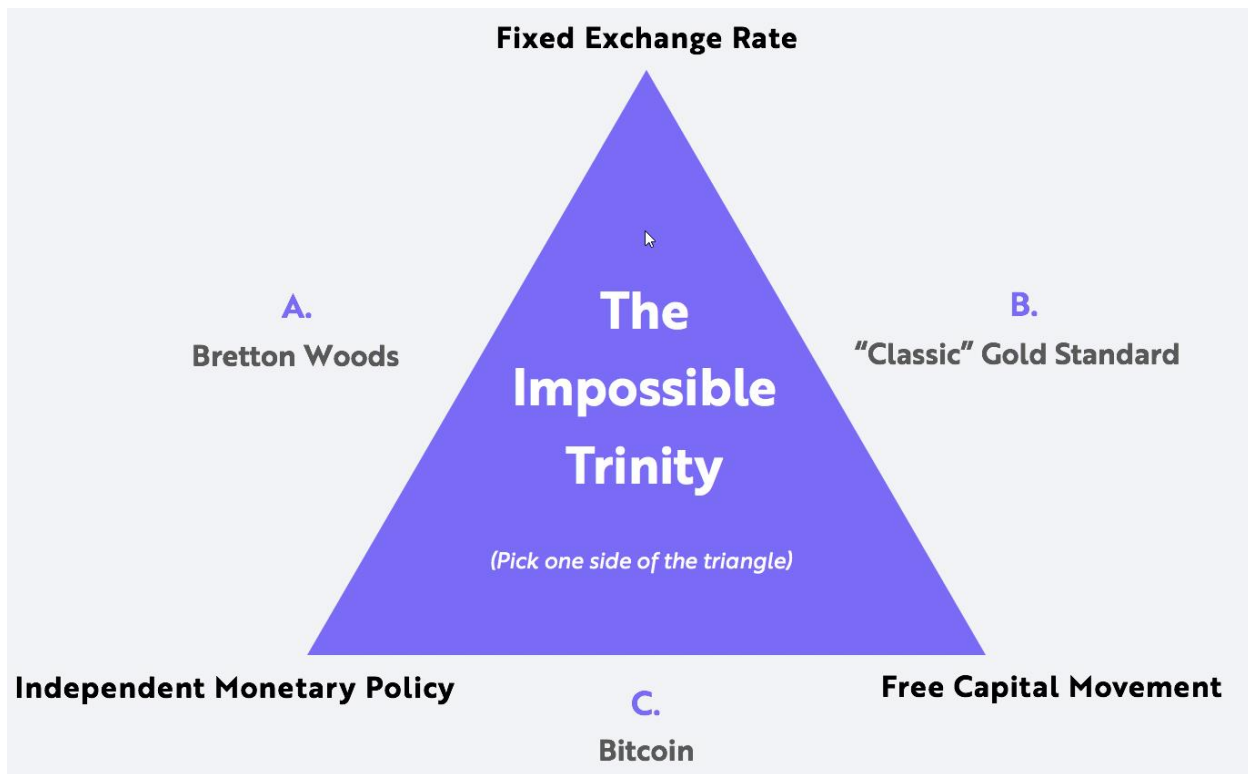
Claim: bitcoin is too volatile to serve as a store of value.

Counter-Claim: bitcoin's volatility highlights the credibility of its monetary policy.

Critics often point to bitcoin's volatility as a "store-of-value deal breaker." Why would anyone want to store value in an asset with such dramatic swings in its day to day price?

In our view, these critics do not understand why bitcoin is volatile and why its volatility is likely to diminish.

While distracting naysayers from assessing its role as a store of value, bitcoin's volatility actually highlights the credibility of its monetary policy. The Impossible Trinity, a macroeconomic policy trilemma, explains why. As illustrated below, the trilemma postulates that, when formulating monetary goals, policymakers can satisfy two out of three objectives, not all three, as the third will contradict one of the first two.



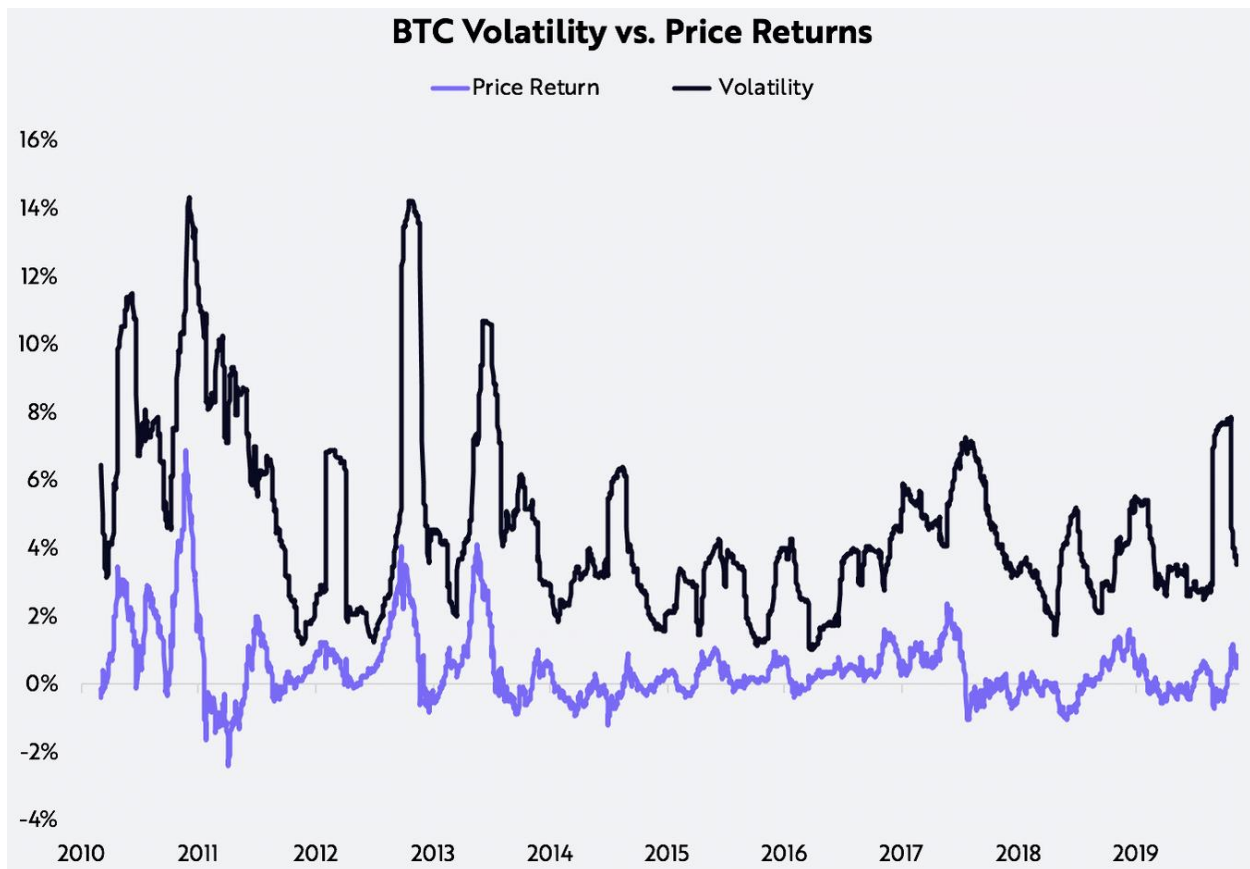
Source: ARK Investment Management LLC, 2020

Each side of the trilemma triangle is mutually exclusive to the others. A monetary authority choosing to fix exchange rates and allow the free flow of capital, for example, cannot control growth in the supply of money. Likewise, a monetary authority choosing to fix exchange rates and control money cannot accommodate the free flow of capital, and one choosing to accommodate the free flow of capital and control the supply of money cannot fix exchange rates.

Based on the trilemma, we can understand why volatility is a natural consequence of Bitcoin's monetary policy. In contrast to modern central banking, it does not prioritize exchange rate stability. Instead, based on a quantity rule of money, Bitcoin limits the growth of money supply and allows the free flow of capital, forgoing a stable exchange rate. As a result, bitcoin's price is a function of demand relative to its supply. Its volatility should come as no surprise.

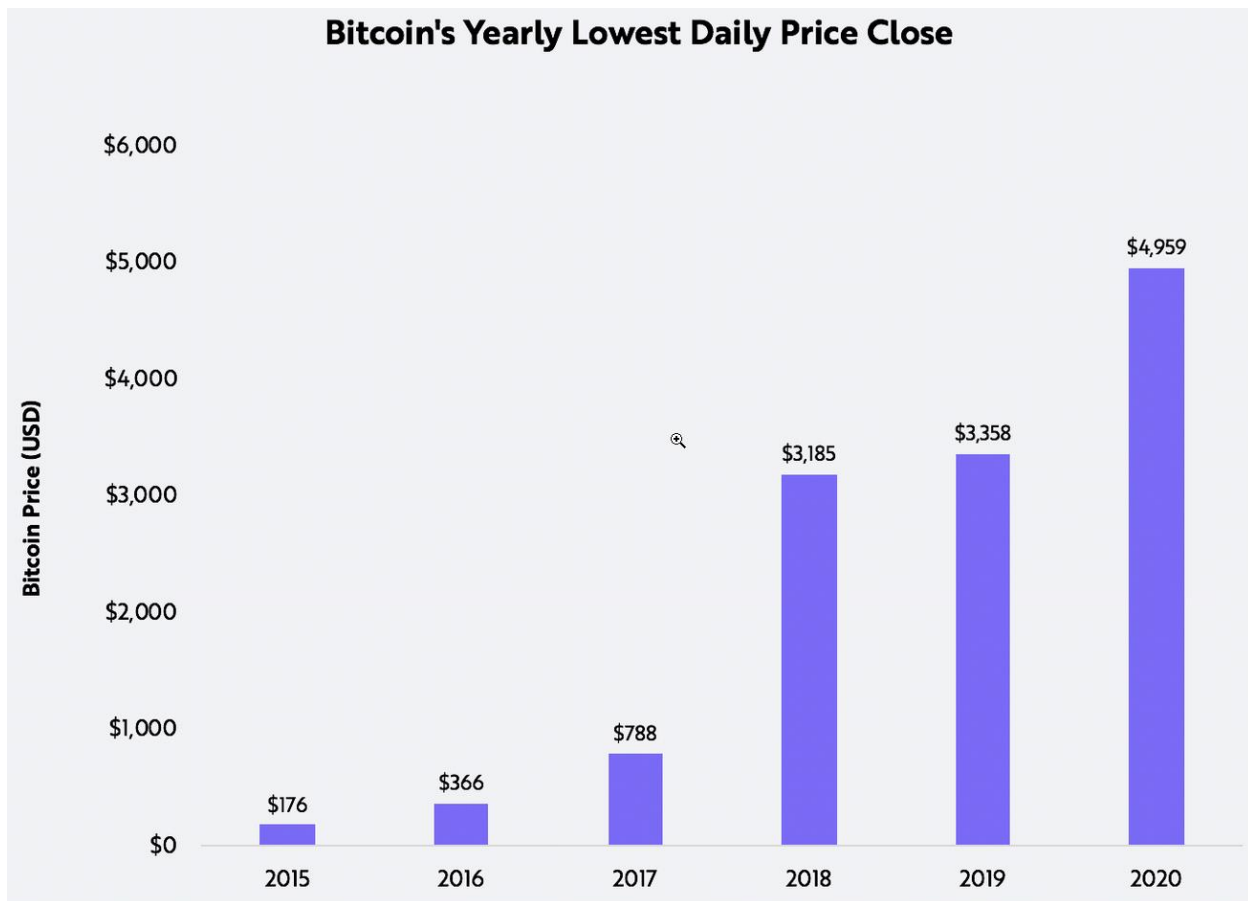
That said, bitcoin's volatility is diminishing over time, as shown below. As its adoption increases, the marginal demand for bitcoin should become a smaller percentage of its total network value, diminishing the magnitude of price swings. All else equal, for example, \$1 billion in new demand on a \$10 billion market capitalization, or network value, should impact bitcoin's price more significantly than \$1 billion in new demand on a \$100 billion network value. Importantly, we believe volatility should not preclude bitcoin as a store

of value, primarily because it typically has coincided with significant upward moves in its price.



Source: ARK Investment Management LLC, 2020. Data Source: Coinmetrics

Over long time horizons, bitcoin's purchasing power has increased significantly. Since 2011, for example, the price of bitcoin has compounded at an annual rate of roughly 200% and, despite significant intra-year moves, it has appreciated on a year-over-year basis every year since 2014 as measured by its lowest value of the year.



Source: ARK Investment Management LLC, 2020. Data Source: Coinmetrics

Claim: bitcoin is in a bubble.

Counter-Claim: bitcoin is a contender for the role of a global money.

Some economists like [Nouriel Roubini](#) argue that bitcoin is in a bubble that will pop and disappear. The line of reasoning is that bitcoin has no intrinsic value, its appreciation dependent on speculation like a game of hot potato or tulips and “a greater fool” willing to pay a higher price. In their view, bitcoin is not an investable asset.

We believe this argument dismisses the reason why bitcoin accrues value over time. True, bitcoin does not behave like a traditional investable asset.^[1] Equity values are determined by discounting expected cash flows. Given higher future cash flows based on growth and/or returns on invested capital, equities appreciate independent of their shareholder bases.

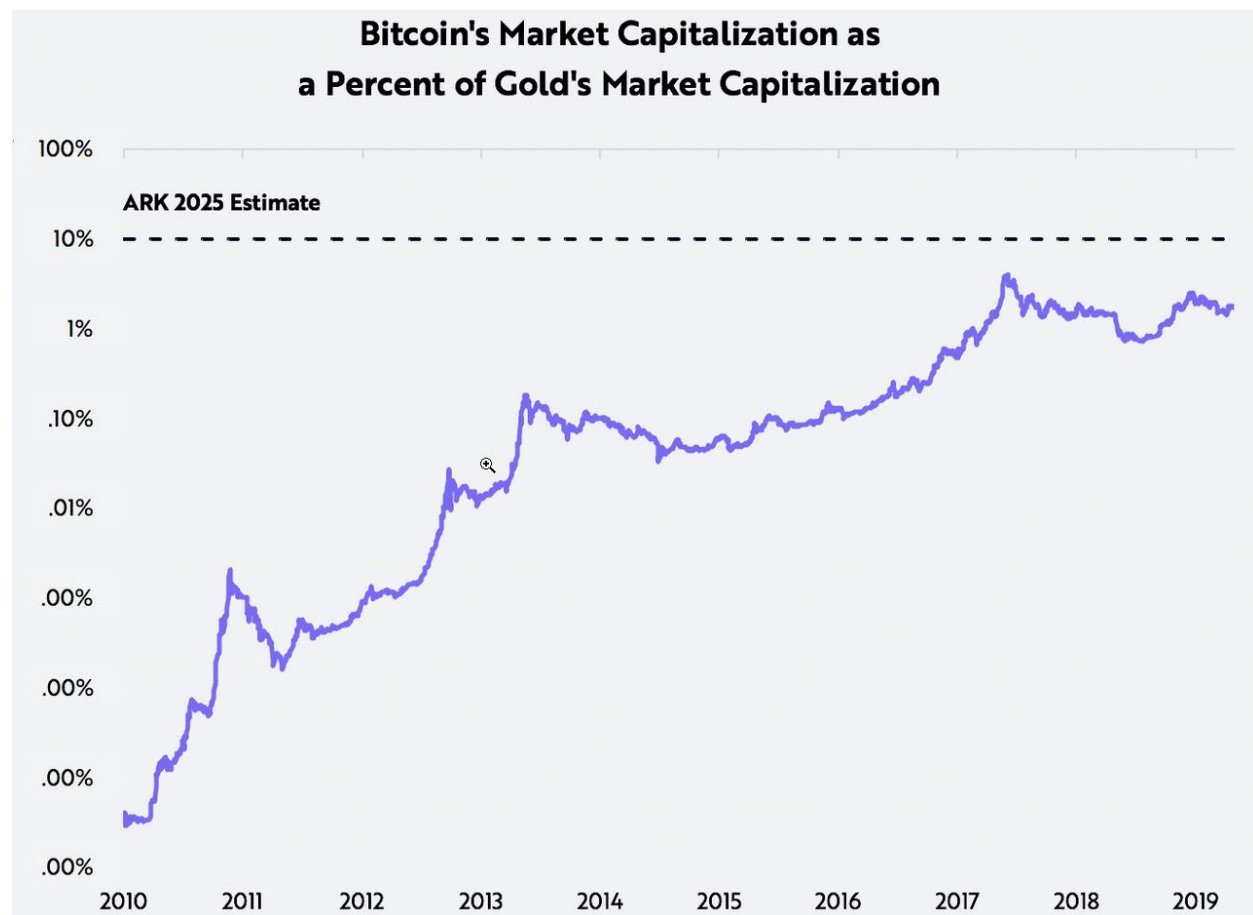
A monetary asset like bitcoin, however, is nonproductive, its appreciation based on how effectively it preserves or enhances value over time. In a way, the value proposition is circular: a monetary asset will appreciate as more people demand it, and more people will demand it if it is an effective

monetary asset. In other words, “money is a shared illusion” and “money is valuable because others believe it is valuable”.

Claims that the value of money relies exclusively on a shared illusion, however, suggests that its form is arbitrary. In reality, according to monetary history, the most common and sustainable monies possessed qualities that sustained their demand. For thousands of years, for example, economists have recognized gold as the most successful form of money, thanks to its scarcity, fungibility, and durability.

Often called digital gold, we believe bitcoin not only shares many of gold's characteristics but also improves upon them. While scarce and durable, bitcoin also is divisible, verifiable, portable, and transferable, a range of monetary characteristics that confer superior utility, potentially driving demand and deeming it suitable, if not superior, for the role of global digital money.

We believe as a suitable contender for the first global digital money, bitcoin should attract demand similar, at a minimum, to that for gold. Yet, contrary to claims that it is in a massive bubble, bitcoin's network value – or market cap – is less than 2% that of gold's, as shown below.



Forecasts are inherently limited and cannot be relied upon.

Source: ARK Investment Management LLC, 2020. Data Source: Coinmetrics

Claim: bitcoin will lose value to ‘forks’ and digital copies.

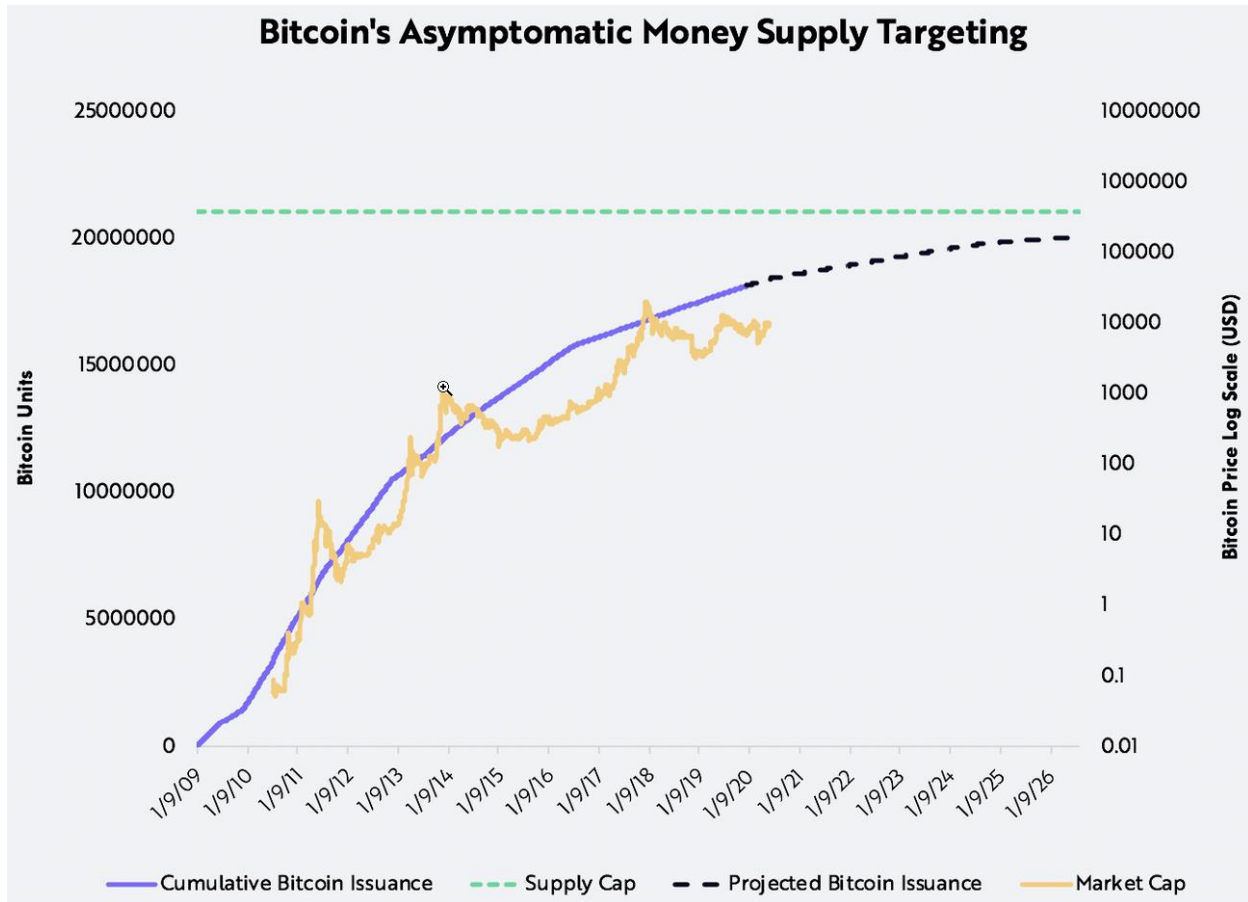
Counter-Claim: bitcoin’s value cannot be replicated by software alone.

In the digital realm, goods are intangible and can be copied easily without destroying the original. An individual can email a word document widely, for example, while preserving the original copy. Likewise, millions of people can listen to a song simultaneously and repetitively, actually enhancing the value of the original, especially as other songwriters mimic its differentiated sound.

Bitcoin’s software is no different. It is free and open source. Individuals can copy the software, “forking the network” and creating their own version. Yet, skeptics still ask how bitcoin can be scarce if it is based on open source software that can be copied ad infinitum?

First, forking the Bitcoin network does not create new bitcoin units, much like inflating the Venezuelan bolivar does not add dollars to the US monetary base. Instead, forking Bitcoin creates a new network with new units or coins. While existing bitcoin holders have rights to the new coins, the forked network operates under an independent set of rules supported by unique stakeholders. Instead of diluting the money supply of the original network, open source software encourages not only inexpensive experimentation and new networks, but also new coins and a competitive market.

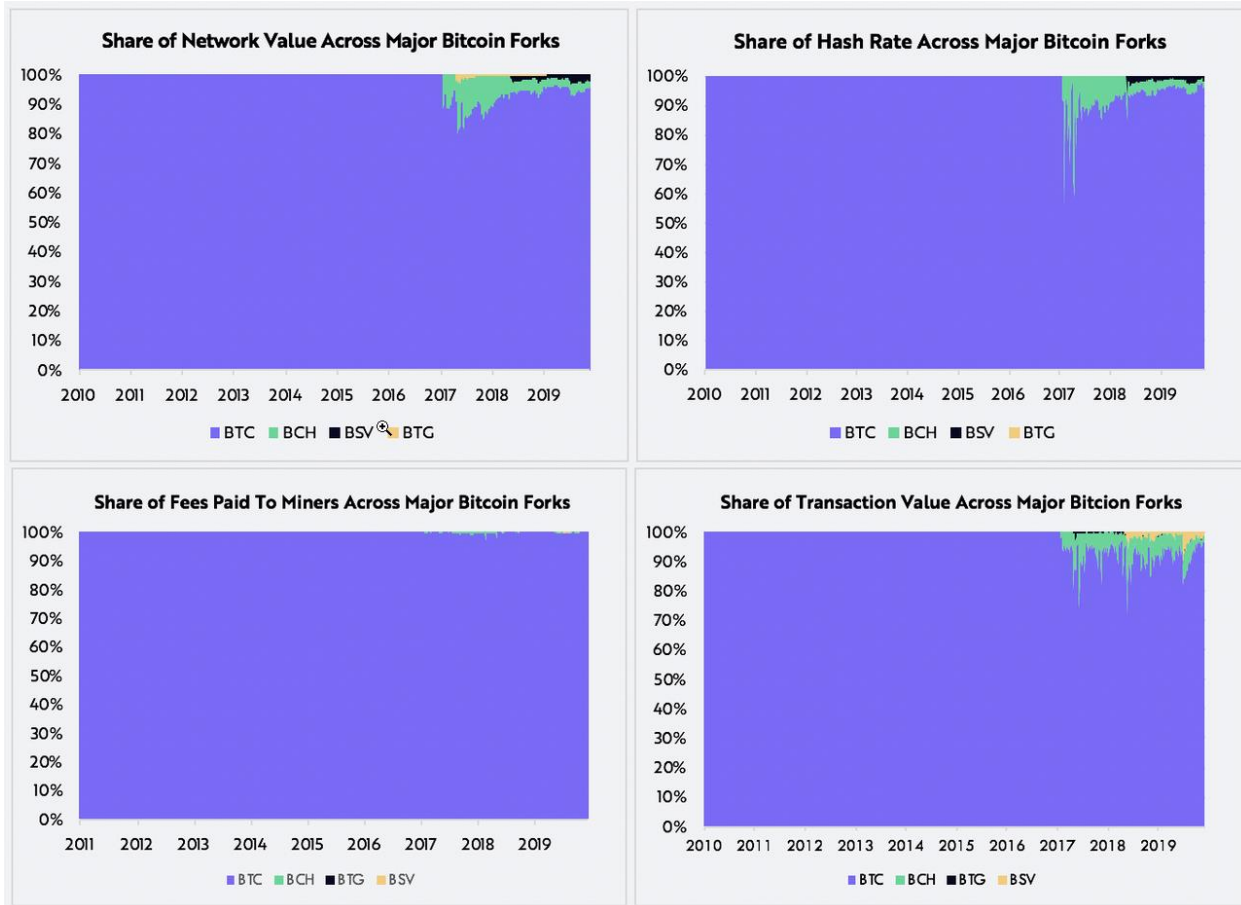
Bitcoin’s scarcity is critical to its network. Now at 18 million units, the number of bitcoin is mathematically metered to top out at 21 million units, as shown below. Each bitcoin is linked to one wallet at a time and cannot be copied. Importantly, the only way to control a user’s bitcoin is to have access to its associated private key.



Source: ARK Investment Management LLC, 2020. Data Source: Coinmetrics

So, as it forks, what makes the 21 million units in Bitcoin's network more valuable than the 21 million units in a Bitcoin (BTC) fork like Bitcoin Cash (BCH)? Equating the value of Bitcoin Cash to the value of Bitcoin would be equivalent to assuming that Facebook's source code could "fork" and automatically duplicate the value of its 2.6 billion users and 50,000 employees. Their value stems from Bitcoin's and Facebook's network effects, not just their existence.

In the case of Bitcoin, we believe network effects include not only the hashrate dedicated to securing the blockchain, but also bitcoin's liquidity and the infrastructure supporting its adoption and usage. If dilutive, the fork would have to take share of Bitcoin's hashpower, users, and liquidity. As shown below, Bitcoin Cash and other forks appear to have failed to derail Bitcoin's network effect.



Source: ARK Investment Management LLC, 2020. Data Source: Coinmetrics

Claim: Bitcoin is for criminals.

Counter-Claim: Bitcoin is censorship-resistant.

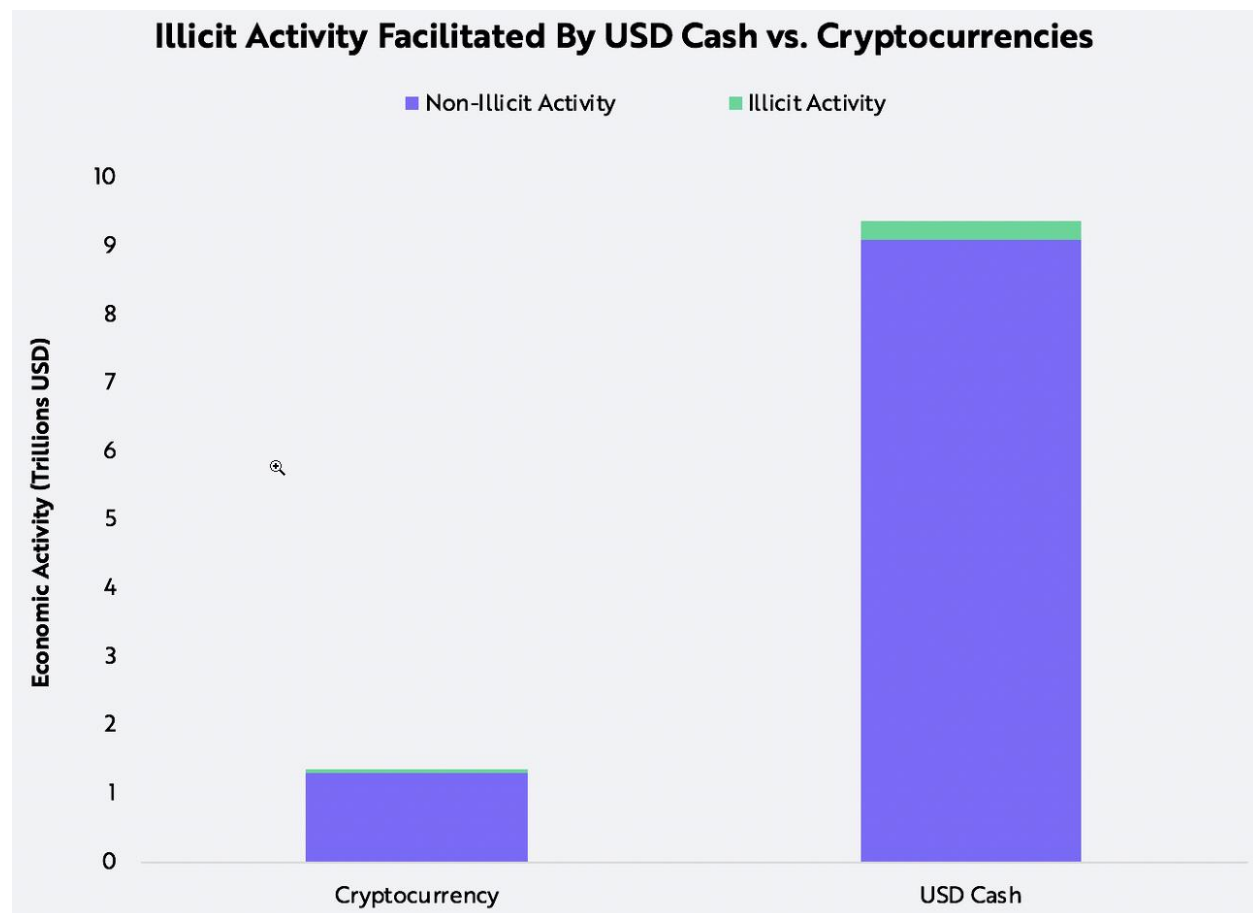
Critics still accuse Bitcoin of enabling criminal activity because of nefarious activity in its earliest days. In its first few years, bitcoin financed the Silk Road, an online black market platform best known for selling illegal drugs.

We believe that to criticize Bitcoin for facilitating criminal activity is to criticize one of its fundamental value propositions: censorship-resistance. As a neutral technology, Bitcoin allows anyone to transact and cannot identify “criminals”. Instead of relying on a centralized authority to identify participants by name or IP address, it distinguishes them by cryptographic digital keys and addresses, conferring upon Bitcoin strong censorship-resistance. As long as participants pay fees to miners, anyone can transact anywhere at any time. Once secured, the transaction cannot be easily reversed.

If criminal activity could be censored on the Bitcoin network, then all activity could be censored. Instead, Bitcoin enables anyone to exchange value globally and permissionlessly. This does not make it an inherently criminal

tool. Phones, cars, and the Internet are no less bannable for facilitating criminal activity than Bitcoin is.

That said, it appears that only a small percentage of bitcoin transactions are for illicit purposes. According to Chainalysis, the number of bitcoin transactions linked to illicit activities remains below 1%, perhaps a tribute to Bitcoin's transparency. Any user can view the complete history of transactions on the network, suggesting that physical cash is the better medium for illicit activity. Indeed, as indicated below, cash transactions account for a larger share of illicit activity than do cryptocurrency transactions, on both absolute and relative terms.



Source: ARK Investment Management LLC, 2020. Data Source: <https://go.chainalysis.com/rs/503-FAP-074/images/2020-Crypto-Crime-Report.pdf>

Claim: Bitcoin wastes too much energy.

Counter-Claim: Bitcoin's energy consumption is more efficient than that of gold and traditional banks.

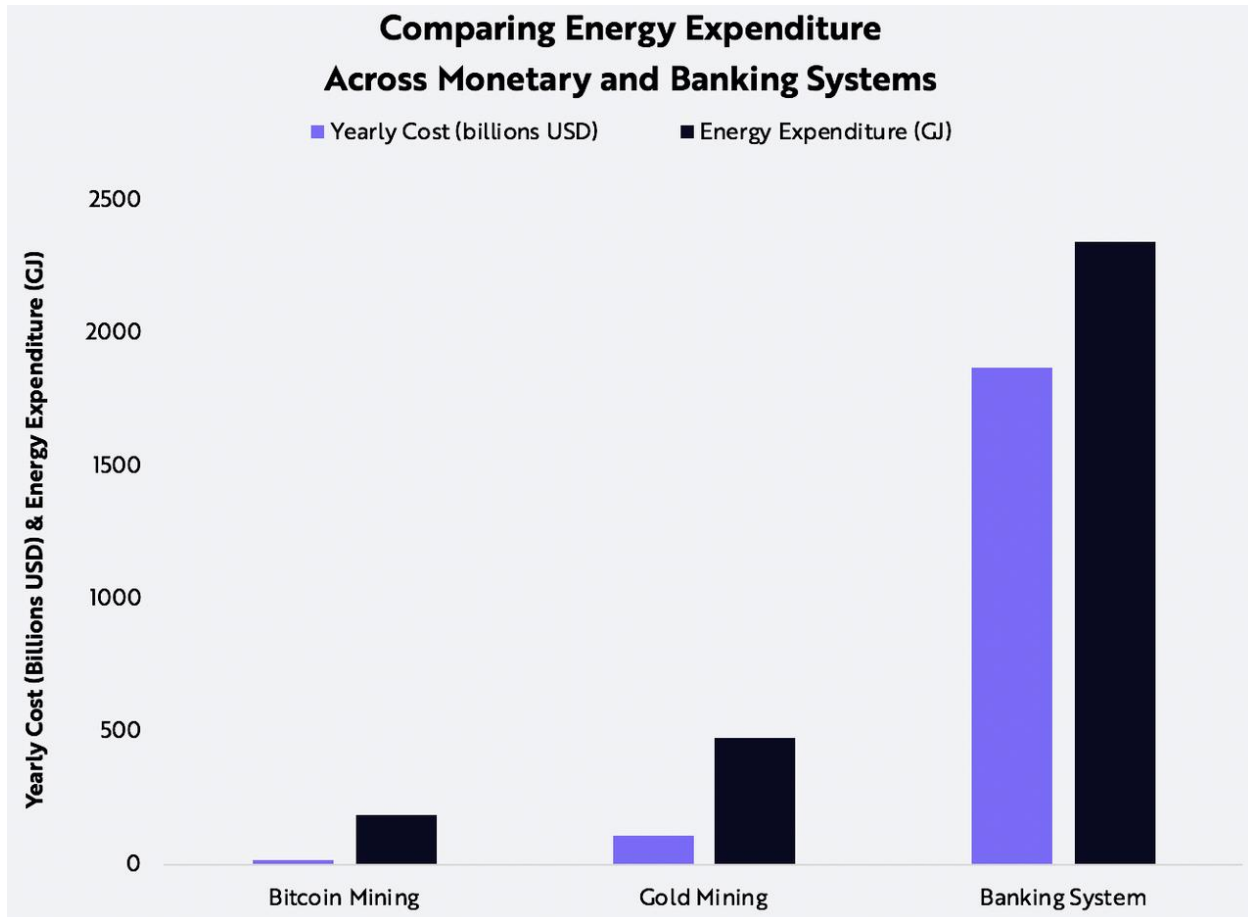
Bitcoin critics often assert that mining consumes more resources, specifically energy, than the benefits it creates. What critics deem computationally

inefficient and unscalable, however, advocates consider not only an intended tradeoff but a fundamental feature. As highlighted by founder of Bit Gold and Bitcoin pioneer, Nick Szabo, “Prolific resource consumption and poor computational scalability unlock the security necessary for independent, seamlessly global, and automated integrity.”

ARK believes that Bitcoin has a unique ability to provide settlement assurances in a decentralized – or trust-minimized – manner because specialized, dedicated hardware proves transparently that the computer has executed a costly computation.

Bitcoin makes the tradeoff explicit: by allocating significant real-world resources to mining, we believe the network guarantees settlement like none other. In The Anatomy of Proof of Work, Chaincode Labs resident Hugo Nguyen explains, “Under the hood, proof-of-work mining converts kinetic energy (electricity) into a ledger block. By attaching energy to a block, one gives it ‘form’, allowing it to have real weight and consequences in the physical world.”

Easier to quantify, Bitcoin’s energy footprint is open to superficial criticism. However, as measured by electricity costs alone, Bitcoin is much more efficient than traditional banking and gold mining on a global scale. Traditional banking consumes 2.34 billion gigajoules (GJ) per year and gold mining 500 million GJ, while Bitcoin consumes 184 million GJ, less than 10% and 40% of traditional banking and gold mining, respectively. Additionally, Bitcoin mining’s estimated dollar cost per GJ expended is 40 times more efficient than that of traditional banking and 10 times more efficient than that of gold mining.



Source: ARK Investment Management LLC, 2020. Data Source:
<https://medium.com/@danhedl/pow-is-efficient-aa3d442754d3>

Contrary to consensus thinking, we believe the environmental impact of bitcoin mining is di minimis. Renewables, particularly hydroelectric power, accounts for a large percentage of bitcoin's energy mix. As Castle Island Ventures partner, Nic Carter, has noted, in their search for the cheapest form of electricity, miners will continue to flock to regions offering a glut of renewable electricity, unlocking stranded energy assets as "electricity buyer[s] of last resort, creating a highly mobile base-demand for any electricity sources able to produce at prices below current producers, regardless of location." As a result, from a climate perspective, bitcoin mining could be a net positive.

Conclusion

Bitcoin's complexity should not prevent financial institutions from analyzing it in depth. In this piece, we have discussed some of the most common objections to Bitcoin, hoping to stir conversation and debate in the institutional investment community. As the Bitcoin network continues to mature, we believe that it will cement bitcoin's role as an

emerging monetary asset and that financial institutions will do well to consider it seriously.

- 1 In the absence of hard forks or airdrops.
-

Bitcoin: Separating Money From State

With the introduction of Bitcoin, we discuss the key achievement and massive win for the people of today: the separation of money from the state.

By Pedro Febrero

Posted July 29, 2020

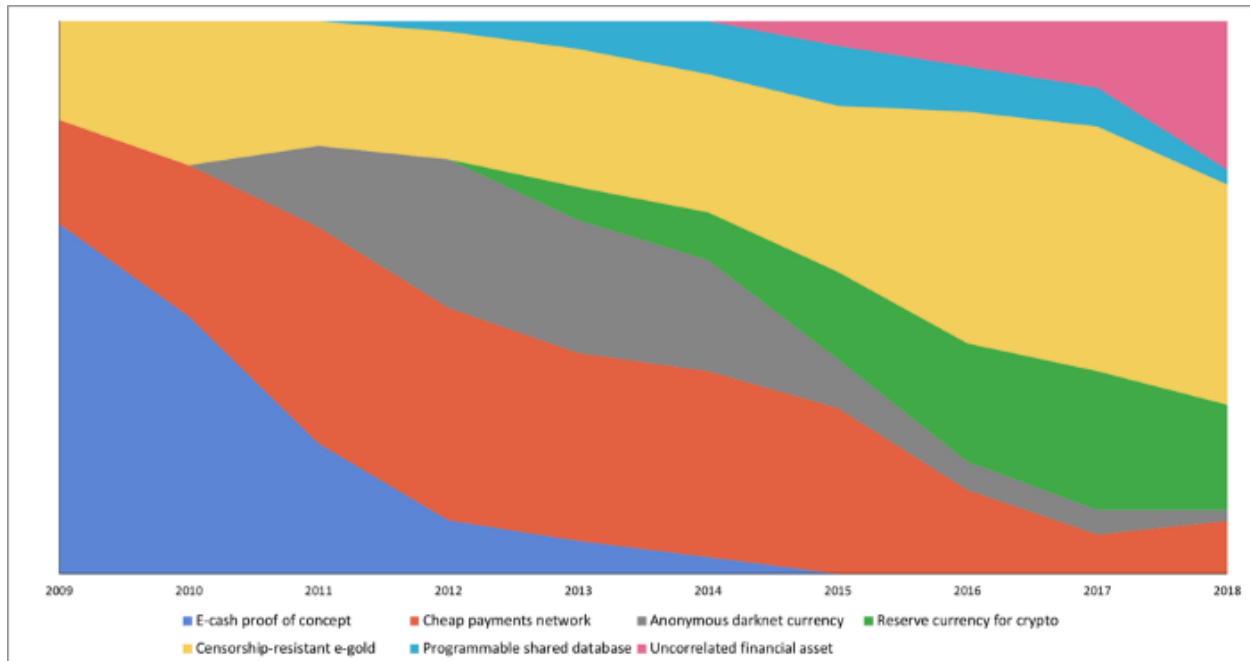
Image: Author

Today our goal is to give readers a comprehensive analysis of what makes Bitcoin unique and how this digital commodity may break the shackles of state currency.

We will look into how the Bitcoin network has evolved, from a simple payments network, to digital gold; the reason why Bitcoin is, in fact, a living organism that adapts to new situations and overcomes any challenge that crosses its way; and, finally, the path Bitcoin must take to conquer the entire digital space.

Only now, 10 years after the creation of Bitcoin, the picture of themes brewing around the cryptocurrency starts to take shape. Nic Carter wrote one of the most important pieces to describe the narratives surrounding Bitcoin. Below you can see the juice of his ideas: the evolution of Bitcoin as an e-cash proof of concept toward an uncorrelated financial asset.





Hasufl and Nick Carter's "Visions of Bitcoin"

What Carter concluded, and we tend to agree with him, is that Bitcoin is not just a technology, and it does not represent a single narrative. Markets and the "crowd" define the narratives behind what any asset is, and Bitcoin is clearly a colourful melting pot of ideas.

It went from being an e-cash proof of concept from 2009 until 2015, from anonymous darknet currency from 2010 until 2018, while today, Bitcoin still aims to be a cost-effective payments network, perhaps through the Lightning Network, and a censorship-resistant e-gold.

We cannot state for sure whether those narratives will die off, much like e-cash and darknet currency did, or whether they'll survive and mingle with the reserve currency for crypto, programmable shared database and, most recently, uncorrelated financial asset narratives.

What Carter helps readers understand is how easy it is to change a narrative around a technology, especially one that separates money from the state.

But let's not get ahead of ourselves.

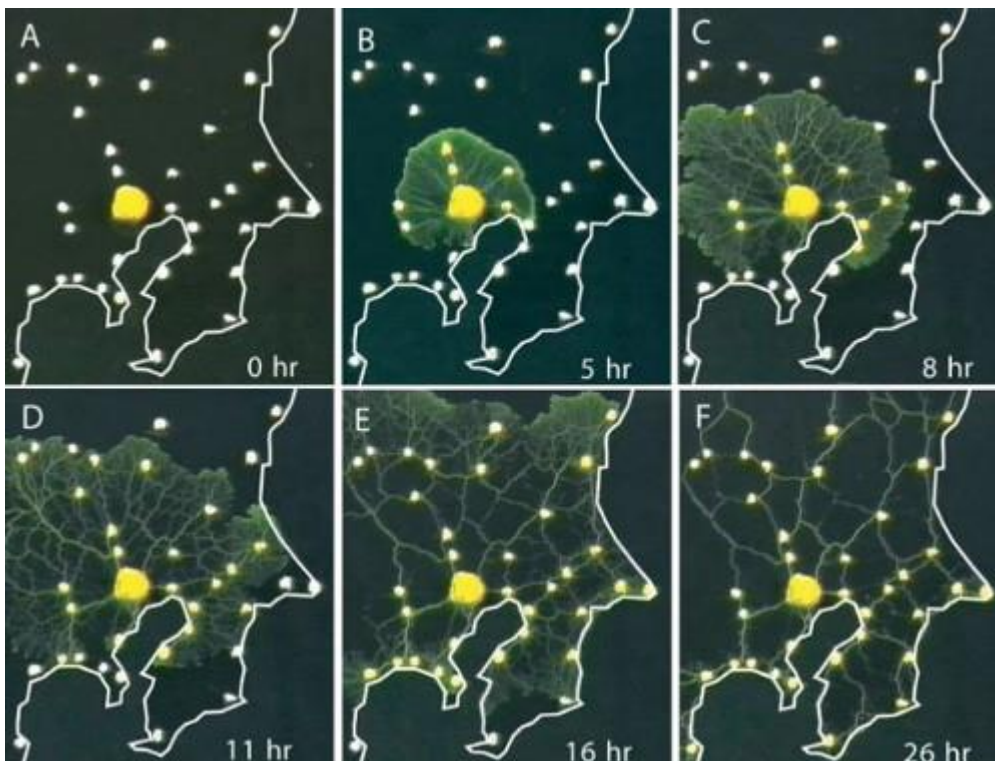
Bitcoin, a living organism

To come from such humble means, much like cheap payments and darknet currency, to global crypto reserve currency or censorship-resistant digital gold, Bitcoin had to evolve.

What we want to emphasize is that the community that supports the technology changed gears, and understood how one simple proof-of-work cryptocurrency could, in fact, change paradigms: Slowly, but surely.

Indeed, Bitcoin had to metamorphose from its initial larva state into a butterfly.

The narratives prove that Bitcoin wasn't initially seen, or discussed, as a potential replacement for central banks, by the majority of early adopters. Further, they didn't note that it possessed sound-money properties, or that it could be the first worldwide settlements network.



Slime Mold designing Tokyo Subway System, image by Brandon Quittem

Great things take time to build. Let's take a look at nature, as a source of inspiration. One of the most astonishing organisms living on this planet is mycelium, a communication layer between fungi. Mycelium helps fungi communicate

across vast regions. However, it took fungi millions of years to develop such a complex mycelium network. Such is the fate of any great and overachieving technology: it takes time to build and adopt. And BTC is no different.

Brandon Quittem showed us exactly that, in his brilliant research papers comparing the Bitcoin network to a living organism (fungi, mushrooms).

An example we would like to pick up is how decentralized networks can, in fact, be considerably more efficient at resource allocation than centralized networks when it comes to decision-making.

"Scientists conducted an experiment where an ancient fungus (slime mold) was incentivized to recreate the Tokyo subway system. Each subway stop (node) was marked with the slime molds favorite food (oat flakes).

After a short while, the slime mold grew to connect all the nodes/stops in a more efficient design than the centrally planned committee of engineers hired by the Japanese government.”

Isn't it amazing that fungi could be smarter than scientists?

Of course, this is an example that we've stretched a bit, in order to show how decentralized networks can have better results than a traditional top-to-bottom decision-making process.

However, the path to global adoption of bitcoin is painful, full of ups and downs, where problems such as critical software bugs and overreaching regulation will most likely happen. Therefore, one should be patient and keep a macro, long-term perspective on the development of the Bitcoin network.

Image by author



Bitcoin: The Road To Independence

Before we dig deep into the core subject of the paper, we would like to explain why Bitcoin is the de facto asset which could change the way the world operates.

In the introduction, we spoke of a great number of qualities Bitcoin possesses, which makes it an incredible foe to central banks, settlement layers and other payments and financial institutions.

Bitcoin opened the doors to digital scarcity. With digital scarcity, we were able to build sound-money-

like assets — which are deflationary or disinflationary, as the brilliant Jason Deane explains in this piece.

With scarcity built in a sound-money-like digital asset (aka, bitcoin), there is a chance a new system can take a run at being the internet currency. Above all, the fact this asset's transactions are transparent while the rules of the protocol are quite easy to enforce and verify, but expensive to change, helped the Bitcoin network to grow.

More, however, Satoshi implemented an anti-inflationary measure, known as the halving, which takes place roughly every four years.

Not only that, but bitcoin gave birth to triple-entry bookkeeping. If you are wondering why triple-entry bookkeeping is much more interesting than double-entry bookkeeping, we'll give you the juice of it.

Essentially, while double-entry bookkeeping requires each party transacting to keep a record of the ledger, for comparison by a third-party (like a government body such as the IRS), triple-entry bookkeeping is much simpler to audit, since transactions from all parties are stored in a common, shared and public ledger.

All these unique developments kick-started the decentralized finance (DeFi) space (sorry Ethereum. But Bitcoin is the original #DeFi).

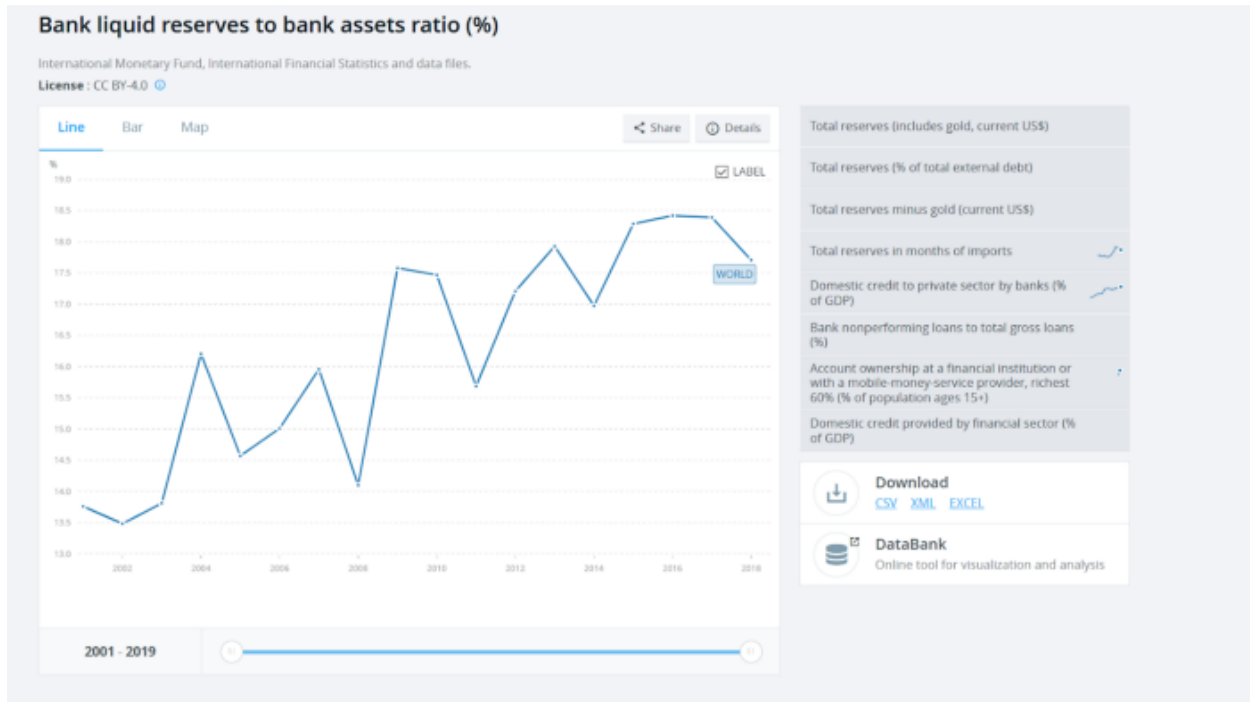
However, the greatest achievement of all is yet to come.

Bitcoin: Digital Hard Money

To fully understand concepts like open-source currency, digital sound money, DeFi, or the ability to store value digitally without a central entity controlling transaction flows and/or accounts, one needs to accept that money and the state are two separate entities.

The way currency gets created today is mostly through debt and deposits. What this essentially means is that either central banks mint new currency, which local governments buy through IOUs, or people put currency in a bank as a deposit or as debt, which also gives banks the ability to leverage those reserves and create new currency (credit) on top.

As of 2018, banks around the world held liquid reserves equal to 17.7% of their total assets, according to World Bank Data.



Bank Reserves Liquidity Ratio, by [World Bank Data](#)

Recently, the Fed lowered the reserve requirement ratio to zero, a move that may have some worried. In fact, many banks actually increased their reserves in the wake of COVID-19 in order to protect themselves from the eventual economic fallout.

Why is this bit so important? Because the way currency is created is only possible due to the actions of the government bodies.

The main reason behind the abolishment of the gold standard in 1971 is the same behind executive order 6102, which forbade Americans from owning gold: to give governments the power to print money.

However, there is more to money than simply being a currency.

The message we're trying to pass on is that sound-money, such as gold and bitcoin, exists in nature and cannot simply be printed. It's a hard asset because it requires much energy to mint an extra unit. What this means is that it's much more difficult for central banks to leverage deposits and to create "value" out of thin air, and for governments to keep increasing public debt.

Bitcoin: Separating Money From State

To conclude our thesis of why the separation of money and state is the most amazing invention of the 20th century, and how Bitcoin enables human beings to achieve such an outcome, we need to discuss some of the current

issues that exist with how currency is produced and some of the problems that arise from such a framework.



Jimmy Song (송재준)
@jimmysong

The only reason the (corporate) welfare state can exist is because of fiat money and fiat money has always been and always will be autocratic.

#Bitcoin  is our hope in a better system.

12:02 AM · Apr 24, 2020 · Twitter Web App

35 Retweets and comments 186 Likes

✓ Jimmy Song's twitter post

As Jimmy Song, a Bitcoin developer, teacher and author, explains in the tweet above, fiat currency is an autocratic system, where governments enforce the use of a certain currency within their borders.

One major problem of fiat currencies is that they can result in significant inflation, and in some cases, hyperinflation. Investopedia explains these difficulties rather effectively.

Additionally, by conveying the ability to mint currency to a select group of individuals, we give rise to other problems.



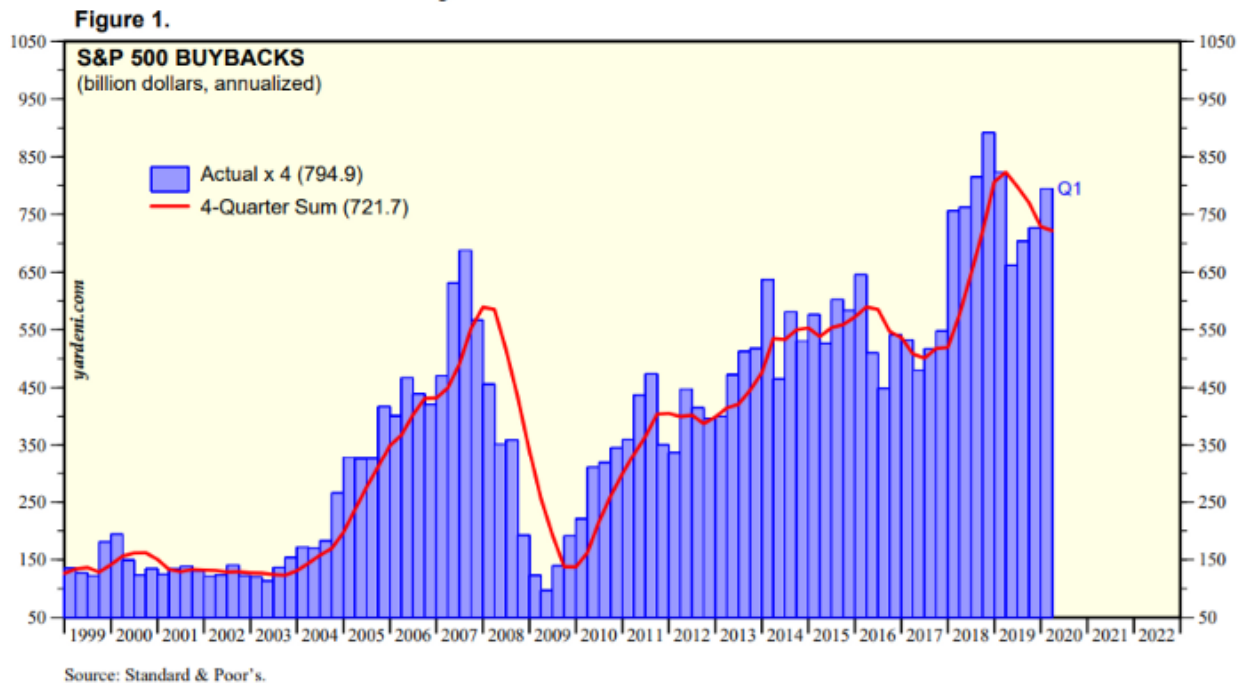
This chart shows the S&P 500 and the Dow Jones Industrial Average, 2008–2020 (Source: <https://www.tradingview.com/x/O5sPX7vu/>) Pink periods indicate quantitative easing. Blue periods indicate quantitative tightening.

As we've discussed previously, the measures being implemented by central banks worldwide, such as Quantitative Easing (QE), appear to favour the few over the many. As we discuss in this paper, where we took the chart from, QE seems to be quite correlated to the rising value of stock markets. In the example above, it seems there is a clear connection between QE periods and market cycles.

What QE gives birth to is currency and asset price manipulation by central banks, as we discuss in [this](#) article.

After all, only a minority of existing companies can create bonds and synthesize debt into financial products. Not only that, but such companies are usually publicly traded and have been using the extra cash to go into the markets and pump their own shares through share buybacks, as we can see below, courtesy of [Yardeni Research](#).

Buybacks & Dividends



Standard & Poor's, [S&P 500 Buybacks](#)

Now, if we can conclude currency is not being fairly distributed, as some people and companies are favoured instead of others, what can we do about that? Is there a meaningful way Bitcoin can really tackle this issue?

The short answer is: yes. Bitcoin does help.

If you take a look at [this](#) piece we wrote, discussing what the Cantillon Effect is, and how it takes place within the Bitcoin ecosystem, you'll notice we reach quite a staggering conclusion.

That bitcoin addresses holding large sums of BTC, over 1,000, are diminishing versus the number of addresses holding small sums, between 0.1 and one bitcoin.

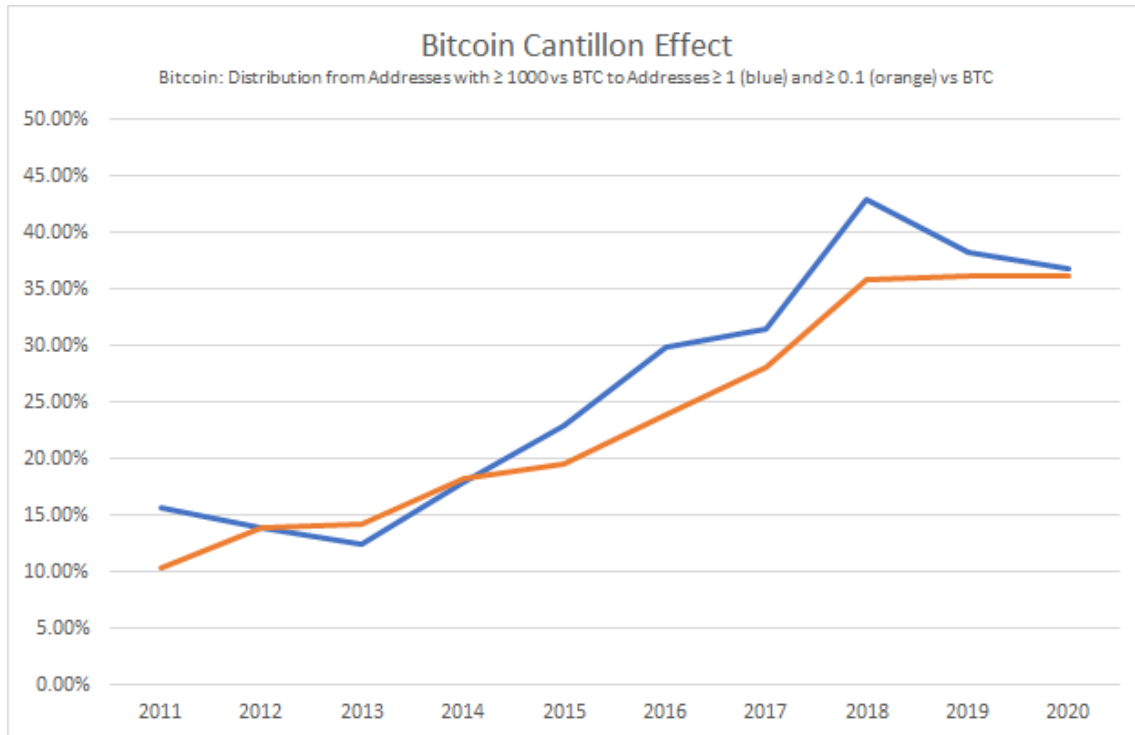


Image by author: The distribution of the volume of BTC held by addresses ≥ 1 and ≥ 0.1 versus addresses ≥ 1000 bitcoin

What the data shows is something rather spectacular. The percentage of the total bitcoin volume held by addresses with at least one and 0.1 bitcoin seems to be growing compared to the addresses containing a minimum of 1,000 bitcoin, which shows how evenly BTC is being distributed.

Since 2013, the number of bitcoin held by addresses with a minimum of one and 0.1 bitcoin more than doubled, from 15% to over 30%. At its peak, the amount of bitcoin volume held by addresses with at least one BTC was almost 45% of the total volume of bitcoin held by addresses with no less than 1,000 BTC. Interestingly, this top coincided with the BTC/USD all-time high.

In sum, the Cantillon Effect in the Bitcoin network is precisely the opposite to traditional currency networks: because no one can dilute your position by increasing the total currency supply (without a public minting schedule), your bitcoin isn't losing value.

Therefore, the satoshis you hold will never be diluted. This means the Cantillon Effect disappears with Bitcoin since no one can allocate extra currency, not planned in the protocol, to be minted and given to a group of people or companies. Bitcoin can only be minted the hard way: by producing valid proof-of-work.

Essentially, Bitcoin's greatest innovation was to completely separate money production from central banks and states. Perhaps, that was the greatest achievement of the century.

Conclusion

Before we conclude this piece, it's important to underline a key message recently shared by Ray Dalio, CEO of Bridgewater Associates.

In one of his latest interviews, Dalio mentions a key aspect most people tend to forget, that technology changes at a much faster pace than human behaviour, morals and values. Hence, the seemingly long time it takes for a technology such as Bitcoin to get massively adopted.

Think of the most important technologies developed to date. Think of the somewhat distant past.

The fact of the matter is only when humankind separated the church from the state, by inventing the printing press, we were able to kick-start the enlightened ages. Before that, science was virtually non existent and publications were dominated by the clergy.

The same logic can be applied to currency. While it remains linked to central powers, the ability for humans to truly be free will always be limited. Only when we accept, as a global species, that money should be decentralized and not linked to central institutions, can we perhaps dream of giving people an easy way to accumulate wealth across generations.

Bitcoin, being a digital hard-money native asset, fixes this problem. It takes away the ability of any government or central power to easily coerce their population by destroying local purchasing power.

If people can easily opt out of the system, with a few clicks, then digital gold is, de facto, born.

What's the point of storing wealth in an inflationary currency, when there's a hard-money digital asset you can own, just a few clicks away, that will most likely protect your hard-earned money in the long term?

In our humble opinion, there is a chance for Bitcoin to be the spark that lights up the movement against state-controlled currencies. Each and every year that Bitcoin survives against attacks, be it a bug, a malicious actor or even regulatory bodies, the likelihood it will continue to exist increases.

Therefore, Bitcoin could be the main driver for a global hard money economy.

Bitcoin mining has the potential to save distressed heavy industrial businesses

By Michael Nov & Harry Sudock

Posted July 31, 2020

TLDR: When executing a sponsor backed buyout of a distressed Energy Intensive Manufacturing business (heavy manufacturing, mining, etc.), adding a Bitcoin mining layer to the transaction can reduce the fixed costs burdened by the business, improve IRR and reduce risk of the overall transaction.



Introduction

Modern industrial America has been particularly unkind to a subset of the Energy Intensive Manufacturing Sector; a combination of increasing globalization, tightening labor markets, and overall rising COGS created a dynamic where many of these businesses became unprofitable on a marginal basis. COVID-19 combined with all these headwinds became the final nail in the coffin for many.

The system wide demand shock caused by Covid-19 significantly impacted every element of manufacturing businesses, starting from the top line. As most of the US went on lock down, demand vanished. The prevailing strategy was to buy time at all costs. Some businesses were able to temporarily mitigate this financial impact by laying off employees or receiving financial aid in the form of Federal / State programs such as the Payroll Protection Program ("PPP"). The PPP, as well as most other aid programs, were designed to support payroll (PPP requires businesses to allocate at least 60% of the forgivable amount to payroll). **Businesses that have a higher than average utility expenses as % of their cost structure faced a tough decision — to lay off employees or pay the utility bill.**

Over the last decade the Bitcoin mining industry significantly matured and, today, **most North American Bitcoin miners are VC / PE backed and are well regulated**, no more mining in garages or basements. Furthermore, many of the traditional risks that were associated with Bitcoin mining, including the Bitcoin price volatility, can be mitigated through commonly

used hedging tools. **The Bitcoin mining industry evolved into an infrastructure business that is designed to directly monetize electricity.**

As many manufacturing businesses find themselves in financial distress, **integrating a Bitcoin Mining facility into an existing factory creates a unique opportunity to mitigate a short-term financial shock** and provide skilled operators with a one-to-two year window for a comprehensive restructuring.

Bitcoin Mining Ecosystem



Bitcoin mining has significantly matured over the last decade from a fringe hobby to a multi-billion dollar industry that consumes more electricity than a mid-size country such as Switzerland. The role of Bitcoin miners within the ecosystem is simple — to secure the network. Bitcoin miners run a small computer (Application Specific Integrated Circuit, “ASIC”) that solves a difficult mathematical equation. If the miner solved the equation correctly, s/he is compensated in the form of Bitcoin.

The Bitcoin mining operational model is relatively simple; continuously optimize for electricity as it represents between 60% — 70% of Opex.

While the model itself might be simple, reality is far from it. Effectively mining Bitcoin over multiple years requires the operating team to be very diverse and proficient in many fields including network security, electrical engineering, hardware performance and maintenance, financial engineering

and, of course, regulatory maneuvering. **Bitcoin mining could be viewed as the child of Gold Mining and Data Center Management.**

Today, the Bitcoin mining ecosystem includes established and well-funded players such as:

- **Miners:** Layer1 (raised \$50M from Shasta Ventures and Peter Thiel), Crusoe Energy (Bain Capital Ventures, Upper90, Founders Fund), GRIID Infrastructure, and others
- **Equipment Providers:** BitMain Technologies (Sequoia backed Deca-corn), MicroBT (>\$1Bn in 2020 already), Canaan Creative (Successful NASDAQ IPO)
- **Mining Pools:** F2Pool, Poolin, BTC.com

Additionally, traditional “players” such as exchanges, derivative providers, and underwriters also play a significant role in the industry.

10 years after the first Bitcoin was mined, the industry has finally matured to one that can be legally operated and reported in the US, without (significant) regulatory scrutiny. **Bitcoin mining is just another business that uses technology to earn the good old USD.**

Energy Intensive Manufacturing Sector

To mine Bitcoin one needs very little — cheap power, some electrical infrastructure, dedicated ASIC equipment, and space. Many industries can satisfy these criteria; however, energy intensive manufacturing stands out due to the cost structure of most companies and their unique relationships with utility providers.

Industry participants across all sub-sectors including heavy industrials, pulp and paper manufacturing, and refining have high Capex and a significant part of their expenses is dedicated towards paying the utility bill, and specifically paying for electricity. **To optimize this cost, businesses build contracts with local utilities giving the business a lower KWh cost, and in some cases electrical infrastructure support.** To justify these lower rates, the utility requires the EIM business to guarantee a monthly minimal electricity consumption — a win-win.

EIM is a low margin business with very high COGS (up to 70% in some cases) which could be further decomposed into a few key elements — payroll, raw materials, and utility bills (mainly electricity). While payroll and raw materials expense are variable, a portion of the utility bill is fixed; the payment for electricity does not stop when production stops.

In early March of 2020, as Covid-19 was making its way through the rustbelt, many businesses stopped production and furloughed their employees, however they had to continue paying for electricity increasing their financial distress.

Transaction Stakeholders, Structure, and Opportunity

Multiple structures can be created to combine Bitcoin mining with a “traditional” middle market EIM business. However, all structure will include the same set of roles (in some cases a stakeholder could fill multiple roles). The following stakeholder roles will exist:



- **Target EIM** — distressed Energy Intensive Manufacturing business with TTM EBITDA of \$3M — \$5M which was significantly impacted by Covid-19
- **Mining Operator** — existing Bitcoin miner with experience operating multiple facilities and established relationships in the crypto space (e.g., equipment sourcing, security, liquidation)
- **Financial Sponsor** — Middle market focused Private Equity / Family Office with interest and mandate to acquire energy intensive manufacturing businesses
- **Credit Facility Provider** — financial institution (Crypto / traditional) with experience / desire to provide \$10M — \$20M in debt for crypto mining (collateralized by mining equipment)

The **transaction itself should be led by the Financial Sponsor** who has an existing investment thesis around Energy Intensive Manufacturing businesses (across all sub-sectors) and a target acquisition price of \$10M — \$15M. Post-acquisition, to mitigate the temporary decline in profitability, Financial **Sponsor will create and lease part of the facility to the Bitcoin mine operator, who in return will guarantee the consumption of the minimal electricity contract.**

Additionally, to align interests on both sides, the following areas should be considered:

- Electrical build out for the mining operation will be paid by the Bitcoin miner, however the existing EIM facility will be leveraged to decrease the costs to under \$100k/Mw

- Financing for the Bitcoin mining operations will be provided through a dedicated credit facility collateralized by only the mining equipment (Credit Facility Provider) i.e., fully separated from the EIM
- To reduce transaction risk, Bitcoin miner will provide Financial Sponsor with a 12 months Opex guarantee (electricity costs) for the first 2 years through hash / BTC futures

Due to the nature of EIM businesses a 30% — 50% decline in revenue can create >50% decline in EBITDA. Knowing that electricity representing 20% — 40% of COGS, in the above scenario an EIM will pay between \$2M — \$3.5M annually for electricity implying a monthly capacity of 15–20 Mw. Assuming the Financial Sponsor has a standard 5–7 years hold period, an annual decrease of ~\$1M in Opex for the first 2 years will significantly improve the leverage ratio of the transaction, grow IRR, and give the Financial Sponsor a expense “safety net” to restructure the business.

Target Selection Criteria

Multiple targets can fit the criteria of distress middle market EIM businesses; however, a specific set of criteria should be evaluated to ensure the fit:

Electricity Contract:

- Signed contract with local/regional Utility for electricity consumption
- Under \$0.03c KWh cost
- Power costs guaranteed up to at least the EIM minimum capacity and overall power cost is reflected by both Miner and EIM
- Guaranteed monthly minimal consumption of 20% of capacity

Business:

- TTM Target Revenue: \$10M — \$15M (assuming 33% gross margin)
- Profitable on unit basis but not profitable overall
- YoY decline in revenue of 5% — 20%
- Electricity consumption of TTM prior to Covid-19 was 10% — 30% below minimal guaranteed consumption
- Negatively impacted by Covid-19 and is in a cash crunch

Note: while this thesis was focused on EIM businesses, it can be adjusted to serve mature renewable energy producers with over capacity

Disclaimer:

WORDS

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

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

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

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

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

DYOR | BTFD | HODL



I hope you enjoy this project. I'm on a mission to archive the great works of Bitcoin thinkers. Onward!

Read **WORDS**

- [@_joerodgers](#)