



WORDS

January 2018

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

Contents

Contents.....	2
Goals and Scope	4
Support WORDS.....	5
Bitcoin Mayer Multiple	6
How a Bitcoin System is Like and Unlike a Gold Standard.....	12
My Plan for Hyperbitcoinization.....	16
Stop Comparing Bitcoin to the Internet.....	20
Bitcoin - It may fail but we now know how to do it.....	32
Blockchain Proof-of-Work Is a Decentralized Clock.....	34
Bitcoin Surveillance: an Ahistoric Market Error	40
Disclaimer:.....	46

Goals and Scope

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

History

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

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

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

Support WORDS

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

 Support WORDS

Spread the word

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

Follow us on social media

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

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

 Twitter

Subscribe to our newsletter

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

Subscribe

Our pledge

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

Bitcoin Mayer Multiple

By Trace Mayer

Unsure on original post date

Below is a distribution chart of the multiple of the bitcoin price over the 200-day moving average. If a person decides to allocate a small portion of their portfolio to Bitcoin, this tool is intended to help people understand their emotions and corresponding probabilities of various price multiples (from a historical context). **The charts and following information is not telling you to buy or sell Bitcoin.** Bitcoin is insanely volatile. The charts do not suggest future results will be the same as the past. Please note, some suggest the long-term value of Bitcoin is high (in excess of \$100,000 per Bitcoin), but there are also others that say Bitcoin is a mania and will be deeply regulated by the government if it is allowed to get too large. Either way, this page is simply a study to understand the probabilities of price multiples and what is normal and abnormal levels (from a historical context).

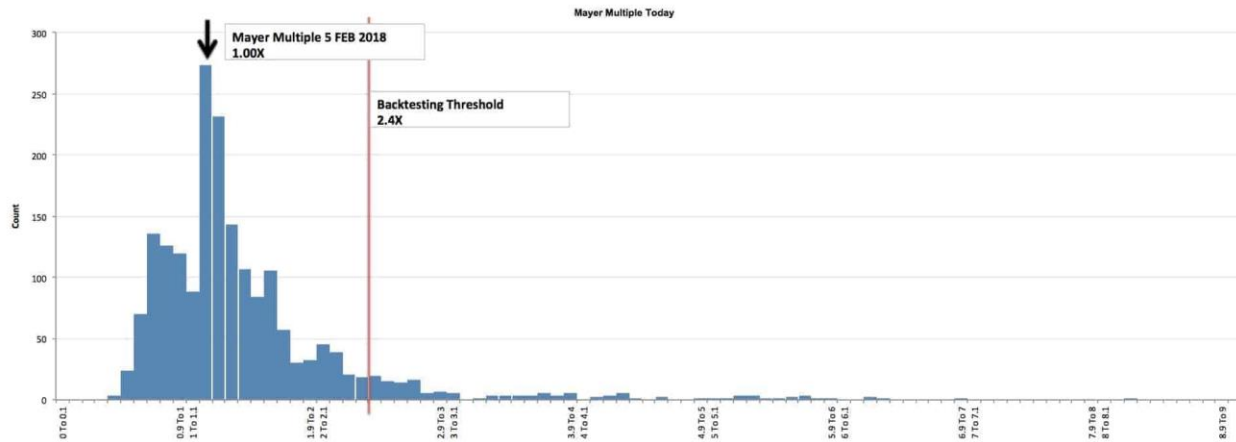
HOW THE MAYER MULTIPLE WORKS

The following explanation is how to interpret the Mayer Multiple using 5 February 2018 at 4.00 PM EST as an example. Remember to check this page or follow us on Twitter, to get updates daily.

The 200 Day Moving Average is: **\$6858**

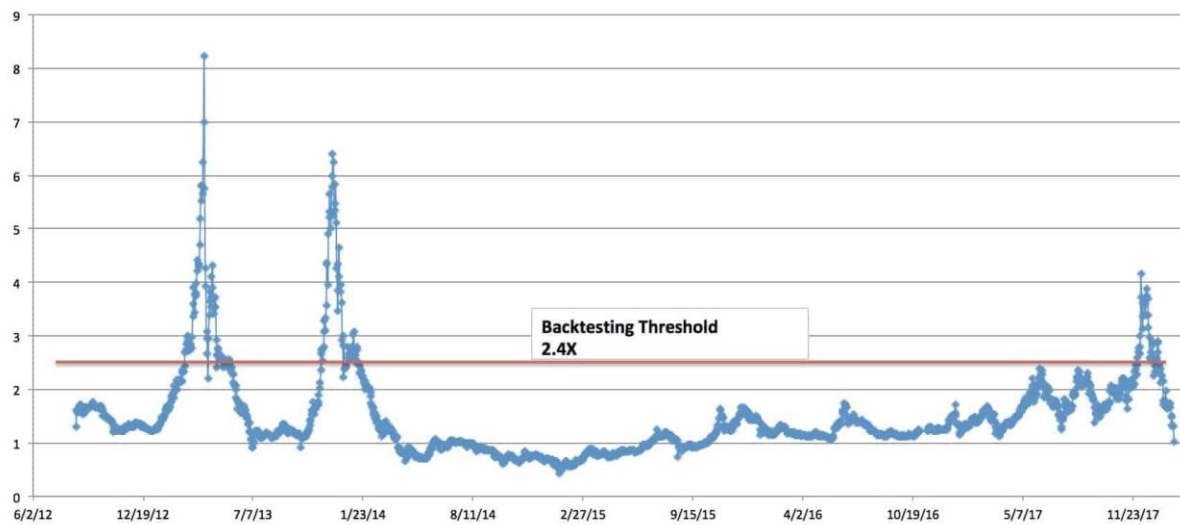
The average Mayer Multiple is **1.47** for the history of Bitcoin.

The multiple on 5 February 2018 is **1.00X**. A higher multiple has historically happened 75% of the time. A price less than \$16461 would put the Mayer Multiple below 2.4X on 5 February 2018. A price of \$10145 would put the price on the average multiple of 1.47X. The BTC price when this calculation was last conducted was \$7000 USD.

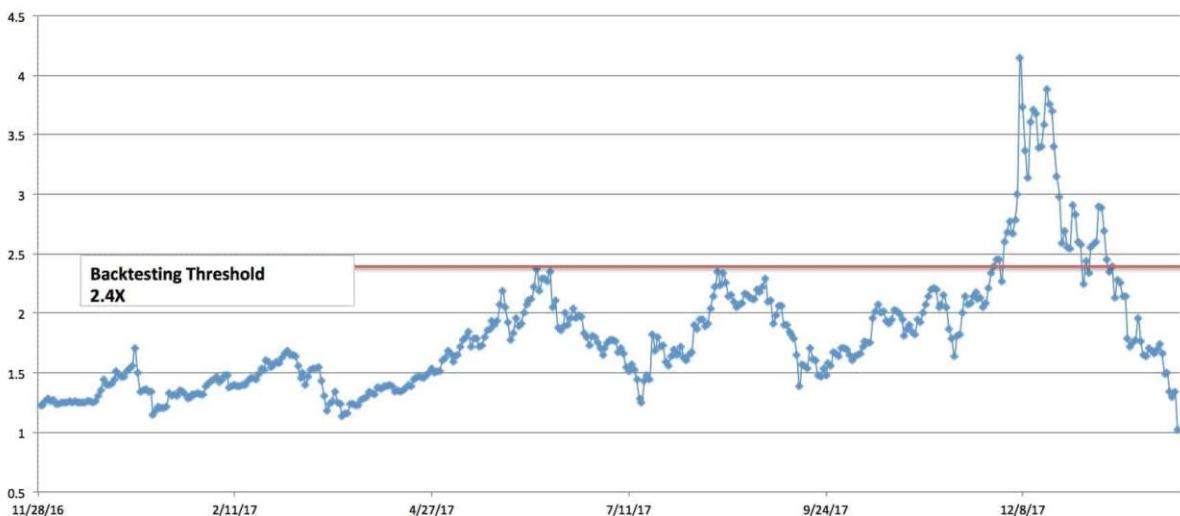


THE MAYER MULTIPLE SINCE THE INCEPTION OF BITCOIN

Bitcoin Price / 200 day Move Average (The Mayer Ratio)



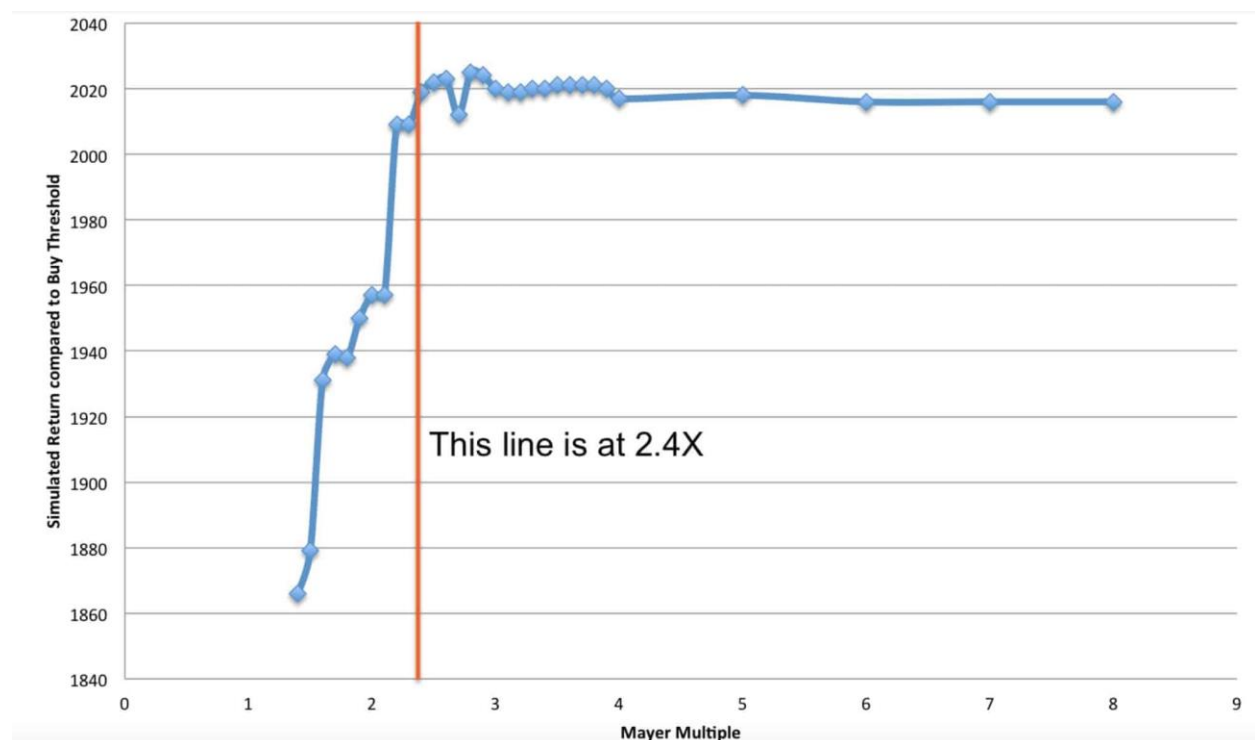
Bitcoin Price / 200 day Move Average (The Mayer Ratio) 1 Year of Data



Please note: Bitcoin is not normally distributed. As a result, a typical Standard Deviation model is not accurate when talking about probabilities. With that said, this is the only model we can use to try and characterize normal and abnormal behavior. If you don't like the use of this model, contact your college statistics teacher and he can help you invest in only absolute scenarios. Regardless of our distaste for academia, this model does have limitations and might not be the best way to represent the bitcoin price!

Frequency distribution of Multiple					
Multiple	Count	Cumulative Count	Percent	Cumulative Percent	
0.4 To 0.5	4.	4.	0.21%	0.21%	3SD 2SD ish
0.5 To 0.6	24.	28.	1.26%	1.47%	
0.6 To 0.7	70.	98.	3.66%	5.13%	
0.7 To 0.8	136.	234.	7.12%	12.25%	
0.8 To 0.9	126.	360.	6.60%	18.85%	
0.9 To 1	120.	480.	6.28%	25.13%	1 SD
1 To 1.1	88.	568.	4.61%	29.74%	
1.1 To 1.2	273.	841.	14.29%	44.03%	
1.2 To 1.3	232.	1,073.	12.15%	56.18%	
1.3 To 1.4	143.	1,216.	7.49%	63.66%	
1.4 To 1.5	107.	1,323.	5.60%	69.27%	Mean
1.5 To 1.6	84.	1,407.	4.40%	73.66%	
1.6 To 1.7	106.	1,513.	5.55%	79.21%	
1.7 To 1.8	57.	1,570.	2.98%	82.20%	
1.8 To 1.9	30.	1,600.	1.57%	83.77%	
1.9 To 2	33.	1,633.	1.73%	85.50%	1SD
2 To 2.1	45.	1,678.	2.36%	87.85%	
2.1 To 2.2	39.	1,717.	2.04%	89.90%	
2.2 To 2.3	21.	1,738.	1.10%	90.99%	
2.3 To 2.4	19.	1,757.	0.99%	91.99%	
2.4 To 2.5	20.	1,777.	1.05%	93.04%	
2.5 To 2.6	15.	1,792.	0.79%	93.82%	
2.6 To 2.7	14.	1,806.	0.73%	94.55%	
2.7 To 2.8	16.	1,822.	0.84%	95.39%	
2.8 To 2.9	6.	1,828.	0.31%	95.71%	
2.9 To 3	7.	1,835.	0.37%	96.07%	
3 To 3.1	6.	1,841.	0.31%	96.39%	
3.2 To 3.3	1.	1,842.	0.05%	96.44%	
3.3 To 3.4	3.	1,845.	0.16%	96.60%	
3.4 To 3.5	3.	1,848.	0.16%	96.75%	
3.5 To 3.6	4.	1,852.	0.21%	96.96%	
3.6 To 3.7	3.	1,855.	0.16%	97.12%	
3.7 To 3.8	6.	1,861.	0.31%	97.43%	
3.8 To 3.9	4.	1,865.	0.21%	97.64%	
3.9 To 4	6.	1,871.	0.31%	97.96%	
4.1 To 4.2	2.	1,873.	0.10%	98.06%	
4.2 To 4.3	4.	1,877.	0.21%	98.27%	
4.3 To 4.4	6.	1,883.	0.31%	98.59%	
4.4 To 4.5	1.	1,884.	0.05%	98.64%	
4.6 To 4.7	2.	1,886.	0.10%	98.74%	
4.9 To 5	1.	1,887.	0.05%	98.80%	
5 To 5.1	1.	1,888.	0.05%	98.85%	
5.1 To 5.2	1.	1,889.	0.05%	98.90%	
5.2 To 5.3	3.	1,892.	0.16%	99.06%	
5.3 To 5.4	3.	1,895.	0.16%	99.21%	
5.4 To 5.5	1.	1,896.	0.05%	99.27%	
5.5 To 5.6	1.	1,897.	0.05%	99.32%	
5.6 To 5.7	2.	1,899.	0.10%	99.42%	
5.7 To 5.8	4.	1,903.	0.21%	99.63%	
5.8 To 5.9	1.	1,904.	0.05%	99.69%	
5.9 To 6	1.	1,905.	0.05%	99.74%	3SD
6.2 To 6.3	2.	1,907.	0.10%	99.84%	
6.3 To 6.4	1.	1,908.	0.05%	99.90%	
6.9 To 7	1.	1,909.	0.05%	99.95%	
8.2 To 8.3	1.	1,910.	0.05%	100.00%	

The chart below was determined by a simulation. The simulation assumed a person had \$100 to invest in Bitcoin everyday since inception. There was only 1 control variable – the Mayer Multiple. If the price was $< x$ Mayer Multiple, then the individual would buy \$100 worth of BTC. If the price was $\geq x$ Mayer Multiple, the person would accumulate fiat until the price dropped back below x . The various x multiples that were tested are listed on the x axis below. When the simulation was run for various Mayer Multiples, it produced various returns (displayed in BTC on the y axis of the chart below). The chart demonstrates that anything over a Mayer Multiple of 2.4X failed to produce better results. When a multiple was selected below 2.4X, the BTC buyer got dramatically worse results. But, it's very important to note that a new entrant buying below a 2.4X threshold would have an easier time emotionally during the first few quarters of ownership. **Please note, every time the Mayer Multiple has gone above the 2.4X line, it has returned below 1.5X.** In our simulation, we did not hold cash until reaching 1.5X (instead, the model simply purchased more BTC once below the 2.4X threshold). If the simulation would have waited for repurchase below 1.5X (after movement above 2.4X was achieved), the results would have likely been better than depicted below. This, however, may or many not be indicative of how the market might perform in the future, so those enhanced results were not displayed.

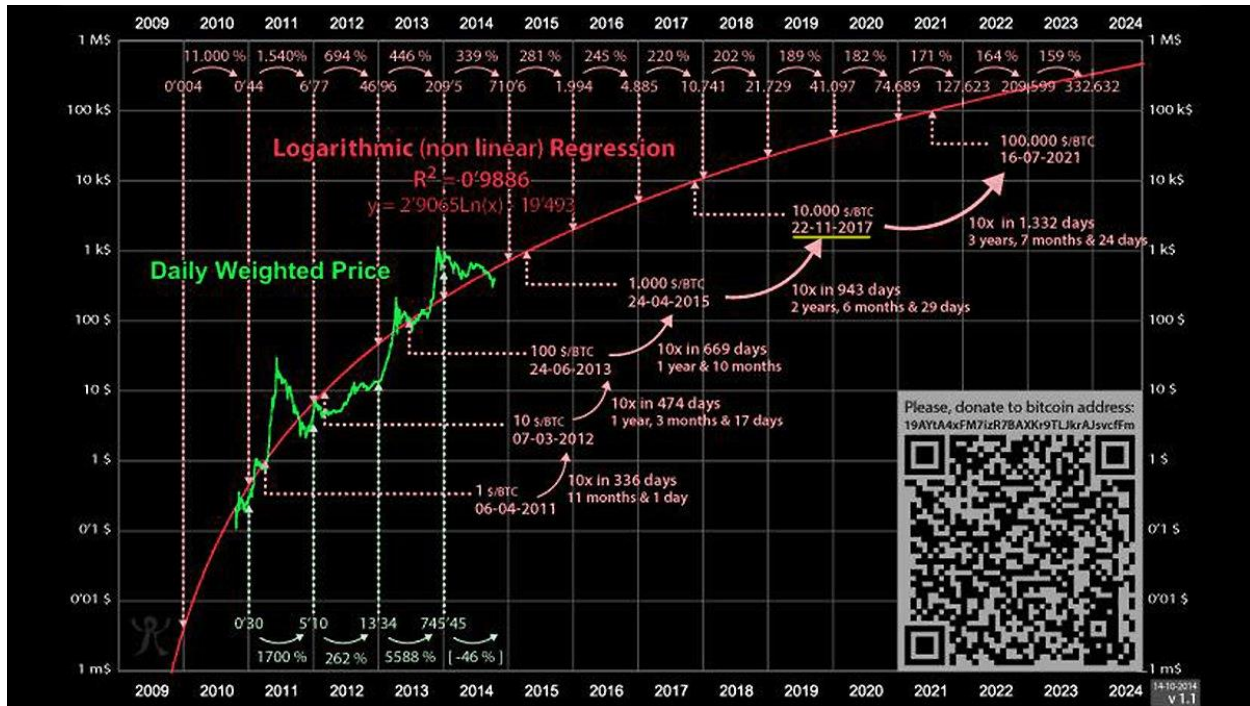


THE INTRINSIC VALUE AND NETWORKING EFFECT

The graph below shows how the value of Bitcoin might increase exponentially. The graph is derived from Metcalfe's law that states that the

value of a telecommunications network (fax machines, telephones, etc.) is proportional to the square of the number of connected users of the system. Companies like Facebook and Tencent showed that Metcalfe's law, originally presented in 1980, held for both.

94% of the price movements from 2013-2017 has been explained by this law.



Questions? Please contact [Preston Pysh](#) or [Trace Mayer](#).

How a Bitcoin System is Like and Unlike a Gold Standard

By Larry White

Posted January 11, 2018

Many commentators have compared Bitcoin to gold as an investment asset. “Can Bitcoin Be Gold 2.0?,” asks a portfolio analyst. “Bitcoin is increasingly set to replace gold as a hedge against uncertainty,” suggests a Cointelegraph reporter.

Economists, by contrast, are more interested in considering how a monetary system based on Bitcoin compares to a gold-standard monetary system. In a noteworthy journal article published in 2015, George Selgin characterized Bitcoin as a “synthetic commodity money.” Monetary historian Warren Weber in 2016 released an interesting Bank of Canada working paper entitled “A Bitcoin Standard: Lessons from the Gold Standard,” which analyzes a hypothetical international Bitcoin-based monetary system on the supposition that “the Bitcoin standard would closely resemble the gold standard” of the pre-WWI era. More recently, University of Chicago economist John Cochrane in a blog post has characterized Bitcoin as “an electronic version of gold.”

In what important respects are the Bitcoin system and a gold standard similar? In what other important respects are they different?

Bitcoin is similar to a gold standard in at least two ways. (1) Both Bitcoin and gold are stateless, so either can provide an international base money that is not the creature of any national central bank or finance ministry. (2) Both provide a base money that is reliably limited in quantity (this is the grounding for Selgin’s characterization), unlike a fiat money that a central bank can create in any quantity it likes, “out of thin air.”

Bitcoin and the gold standard are obviously different in other ways. Gold is a tangible physical commodity; bitcoin is a purely digital asset. This difference is not important for the customer’s experience in paying them out, as ownership of (or a claim to) either asset can be transferred online, or in person by phone app or card. The “front ends” of payments are basically the same nowadays. The “back ends” can be different. Gold payments can go peer to peer without third-party involvement only when a physical coin or bar is handed over. Electronic gold payments require a trusted vault-keeping intermediary. Bitcoin payments operate on a distributed ledger and can go peer-to-peer electronically without the help of a financial institution. In

practice, however, many Bitcoin transactions use the services of commercial storage and exchange providers like Coinbase.

The most important difference between Bitcoin and gold lies in their contrasting supply and demand mechanisms, which give them very different degrees of purchasing power stability. The stock of gold above ground is slowly augmented each year by gold mines around the world, at a rate that responds to, and stabilizes, the purchasing power of gold. Commodity (non-monetary) demands also respond to the price of gold and dampen movements in its value. The rate of Bitcoin creation, by contrast, is entirely programmed. It does not respond to its purchasing power, and there are no commodity demands.

Let's consider supply in more detail. Secularly, annual production of gold has been a small percentage (typically 1% to 4%) of the existing stock but not zero. Because the absorption of gold by non-monetary uses from which it is not recoverable (like tooth fillings that will go into graves and stay there, but unlike jewelry) is small, the total stock of gold grows over time. Historically this has produced a near-zero secular rate of inflation in gold standard countries. The number of BTC in circulation was programmed to expand at 4.0 percent in 2017, but the expansion rate is programmed to fall progressively in the future and to reach zero in 2140. At that point, assuming that real demand to hold BTC grows merely at the same rate as real GDP, Bitcoin would exhibit mild secular growth in its purchasing power, or equivalently we would see mild deflation in BTC-denominated prices of goods and services. (Warren Weber's paper similarly derives this result.) This kind of growth-driven deflation is benign, but the difference is small in real economic welfare consequences between a money stock that steadily grows 3% per year and one that grows 0%.

The key difference in the supply mechanisms is in the *induced variation* in the rate of production of monetary gold in response to its purchasing power, by contrast to the non-variation in BTC. A rise in the purchasing power of BTC does not provoke any change in the quantity of BTC in the short run or in the long run. In Econ 101 language, the supply curve for BTC is always vertical. (The supply curve is, however, programmed to shift to the right over time, ever more slowly, until it stops at 21 million units). By contrast, a non-transitory rise in the purchasing power of gold brings about some small increase in the quantity of monetary gold in the short run by incentivizing owners of non-monetary gold items (jewelry and candlesticks) to melt some of them down and monetize them (assuming open mints) in response to the rising opportunity cost of holding them and to the owners' increased wealth. The short-run supply curve is not vertical. Still more importantly, the rise will bring about a much larger increase in the longer run by incentivizing owners

of gold mines to increase their output. The “long-run stock supply curve” for monetary gold is fairly flat. (I walk through the stock-flow supply dynamics in greater detail in chapter 2 of [my monetary theory text](#).) The purchasing power of gold is mean-reverting over the long run, a pattern seen clearly in the historical record.

Because its quantity is pre-programmed, the stock of BTC is free from supply shocks, unlike that of monetary gold. Supply shocks from gold discoveries under the gold standard were historically small, however. The largest on record was the joint impact of the California and Australian gold rushes, which (according to [Hugh Rockoff](#)) together created only 6.39 percent annual growth in the world stock of gold during the decade 1849-59, resulting in less than 1.5 percent annual inflation in gold-standard countries over that decade. For reference, the average of decade-averaged annual growth rates over 1839-1919 was about 2.9 percent.

As a result of the long-run price-elasticity of gold supply combined with the smallness and infrequency of supply shocks, the purchasing power of gold under the classical gold standard was [more predictable](#), especially over 10+ year horizons, than the purchasing power of the post-WWII fiat dollar has been under the Federal Reserve. As I have [written previously](#): “Under a gold standard, the price level can be trusted not to wander far over the next 30 years because it is constrained by impersonal market forces. Any sizable price level increase (fall in the purchasing power of gold) caused by a reduced demand to hold gold would reduce the quantity of gold mined, thereby reversing the price level movement. Conversely, any sizable price level decrease (rise in the purchasing power of gold) caused by an increased demand to hold gold would increase the quantity mined, thereby reversing that price level movement.” Bitcoin lacks any such supply response. There is no mean-reversion to be expected in the purchasing power of BTC, and thus its purchasing power is much harder to predict at any horizon.

Describing gold supply, Warren Weber writes: “Changes in the world stock of gold were determined by gold discoveries and the invention of new techniques for extracting gold from gold-bearing ores.” This is not well put. Changes in the world stock of monetary gold come about every year from normal mining. Gold strikes and technical improvements in extraction brought about changes in the **growth rate** (not the level) of the stock. Historically, the changes in the growth rate were not dramatic by comparison to changes in the postwar growth rates of fiat monies. As often as not, the changes in gold stock growth rates were equilibrating, speeding the return of the purchasing power of gold to trend from above trend. As Rockoff [noted](#), some important gold strikes (like the [Klondike](#) in the 1890s) and some important technical breakthroughs (like the [cyanide process](#) of 1887) were

induced by the high purchasing power of gold at the time, which gave added incentive for prospecting and research.

The phrase from John Cochrane quoted above is part of a sentence that reads in its entirety: "It's an electronic version of gold, and the price variation should be a warning to economists who long for a return to gold." From the consideration of the mean reverting character of the purchasing power of gold, by contrast to Bitcoin's lack of such a character, we can see that the second half of Cochrane's statement is incorrect. The inelastic supply mechanism that produces price variation in Bitcoin should give pause to those who predict that Bitcoin will become a commonly accepted medium of exchange. It says nothing about the purchasing power of gold under a gold standard.

My Plan for Hyperbitcoinization

By Elaine Ou

Posted January 13, 2018

If familial history is any indication, I've got about thirty years left on this planet. Forty if I play my cards right. That's not a lot of time, and I'm worried that I'll miss out on the era of hyperbitcoinization.

See, as Bitcoin establishes itself as a supreme store of value, people will continually abandon their local currencies until central banks capitulate. In time, fiat money will die, all the worlds' wealth will be denominated in bitcoin, and anyone who had the foresight to accumulate even a few satoshis will find themselves tremendously rich.

I've decided that the most extropian thing I can do is have myself cryogenically frozen with my private keys. In a few thousand years, when hyperbitcoinization puts me squarely in the 1%, they'll thaw me out and I'll live like a king. Yessssssss.



For inspiration, I look to King Tutankhamun, Egyptian pharaoh of the 18th dynasty. King Tut was entombed at Luxor in 1323 BC with all manner of gold jewelry and artifacts. With sufficiently advanced medical technology, we could, in theory, rehydrate his mummified body and bring him back to life. Presumably he would demand the return of his buried wealth, which insurers have appraised at \$680 million.

\$680 million is a lot of money! Still, King Tut might be disappointed. The last president of Egypt had a net worth of \$70 billion. The reanimated corpse of Tutankhamun is unlikely to restore his pharaonic privilege with such a relatively meager hoard. Turns out military contracts and foreign property would have made for a better investment.



This high-status dude was buried at the Varna Necropolis. After HODLing for 6600 years, today his gold is worth about \$181,000 by weight.

Perhaps Tutankhamun's mistake was choosing gold to escort his wealth into the afterlife. The purchasing power of gold is mean-reverting over the long run, because mining operations can scale according to the price level. In other words, gold doesn't meet the criteria for a securely constrained supply.



This guy in Sungir, Russia – now he had the right idea. In 32,000 BC, this Paleolithic man was buried with 13,000 mammoth ivory beads. Mammoths have been extinct for four thousand years, so the supply doesn't get any scarcer than this! It might take some time for doctors to figure out how to

revive Sungir Man from his temporarily dead condition, but once they do, boy will he be excited about hypermammothization.

Bad news. Despite embodying all the attributes of trust-minimized money, mammoth ivory has not been embraced as a global store of value. A few weeks ago, an entire mammoth skeleton was auctioned off for just \$645k. The CEO of a roofing company bought it to display at his office.



This family of four sold for \$550k last year.

Things don't look so promising here. It seems that no matter how reliable my store of value, the world will keep producing more wealth. As we all know, you're not truly wealthy unless you have something that no one else can afford.

Let's do one more.



Qin Shi Huang, the first emperor of China, is resting in the largest underground mausoleum in the world. According to historical records, 48 concubines were buried alive to service the emperor in the afterlife. We're really pushing the bounds of medical imagination here, but suppose we brought the harem back to life. The four-dozen ladies would be just as valuable today as they were in 208 BC!

What is the purpose of money if not to increase reproductive success? The Qin emperor cuts right to the chase by stockpiling concubines in his tomb.

There is one catch: Modern-day China does not abide women as chattel the way they did during the Qin dynasty. Wouldn't it suck if the emperor HODLed for 2200 years only to have his wealth emancipated?

Circumstances change. Bitcoin can't be seized or censored, but what if we enter some post-scarcity future with replicators and transporters, where money itself is irrelevant? You know, like Star Trek.



Star Trek's communist utopia transcends money because energy is free and objects can be replicated in abundance. Even then, the Federation recognizes the need for a pecking order. Captain Kirk gets all the ladies while the Redshirts get vaporized. In a world without wealth, social status is denominated by shirt color. Attain it by ingratiating yourself with Hollywood scriptwriters.

So if we're trying to preserve status rather than wealth, that leaves a limited window for hyperbitcoinization. It has to be far enough in the future that society recognizes Bitcoin as a status symbol, but not so distant that it becomes completely irrelevant. I think we're almost there. Live long and HODL. 🙌

Stop Comparing Bitcoin to the Internet

By Dhruv Bansal

Posted January 19, 2018

The market cap of cryptocurrencies dropped almost 50% from ~\$820B to ~\$420B in the last month. This is not the first time cryptocurrencies have experienced such significant losses (though it's one of the fastest) and it certainly won't be the last. Crypto-cynics and unfriendly media were jubilant in their choruses of "I told ya so". There was much hand-wringing and regret expressed by some investors, especially those who only recently acquired their positions, who doubtless sold during the plunge.

Yet, throughout, there remained a population of crypto holders curiously unfazed by the debacle and the clamoring. These investors call themselves "hodlers". They have held cryptocurrencies such as Bitcoin for extended periods, some for many years, and they have weathered downturns like this before. Why did they buy crypto so early? How have they remained so serene when so many others in the market are panicking? Are they crazy? Or is blockchain a religion for them?

The answer is simple: hodlers recognize the true potential of blockchains and this allows them to adopt the long-view on their cryptocurrency holdings. Like value investors, short-term pullbacks in price mean little to them. Rather they relish when prices collapse because it lets them acquire more coins, cheaply.

In this article, I will provide a historical analogy for blockchains which will help you adopt the long-view on cryptocurrencies.

But first, we must dispense with an analogy you might already be familiar with: *blockchains are like the Internet in the 1990s*.

It's not an uncommmon insight:



Chris Burniske ✓
@cburniske



Packet switching: 1960
ARPANET: 1969
Internet: 1973
Mosaic browser: 1993 [#Bitcoin](#) & [#blockchain](#): 2009
WE'VE GOT TIME

♡ 44 2:29 PM - Oct 22, 2016 · Manhattan, NY



💬 37 people are talking about this



Tuur Demeester
@TuurDemeester



Blythe Masters on Blockchain tech: "I would take it, as seriously, as you should have taken the concept of the internet, in the early 1990s"

♡ 17 11:46 PM - Jun 4, 2015



💬 22 people are talking about this



notsofast
@notsofast






It's so obvious to me now that [#cryptocurrency](#), [#bitcoin](#) and [#blockchain](#) in 2015 is exactly like the internet in 1994. [#disruption](#) incoming.





♡ 15 12:22 PM - Nov 8, 2015



💬 17 people are talking about this



**Taylor Pearson**  @TaylorPearsonMe · Oct 27, 2017 
Replying to @TaylorPearsonMe
28/ To date, Churchill's comment has stood true: 'Democracy is the worst form of government, except for all the others.'

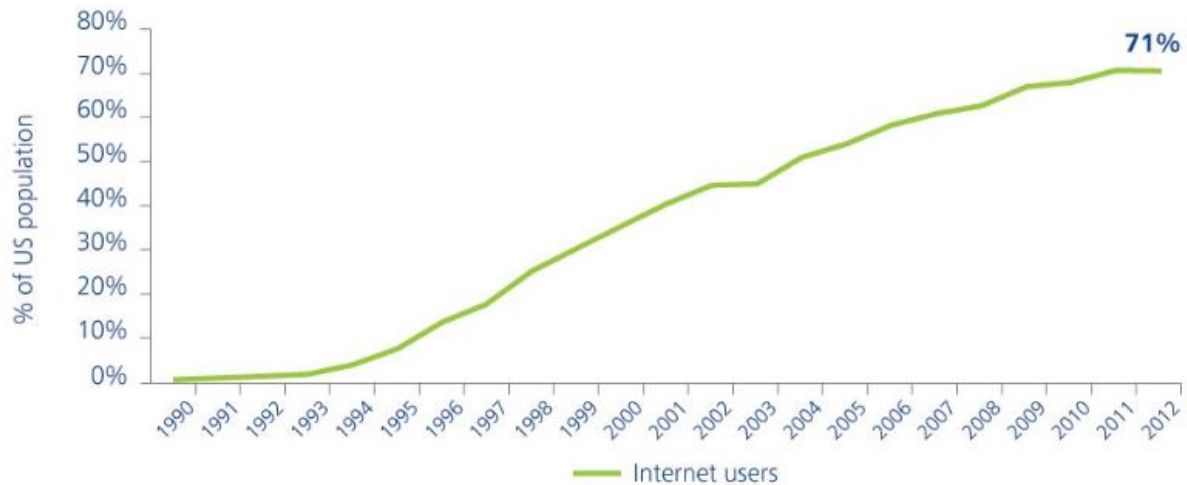
**Taylor Pearson**  @TaylorPearsonMe
29/ The question to me is not "Is blockchain the next internet?" I think it's clear that's the case.
♡ 59 1:49 PM - Oct 27, 2017 
[See Taylor Pearson's other Tweets](#) 

**Venkatesh Rao** @vgr 
Is it just me? I haven't felt this much excitement in tech scene since '97. Between blockchain & machine learning, it's like New Internet 🤔
♡ 127 9:09 AM - May 20, 2017 
[54 people are talking about this](#) **Roger Ver**  @rogerkver 
"Blockchain (Bitcoin) has the potential to be as significant as the internet" - Direct quote from Microsoft
♡ 108 10:37 AM - Jul 19, 2016 · Japan 
[81 people are talking about this](#) 

And it's true: the "Internet in the 1990s" *really is* a good historical analogue for the blockchain in many ways. Blockchains are digital, networked, and will change society, just like the Internet did, so the analogy is sticky. And who didn't love the 1990s, amirite? A 32-bit era of wunderkind programmers

evolving crazy, ambitious startups to speciate a new niche. Crypto-pimps and cheerleaders love using the Blockchain::Internet analogy, because it suggests fantastic, abundant, **imminent** growth. *Invest!*

Figure 4. Internet users (1990–2012)



Source: comScore, Deloitte analysis

Graphic: Deloitte University Press | DUPress.com

If blockchains are where the Internet was in the 1990s, then that means the prices are gonna get even higher. Right guys? Right? [\[Source\]](#)

If blockchains are where the Internet was in the 1990s, then that means the prices are gonna get even higher. Right guys? Right? [\[Source\]](#)

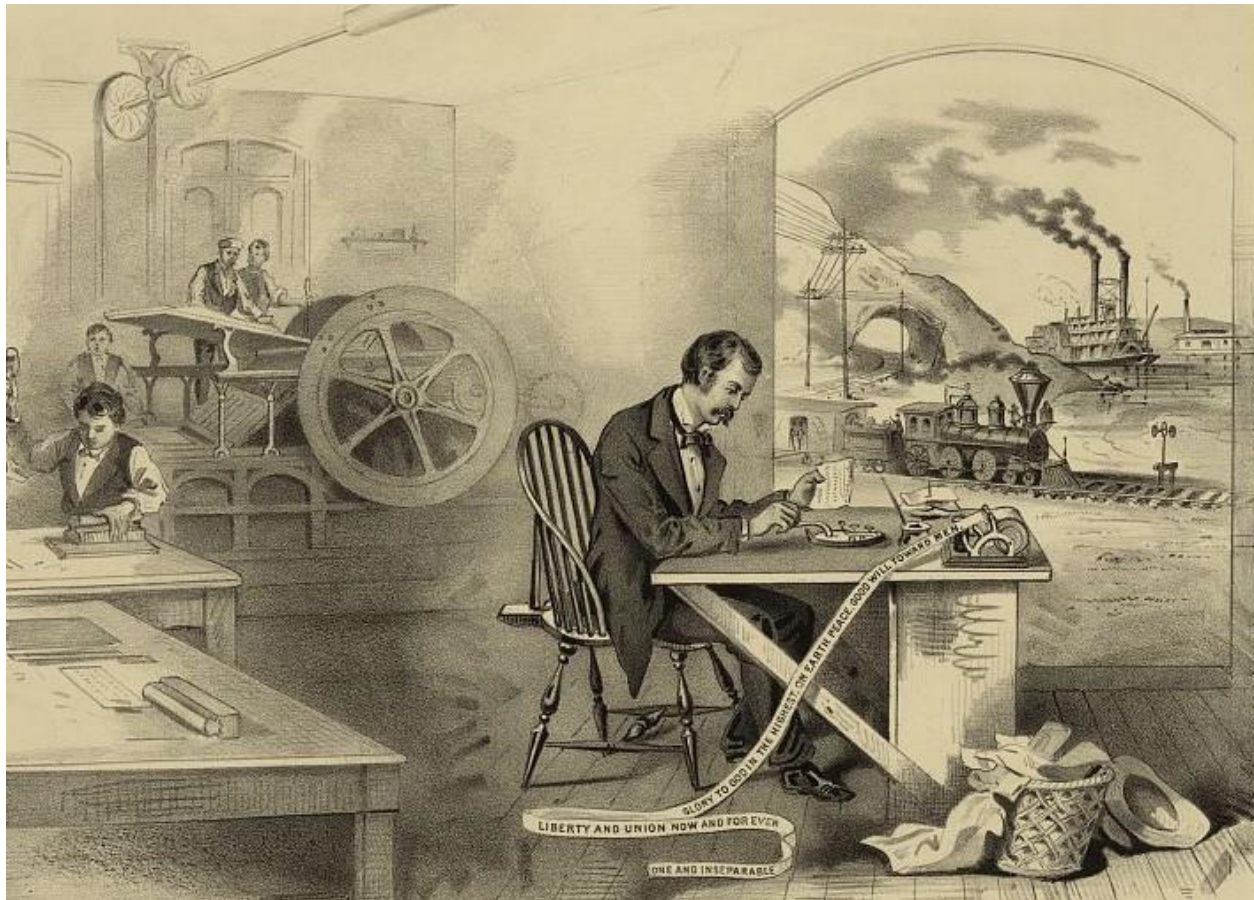
The diligent remember that most tech startups of the 1990s would eventually fail, even some which had tremendous funding. The NASDAQ spike and crash reminds older investors of the “Bitcoin bubble” or mania over ICOs. Crypto-cynics and haters love the Blockchain::Internet analogy as well because it suggests caution and the need for due diligence in the face of irrational exuberance. *Caveat emptor!*

Both of these perspectives on the Blockchain::Internet analogy are correct. Like the Internet in the 1990s, blockchains are poised for tremendous growth, so investing in the right tokens & teams may yield once-in-a-generation returns for investors (the crypto-equivalents of Google, Amazon, Facebook, &c). Yet many (most?) current projects will probably still fail (Pets.com, Webvan, eToys, &c.).

But both these perspectives are also dramatically wrong. Comparing blockchains to the Internet actually **undersells** the eventual value of the industry and the impact it will have on humanity.

No, the *best* analogy for the blockchain is not the Internet, but the lowly **telegraph**. In order to understand why, let's first discuss the telegraph and the technologies that evolved from it.

A modern view of the telegraph



Historical woodcut of a telegraph operator transmitting some dank memes (1839). [Source]

Most people know what a telegraph is (or was): a tappitty-tap electronic gizmo that allowed historical, mustache-oriented peoples to send each other the old-timey equivalent of `LOL ROTFLMAO`.

But allow me to offer a different perspective. The telegraph was the first example of a *new category* of technology:

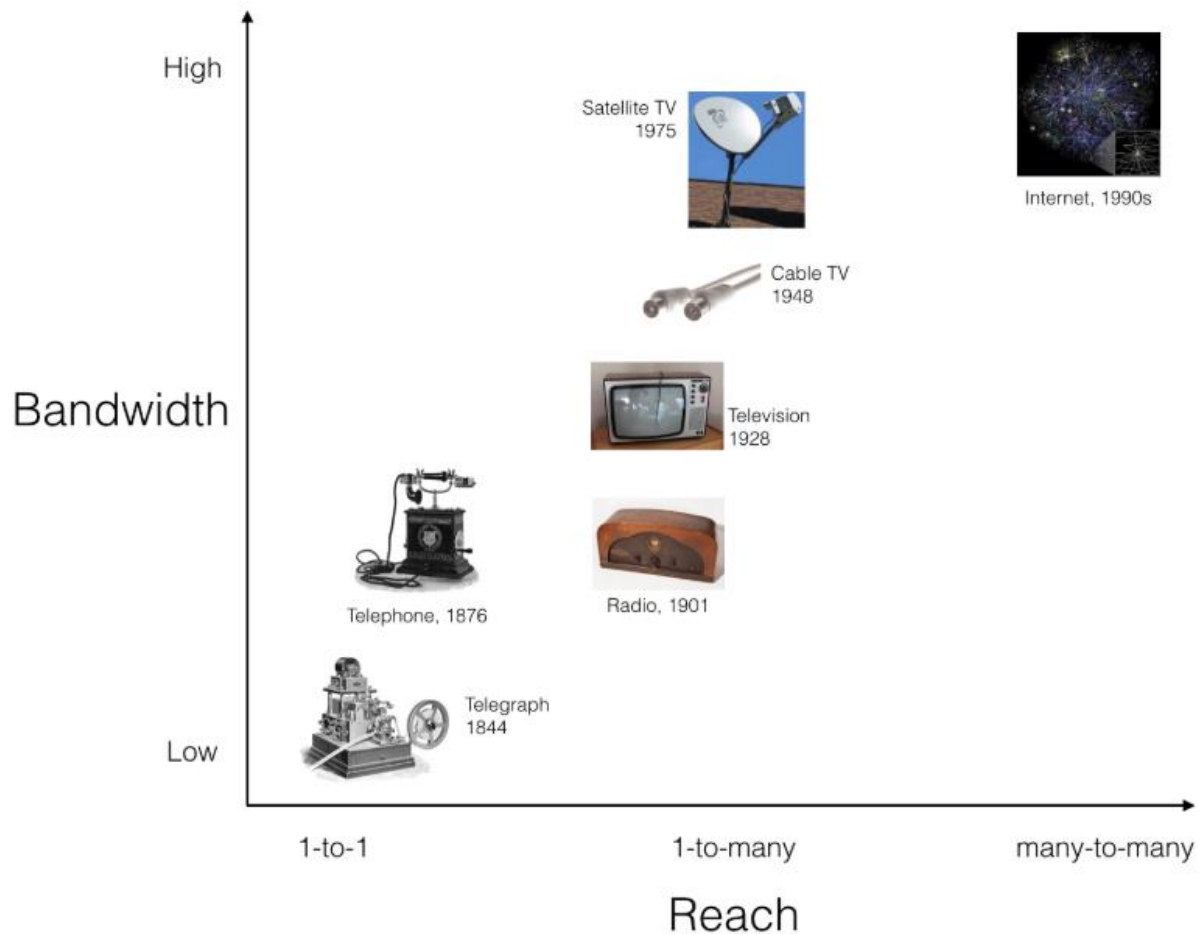
The telegraph was the first *telecommunications* technology: it enabled humanity to transmit digitally encoded information at (near-)instant speeds over long distances using a privately owned network.

Let's unpack that sentence a bit:

- ***telecommunications***: The telegraph was the beginning of the telecommunications industry (ignoring for now earlier, more manual methods such as firing cannons, waving flags, or flashing lights over relay networks of manual operators).
- ***digitally-encoded information***: We are referring to Morse code, of course, the bebop-doo-wop binary line noise of the telegraph's protocol. Telegraph operators transformed users' thoughts and words (themselves already a discrete encoding of sorts) into these data structures before they could flit along the network.
- ***(near-)instant speeds over long distances***: Data transmission through telegraphic wires was (is) so fast that it may as well be called instant (we are neglecting here the practical/engineering issue of needing repeater-stations manned by human operators taking a finite time to repeat each message, but please, forgive us our trespasses into falsehood in pursuit of narrative).
- ***privately owned network***: Telegraph networks were capital-intensive projects with limited throughput, so their private owners charged usage fees.

The Internet is the pinnacle of modern telecommunications, but it also the logical and inevitable outcome of the technological and social change started by the telegraph (1844):

- (1876) The telephone brought telecommunications directly into people's homes and allowed for the direct transmission of audio in addition to just textual characters.
- (1901) The radio introduced the use of the wireless electromagnetic spectrum to transfer data instead of physical telegraph wires. This allowed for one-to-many transmission, enabling content such as entertainment and news beyond just one-to-one, direct communication.
- (1928) Television introduced the digital representation of visual signals in addition to just text and audio.
- (1948) Cable TV and satellite TV (1975), introduced even greater bandwidth and greater speeds and supported more content with greater variety.
- (1990s) The Internet integrated all of these improvements and expanded discourse from one-to-one and one-to-many to many-to-many.



Telecommunications has come a long way in 170 years, increasing reach and bandwidth by orders of magnitude. But it all started with the telegraph. [All images from Wikipedia]

If there were an extremely wise and forward-thinking person alive in 1844 when Samuel Morse sent the first real telegram (WHAT HATH GOD WROUGHT?—totally metal) 44 miles from Washington D.C. to Baltimore, could they have anticipated the Internet? Could they have remarked: *Reginald, darling, what if we use light instead of wires, digitally encode audio and video in addition to just text, increase the bandwidth tremendously, and allow everyone to individually send and receive messages from wherever they are?*

No technology is an island

It would have been extremely difficult for an 1840s telegraph enthusiast to predict the Internet. The evolution of telecommunications did not happen in isolation from all other technological and social change. It was driven by, and drove, the parallel evolution of other industries, most importantly energy, transportation, and computing. Without cheap and ubiquitous energy or

global supply chains, how could we have built communications satellites or iPhones?

But all of these parallel industries already existed, in some rudimentary form or another, by the mid-19th century. The telegraph itself demanded a thorough understanding of electromagnetism, crude oil was being refined from paraffin, combustion engines were in industry, and the Jacquard loom had been long-operating. In each decade following the introduction of the telegraph, these technologies combined to create a more fast-paced, connected, global world with a greater need and desire for instant communications.

The details may have been fuzzy, but to those who saw the telegraph as the first member in a new category of telecommunications technology, the future was clear: a smaller, more connected, but more centralized planet. Some futurists of the time even got pretty close:

A charming Victorian imagining of a Skype video chat in 2012, from 1899. [Source]

So why are blockchains like the telegraph?

Why do we believe the telegraph is the best analogy for blockchains?

It's because blockchains, just like the telegraph, are the first example of a *new category* of technology:

Blockchains are the first *distributed consensus* technology: they use cryptography to enable global coordination through collective self-interest instead of centralization.

Let's unpack this definition, just as we did for the telegraph:

- ***distributed consensus***: This combination of technology and social movement is historically new, and Bitcoin's blockchain is the canonical first example.
- ***cryptography***: Public/private keypairs, hashpower, Merkle trees, &c, are cryptographic tools designed to create or correct imbalances in power between attackers and defenders, spammers and validators, governments and citizens, &c.
- ***global coordination***: Blockchains are distributed systems. They have no inherent saturation size and can (eventually) scale to global demand. Their consensus algorithms (Proof-of-Work and Proof-of-Stake) are completely opt-in and provide coordination without control or coercion.
- ***collective self-interest instead of centralization***: Successful blockchains use valuable tokens to create strong local incentives in delicate balance

from which beneficial collective behavior can emerge. There are no centralized committees or official leadership hierarchies.

If you accept the argument that blockchains are a new category of technology, then the next question to ask is, “Where does it go from here? What will our world look like when Bitcoin is as old as the telegraph?”

The Distributed Future vs. the Centralized Past/Present

This question can't be answered in isolation. The telecommunications industry arose alongside the energy, transportation, and computing industries. These are all democratizing industries, but they are also *centralizing* industries: they each created greater access for the average person but in a way that created ever greater inter-dependency on an ever fewer number of global firms. These industries are all capital-intensive, and cartels and monopolies have risen and been disrupted again and again as market share vacillates during and consolidates between cycles of innovation.

This family tree stops somewhere around 2005 but it shows the forces of centralization at work. So, yeah, AT&T really needs to buy T-Mobile, right?[Source]

Blockchains weren't developed in a vacuum. The principles of robustness, trustworthiness, anti-fragility, and independence through distribution which drove cypherpunks to build Bitcoin are active in other industries today. If we are to predict the future, it is these industries we should consider alongside blockchains:

- **Green energy** will save us from cooking ourselves to death. But it is also a stimulus towards distribution. Energy is thermodynamically expensive to move around, and so it is vital to capture it near where it is being used. Our existing, highly centralized grid is already transitioning to solar, wind, and geothermal driven more by unit economics than by environmentalism. Once energy harvesting is sufficiently distributed, the grid itself will dissolve into a distributed foam of local energy transport networks and just-in-time markets.
- **3D-printing** is still very much in its infancy, but one day (sooner than you think) it will be possible to 3D-print many of the items in our lives, and certainly most of the small, consumable ones. Global supply chains will be completely disrupted. We will mostly ship raw materials, and we will make finished products near to where they are used. Distributing manufacturing processes to the edges of the supply chain amounts to a form of “reverse-Mercantilism”.

- **Mesh networking** IOT is not the only use case for mesh networks. Our centralized telecommunications infrastructure is too easy to monitor and manipulate and people will eventually (later than we hope) realize this. A new Internet, built on top of a planet-spanning fully distributed mesh infrastructure both implemented on and incentivized by some future blockchain is inevitable in our view.

Today, you use the Internet to buy products on Amazon which were made in China using raw materials from around the world. The government monitors your Internet traffic. Amazon knows about everything you buy. Huge amounts of dirty energy are wasted transporting raw materials to places such as Shenzhen and then transporting the finished products through a small number of global shipping firms. The cost for all of this inefficiency & overhead is passed on to you. And then you gotta pay that sales tax.

In the future, you will use a mesh Internet to buy blueprints for a product sold in a distributed marketplace to print out in a local 3D-printer and you will pay for the blueprints and the materials & energy the 3D-printer used with cryptocurrency. No one will be able to monitor your messages or transactions. No single company will know about everything you buy. A minimal amount of matter will be transported to you. The energy required to build your product will be sourced sustainably and locally where you live.

When communications, money, manufacturing, and energy are all distributed in this way why would the corporations providing them remain centralized? Global marketplaces such as Amazon can exist on blockchains without requiring corresponding centralized corporations to build them. There may still be large swaths of the economy controlled by global companies but the fabric of these companies will be distributed.

If it sounds laughable to you to imagine that global mega-corporations such as Amazon or Bosch or Merck will dissolve into distributed autonomous organizations (DAOs), consider that Bitcoin already provides a compelling real-world example. Bitcoin is a DAO which “sells” a token (BTC) which serves as a trusted store-of-value for its holders. Bitcoin mining increases the security of the BTC token for its users so Bitcoin miners are “hired” by Bitcoin and paid in the same token. It sounds circular, but it’s really just smartly-balanced incentives.

ICOs, decentralized exchanges, lending, & investment platforms show that many other financial services beyond storing value & making payments can also be provided by DAOs. “World computers” such as Ethereum are trying to distribute computing while other projects are distributing storage, bandwidth, & data. Together these chains will distribute cloud computing, the basis for so much of the modern economy. Though more nascent, there are projects working to distribute identity, social media, journalism, property

ownership, insurance, &c. Supply-chain oriented blockchains are trying to disrupt shipping, manufacturing, & logistics.

If global corporations are distributable then why not nation states? Plans for state-backed cryptocurrencies are already operating in several nations. How long before the state itself is backed by a blockchain? After all, blockchains can be thought of as the first *political technology* in the history of the world and are absolutely capable storing political capital in addition to monetary capital.

It was impossible to predict all the details of our modern world in 1844, and it is just as impossible to predict the details of the future in 2018. But we can certainly see the trend: a more distributed world where energy and resource allocation will still matter, but centralized supply chains, media & energy networks, and the perverse incentives they create will be gone. Blockchains and the distributive technologies discussed above form a mutually self-reinforcing autocatalytic set which will together distribute the world.

So why does it matter?

The Internet was a tremendous innovation, but it was also the endpoint of a centuries-long evolution in centralizing technology. Blockchains are the beginning of a future evolution in distributing technology. Comparing blockchains such as Bitcoin to the telegraph emphasizes the scope of this future evolution and helps you to adopt the long-view on cryptocurrencies.

Amara's Law applies to blockchains more than any other recent technology:

We tend to overestimate the effect of a technology in the short run and underestimate the effect in the long run.—Roy Amara

If you believe that the ICO token you bought yesterday is going to solve the world's problems tomorrow (as well as make you arrogantly wealthy), you're falling for the first part of Amara's Law. But if you believe that nation states, global supply chains, planet-spanning banks and oil pipelines will not fundamentally change in the next century, you are falling for the second part of Amara's Law. Blockchains may not fix the world, but they are definitely going to change it.

OK OK, but what does this mean for the Bitcoin price?

However the distributed future looks, Bitcoin is positioned to be its global reserve currency. Bitcoin is flawed but beautiful: we may never use it to buy coffee or as a platform for building web applications, but it has proven to be an excellent way of safeguarding wealth against inflation, censorship, forgery, seizure, and corruption. Emerging "Layer 2" solutions such as the Lightning

Network make transacting with Bitcoin even easier. The energy markets, atom exchanges, social networks, global mesh internet, sundry political tribes and, indeed, coffee shops of the distributed future will settle their accounts, eventually, to the Bitcoin blockchain.

Satoshi's promise was that by holding Bitcoin, you potentially hold a share of the total economic activity of the entire future world. This prophecy galvanized early adopters to buy in, but it is the real work of programmers, entrepreneurs, educators, regulators, and ordinary users that will make this vision come true. If these workers can help Bitcoin survive decades of more FUD, alternating adulation and vilification, solve its own scalability and governance issues, and learn to interoperate with the many other blockchains that are succeeding in their own domains, then the price of a single Bitcoin will be many times what it is today.

If you're convinced that the major coins such as Bitcoin, Ethereum, &c. are "too big already" and won't appreciate in price anymore, you're making the mistake of thinking these technologies & social movements are nearing maturity. They are not. They are still early.

Those of you worried about timing your entrance into Bitcoin and other cryptocurrencies, "waiting for the dip", are similarly making the mistake of chasing an extra 20% return in the short-term at the risk of missing out entirely on future growth.

The truth is, BTC at \$5k, \$10k, \$20k or ETH at \$100, \$500, \$1000 are *a bargain*. If Bitcoin really is the telegraph then an entire revolution in technology, politics, and society itself is about to occur—and has already started!

So if you believe you're late to the party, don't worry—we all just got here. This is a great time to learn about and invest in Bitcoin and other cryptocurrencies. Even more important than investing, there's work to be done! There are technologies to scale, interfaces to build, regulators to educate, intransigent uncles to convince, inefficient industries to disrupt, and new business models to explore. Let's get started.

Unchained Capital is working on building the distributed future. We are creating financial instruments for long-term Bitcoin holders who believe in cryptocurrency and don't want to sell their assets but need liquidity.

Bitcoin - It may fail but we now know how to do it

By Nassim Nicholas Taleb

Posted January 22, 2018



It may fail but we now know how to do it

Foreword to the book by Saifedean Ammous

Let us follow the logic of things from the beginning. Or, rather, from the end: modern times. We are, as I am writing these lines, witnessing a complete riot against some class of experts, in domains that are too difficult for us to understand, such as macroeconomic reality, and in which not only the expert is not an expert, but he doesn't know it. That previous Federal Reserve bosses, Greenspan and Bernanke, had little grasp of empirical reality is something we only discovered a bit too late: one can macroBS longer than microBS, which is why we need to be careful on who to endow with centralized macro decisions.

What makes it worse is that all central banks operated under the same model, making it a perfect monoculture.

In the complex domain, expertise doesn't concentrate: under organic reality, things work in a distributed way, as Hayek has convincingly demonstrated. But Hayek used the notion of distributed *knowledge*. Well, it looks like we do

not even need that thing called knowledge for things to work well. Nor do we need individual rationality. All we need is structure.

It doesn't mean all participants have a democratic sharing of decisions. One motivated participant can disproportionately move the needle (what I have studied as the *asymmetry of the minority rule*). But every participant has the option to be that player.

Somehow, under scale transformation, emerges a miraculous effect: rational markets do not require any individual trader to be rational. In fact they work well under zero-intelligence –a zero intelligence crowd, under the right design, works better than a Soviet-style management composed to maximally intelligent humans.

Which is why Bitcoin is an excellent idea. It fulfills the needs of the complex system, not because it is a cryptocurrency, but precisely because it has no owner, no authority that can decide on its fate. It is owned by the crowd, its users. And it has now a track record of several years, enough for it to be an animal in its own right.

For other cryptocurrencies to compete, they need to have such a Hayekian property.

Bitcoin is a currency without a government. But, one may ask, didn't we have gold, silver and other metals, another class of currencies without a government? Not quite. When you trade gold, you trade "loco" Hong Kong and end up receiving a claim on a stock there, which you might need to move to New Jersey. Banks control the custodian game and governments control banks (or, rather, bankers and government officials are, to be polite, tight together). So Bitcoin has a huge advantage over gold in transactions: clearance does not require a specific custodian. No government can control what code you have in your head.

Finally, Bitcoin will go through hick-ups (hiccups). It may fail; but then it will be easily reinvented as we now know how it works. In its present state, it may not be convenient for transactions, not good enough to buy your decaffeinated espresso macchiato at your local virtue-signaling coffee chain. It may be too volatile to be a currency, for now. But it is the first organic currency.

But its mere existence is an insurance policy that will remind governments that the last object establishment could control, namely, the currency, is no longer their monopoly. This gives us, the crowd, an insurance policy against an Orwellian future.

Blockchain Proof-of-Work Is a Decentralized Clock

By Grisha Trubetskoy

Posted January 23, 2018

This is an explanation of the key function on Proof-of-Work in the Bitcoin blockchain. It focuses on the one feature of Proof-of-Work that is essential and shows that other features often talked about such as security are secondary side-effects, useful, but not essential. This explanation rests on illustrating a few interesting properties of how Proof-of-Work is used in the blockchain that are not immediately obvious and sometimes are rather counter-intuitive, for example how participants collectively solve a problem without *ever communicating*. Having understood each of these properties, one should conclude that Proof-of-Work is primarily a mechanism which accomplishes a distributed and decentralized system of timing, i.e. a clock. Note that this write up isn't about Proof-of-Work *per se*, it explains how the blockchain takes advantage of it. If you do not know anything about Proof-of-Work, then this link might be a good start.

The Decentralized Ledger Time Ordering Problem

Before describing the solution, let us focus on the problem. Much of the literature around Proof-of-Work is so confusing because it attempts to explain the solution without first identifying the problem. Any ledger absolutely needs order. One cannot spend money that has not been received, nor can one spend money that is already spent. Blockchain transactions (or blocks containing them) must be ordered, unambiguously, and without the need for a trusted third party. Even if the blockchain was not a ledger but just data like a log of some sort, for every node to have an identical copy of the blockchain, order is required. A blockchain in a different order is a different blockchain. But if transactions are generated by anonymous participants all over the world, and no central party is responsible for organizing the list, how can it be done? For example transactions (or blocks) could include timestamps, but how could these timestamps be trusted? Time is but a human concept, and any source of it, such as an atomic clock, is a "trusted third party". Which, on top of everything, is slightly wrong most of time due to network delays as well as the effects of Relativity. Even time dilation between someone in an airplane vs the ground, though minute, is sufficient to make ordering impossible. Paradoxically, relying on a timestamp to determine event order is not possible in a decentralized geographically dispersed system. The "time" we are interested in is not the year, month, day, etc. that we are used to. What we need is a mechanism by which we can verify that one event took place before another or perhaps concurrently. First though,

for the notions of before and after to be applicable, a *point in time* needs to be established. Establishing a point in time may seem theoretically impossible at first because there is no technology accurate enough to measure a Planck. But as you'll see, Bitcoin works around this by creating its own notion of time where precise points in time are in fact possible. This problem is well described in Leslie Lamport's 1978 paper "Time, Clocks, and the Ordering of Events in a Distributed System" which doesn't actually provide a comprehensive solution other than "properly synchronized physical clocks". In 1982 Lamport also described the "Byzantine Generals Problem", and Satoshi in one of his first emails explains, how Proof-of-Work is a solution, though the Bitcoin paper states "To implement a distributed *timestamp server* on a peer-to-peer basis, we will need to use a proof-of-work system", suggesting that it primarily solves the issue of timestamping.

Timing is the Root Problem

It must be stressed that the *impossibility of associating events with points in time* in distributed systems was the unsolved problem that precluded a decentralized ledger from ever being possible until Satoshi Nakamoto invented a solution. There are many other technical details that play into the blockchain, but timing is fundamental and paramount. Without timing there is no blockchain.

Proof-of-Work Recap

Very briefly, the Bitcoin Proof-of-Work is a value whose SHA-2 hash conforms to a certain requirement which makes such a value difficult to find. The difficulty is established by requiring that the hash is less than a specific number, the smaller the number, the more rare the input value and the higher the difficulty of finding it. It is called "Proof Of Work" because it is known that a value with such a hash is extremely rare, which means that finding such a value requires a lot of trial and error, i.e. "work". Work in turn implies *time*. By varying the requirement, we can vary the difficulty and thus the probability of such a hash being found. The Bitcoin Difficulty adjusts dynamically so that a proper hash is found on average once every ten minutes.

Nothing Happens Between Blocks

The state of the chain is reflected by its blocks, and each new block produces a new state. The blockchain state moves forward one block at a time, and the average 10 minutes of a block is the smallest measure of blockchain time.

SHA is Memoryless and Progress-Free

The Secure Hash Algorithm is what is known in statistics and probability as *memoryless*. This is a property that is particularly counter-intuitive for us humans. The best example of memoryless-ness is a coin toss. If a coin comes up heads 10 times in a row, does it mean that the next toss is more likely to be tails? Our intuition says yes, but in reality each toss has a 50/50 chance of either outcome regardless of what happened immediately prior.

Memorylessness is required for the problem to be *progress-free*. Progress-free means that as miners try to solve blocks iterating over *nonces*, each attempt is a stand-alone event and the probability of finding a solution is constant at each attempt, regardless of how much work has been done in the past. In other words at each attempt the participant is not getting any “closer” to a solution or is making no progress. And a miner who’s been looking for a solution for a year isn’t more likely to solve a block at the next attempt than a miner who started a second ago. The probability of finding the solution given a specific difficulty in a given period of time is therefore determined *solely by the speed at which all participants can iterate through the hashes*. Not the prior history, not the data, just the hashrate. The hashrate in turn is a function of the number of participants and the speed of the equipment used to calculate the hash. (NB: Though strictly speaking SHA is not progress-free because there is a finite number of hashes, the range of a 256-bit integer is so vast that it is practically progress-free.)

The SHA Input is Irrelevant

In the Bitcoin blockchain the input is a block header. But if we just fed it random values, the probability of finding a conforming hash would *still be the same*. Regardless of whether the input is a valid block header or bytes from /dev/random, it is going to take 10 minutes on average to find a solution. Of course if you find a conforming hash but your input wasn’t a valid block, such a solution cannot be added to the blockchain, but it is still Proof-of-Work (albeit useless).

The Difficulty is Intergalactic

Curiously, the difficulty is *universal*, meaning it spans the entire universe. We could have miners on Mars helping out, they do not need to know, or communicate with the Earth miners, the problem would still be solved every 10 minutes. (Ok, they’ll need to somehow tell the Earth people that they solved it if they do, or else we’ll never know about it.) Remarkably, the distant participants are communicating without actually communicating, because they are collectively solving the same statistical problem and yet they’re not even aware of each other’s existence. This “universal property” while at first seemingly magical is actually easy to explain. I used the term “universal”

because it describes it well in one word, but really it means “known by every participant”. The input to SHA-256 can be thought of as an integer between 0 and 2256 (because the output is 32 bytes, i.e. also between 0 and 2256, anything larger guarantees a collision, i.e. becomes redundant). Even though it is extremely large (exponentially larger than the number of atoms in the perceivable universe), it is a set of numbers that is known by every participant and the participants can only pick from this set. If the input set is universally known, the function (SHA-256) is universally known, as well as the difficulty requirement is universally known, then the probability of finding a solution is also indeed “universal”.

Trying a SHA Makes You a Participant

If the stated problem is to find a conforming hash, all you have to do is to try it once, and bingo, you’ve affected the global hash rate, and for that one attempt you were a participant helping others solve the problem. You did not need to tell others that you did it (unless you actually found a solution), others didn’t need to know about it, but your attempt *did* affect the outcome. For the whole universe, no less. If the above still seems suspicious, a good analogy might be the problem of finding large prime numbers. Finding the largest prime number is hard and once one is found, it becomes “discovered” or “known”. There is an infinite number of prime numbers, but only one instance of each number in the universe. Therefore whoever attempts to find the largest prime is working on the same problem, not a separate instance of it. You do not need to tell anyone you decided to look for the largest prime, you only need to announce when you find one. If no one ever looks for the largest prime, then it is never going to be found. Thus, participation (i.e. an attempt to find one), even if it’s in total secrecy, still affects the outcome, as long as the final discovery (if found at all) is publicized. Taking advantage of this mind-boggling probabilistic phenomenon whereby any participation affects the outcome even if in complete secrecy and without success, *is* what makes Satoshi’s invention so remarkably brilliant. It is noteworthy that since SHA is progress-free, each attempt could be thought of as a participant joining the effort and immediately leaving. Thus miners join and leave, quintillions of times per second.

The Participation is Revealed in Statistics

The magical secret participation property also works in reverse. The global hashrate listed on many sites is known not because every miner registered at some “miners registration office” where they report their hash rate periodically. No such thing exists. The hash rate is known because for a solution of a specific difficulty to be found in 10 minutes, on average this many attempts (~10²¹ as of this writing) had to have been made by someone somewhere. We do not know who these participants are, they never

announced that they are working, those who did not find a solution (which is practically all of them) never told anyone they were working, their location could have been anywhere in the universe, and yet we know with absolute certainty that they exist. Simply because the problem continues to be solved.

Work is a Clock

And there is the crux of it: The difficulty in finding a conforming hash acts as a *clock*. A universal clock, if you will, because there is only one such clock in the universe, and thus there is nothing to sync and anyone can “look” at it. It doesn’t matter that this clock is imprecise. What matters is that it is the same clock for everyone and that the state of the chain can be tied unambiguously to the ticks of this clock. This clock is operated by the multi-exahash rate of an unknown number of collective participants spread across the planet, completely independent of one another.

Last Piece of the Puzzle

The solution must be the hash of a block (the block header, to be precise). As we mentioned, the input doesn’t matter, but if it is an actual block, then whenever a solution is found, it happened at the tick of our Proof-of-Work clock. Not before, not after, but *exactly at*. We know this unambiguously because the block was part of that mechanism. To put it another way, if blocks weren’t the input to the SHA256 function, we’d still have a distributed clock, but we couldn’t tie blocks to the ticks of this clock. Using blocks as input addresses this issue. Noteworthy, our Proof-of-Work clock only provides us with ticks. There is no way tell order from the ticks, this is what the hash chain is for.

What About the Distributed Consensus?

Consensus means agreement. What all participants have no choice but to agree on is that *the clock has ticked*. Also that everyone knows the tick and the data attached to it. And this, in fact, does solve the Byzantine Generals Problem, as Satoshi explained in an email referenced earlier. There is a separate consensus in a rare but common case of two consecutive ticks being associated with conflicting blocks. The conflict is resolved by what block will be associated with the next tick, rendering one of the disputed blocks “orphan”. How the chain will continue is a matter of chance, and so this too could probably be indirectly attributed to the Proof-of-Work clock.

And that is it

This is what Proof-of-Work does for the blockchain. It is not a “lottery” where miners win the right to solve a block, nor is it some peculiar conversion of real energy into a valuable concept, those are all red herrings. For example the

lottery and the miner's reward aspect is what encourages miners to participate, but it isn't what makes the blockchain possible. Blocks hashes form a chain, but again, that has nothing to do with Proof-of-Work, it cryptographically reinforces recording of the block ordering. The hash chain also makes the previous ticks "more certain", "less deniable" or simply more secure. Proof-of-Work is also the mechanism by which blocks become effectively immutable, and that's a nice side-effect which makes Segregated Witness possible, but it could just as well be done by preserving the signatures (witness), so this too is secondary.

Conclusion

The Bitcoin blockchain Proof-of-Work is simply a distributed, decentralized clock. If you understand this explanation, then you should have a much better grasp of how Proof-of-Work compares to [Proof-of-Stake](#), and it should be apparent that the two are not comparable: Proof-Of-Stake is about (randomly distributed) authority, while Proof-of-Work is a clock. In the context of the blockchain, Proof-of-Work is probably a misnomer. The term is a legacy from the [Hashcash](#) project, where it indeed served to prove work. In the blockchain it is primarily about verifiably taking time. When one sees a hash that satisfies the difficulty, one knows it must have taken time. The method by which the delay is accomplished is "work", but the hash is primarily interesting because it is a proof of *time*. The fact that Proof-of-Work is all about time rather than work also suggests that there may be other similar statistical challenges that are time-consuming but require less energy. It may also mean that the Bitcoin hashrate is excessive and that the Bitcoin clock we described above could operate as reliably on a fraction of the hashrate, but it is the incentive structure that drives up the energy consumption. Figuring out a way to pace ticks with less work is a trillion dollar problem, if you find one, please do let me know! P.S. Special thanks to [Sasha Trubetskoy](#) of [UChicago Statistics](#) for the review and suggestions for the above text.

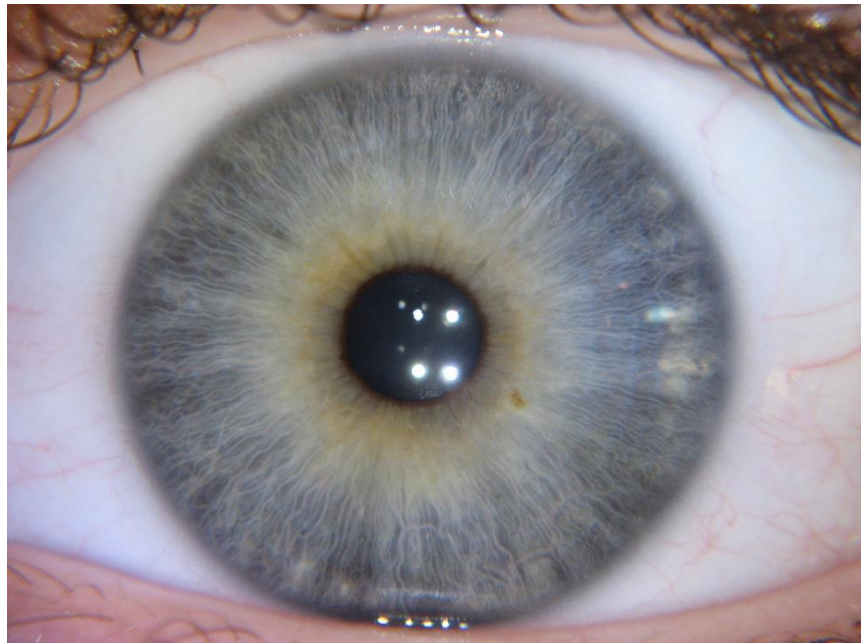
Bitcoin Surveillance: an Ahistoric Market Error

By Beautyon

Posted January 30, 2018

We read from the reliable Vortex that a Bitcoin company has been working on surveillance tools that they've now launched.

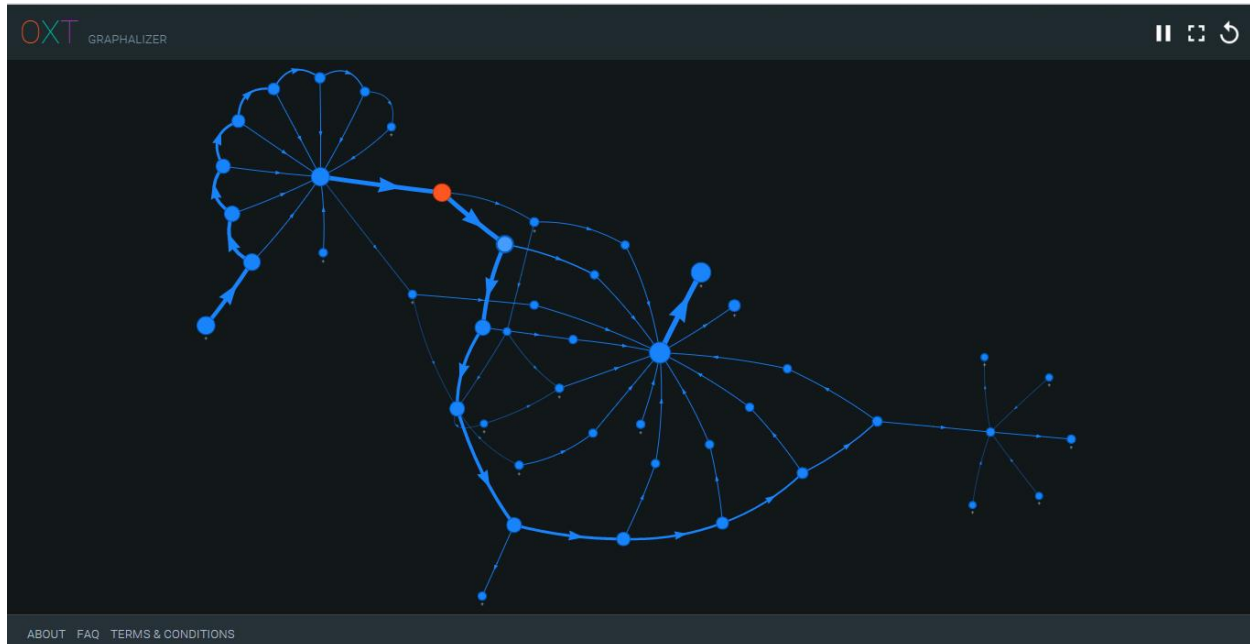
It appears that many people in Bitcoin don't understand several aspects of the future and past of money and its effects, so let's go through some of them now, to put this very curious news into context.



In *Crawford v The Royal Bank* the court held that money in circulation that had been previously stolen but subsequently used legitimately could not be returned to its original owner, even if that owner could prove the notes were his before any subsequent holder. The utility of money was held to be of greater importance to society than restitution of stolen goods, and should the money be returned to the victim of theft it...

“would be to render the Notes absolutely useless, and consequently would in a great Measure deprive the Nation of the Benefit of the Banks, which could hardly subsist without the Circulation of their Notes”

Obviously this historic and important case and principle is directly transposable to Bitcoin today. I will now explain why this is the case, after which you will see why Bitcoin Surveillance is not only an unethical thing, but a dead end on a hiding to nothing. Every Bitcoin, for all intents and purposes, has a serial number attached to it, that can be followed on the public block chain.



A graph showing Bitcoin connections on the OXT site.

Each one of the blue circles on the graph above represents a person, and a Bitcoin transaction on the block chain between two or more parties. If you know what any purchase was for, and who made it, you can trace where those coins go in the future if they move. What this company and others are doing is providing a tool that correlates information on the block chain to people and purchases, scoring and marking each one. This is nothing less than a direct attack on Bitcoin's *fungibility*...

fun·gi·ble

/ˈfʌnjəbəl/

adjective LAW

(of goods contracted for without an individual specimen being specified) able to replace or be replaced by another identical item; mutually interchangeable.

"money is fungible—money that is raised for one purpose can easily be used for another"

In order for money to be useful, each piece of it has to be interchangeable with any other piece. This is what the court held in *Crawford v The Royal Bank*. If all Bitcoin is not equal, then Bitcoin's fungibility is damaged. Obviously it makes no sense for a Bitcoin company to damage the fungibility of the thing it is trading in; this hurts the price (and perception) of Bitcoin and makes it less useful. This causes the rational actor to ask, "Who is really behind such an insane policy, that any Bitcoin company surely must know will damage their business?" This quote may provide the answer...

"The bottom line is it is very critical for the blockchain and all of this technology to really advance," said Bitfury global chief communications officer and former White House deputy press secretary Jamie Smith.

From a Coindesk Magazine report on Bitfury's Surveillance tool

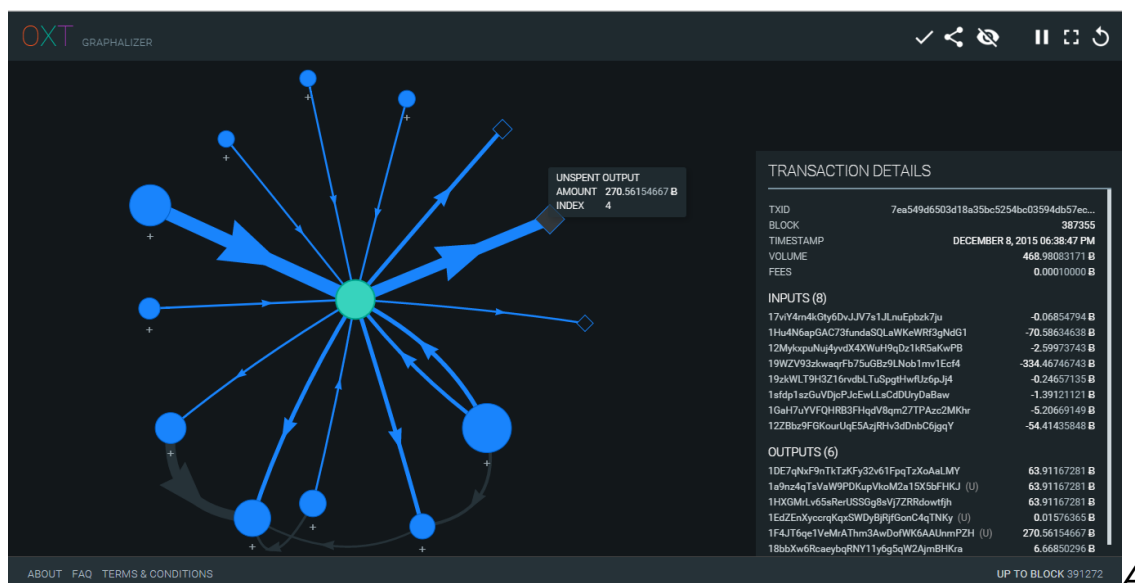
If there were such a thing as a "Conspiracy Theorist", the fact that a former White House deputy press secretary is working at BitFury, where fungibility damaging software has been developed and released, would be a red flag. What better way to destroy Bitcoin than to infiltrate Bitcoin companies and convince them to build tools that insert a layer of mistrust on top of all transactions, burdening business and spreading the contagion of suspicion throughout the network and community? Merchants would be reluctant to take Bitcoin, lest they find themselves burdened with "Dirty Coins" that they can't convert back to fiat or use in onward transactions. This would effectively put brakes and dampeners on Bitcoin's spread through society, **and the Bitcoiners themselves would be the ones doing it, at no cost to the conspirators!** From this speculative, Conspiracy Theoretic perspective, several Bitcoin companies have been infiltrated in exactly this manner, probably completely innocently; the business owners being duped into believing that if they hire an ex-government insider, that they will get some form of immunity and be left alone to innovate. But that is another Conspiracy Theory, obviously. Even without Conspiracy Theories, it is a fact that people from the ex USSR "Satellite States" are still suffering from the brainwashing and momentum of that evil system, that tortured and corrupted them for over seventy years. Eastern Europeans are far more likely to be reflexively accepting of Bitcoin Surveillance, and Statist nonsense, and there are other companies from ex USSR states that are making surveillance their business model. It's important to bear in mind that what is illegal in an ex USSR satellite state may not be illegal in the USA. Someone in the Czech Republic may mark a Bitcoin with a red flag because it was used for a purchase of a book (for example) that is entirely legal in the USA with its guaranteed rights. The only way around this would be to insert meta data on each transaction so that red flagged Bitcoin was tagged, "ILLEGAL BOOK PURCHASE IN CZECH REPUBLIC: RED FLAG" and US users being able to ignore all "criminal" activity marked in ex USSR countries as "NOT OUR PROBLEM IVAN". It would mean that Bitcoin could have many flags on it, from different jurisdictions, accumulated over time.

An Infinite Well of Taint

Remember that the supply of Bitcoin is strictly limited, and **it is never destroyed**, unlike fiat, which is recycled as it is worn out, decommissioning the unique serial numbers that are never re-used.



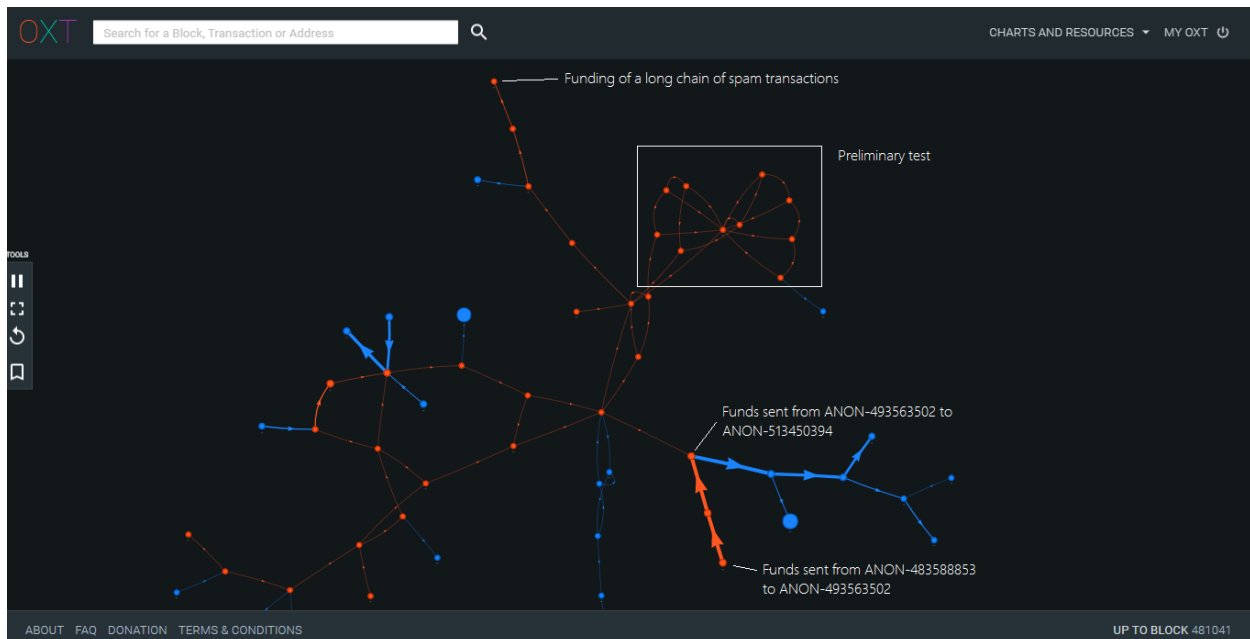
Bitcoin *never wears out, ever*. That means that by the time the last block is mined, each Bitcoin in circulation could have literally *billions* of flags attached to it, and Bitcoin consolidated with coin management tools to optimize wallets would accumulate all the flags of all transactions made with its parts, further compounding the number of flags on every Bitcoin in any wallet. And the opposite of Bitcoin consolidation exacerbates the problem exponentially. Consider this Bitcoin transaction graph...



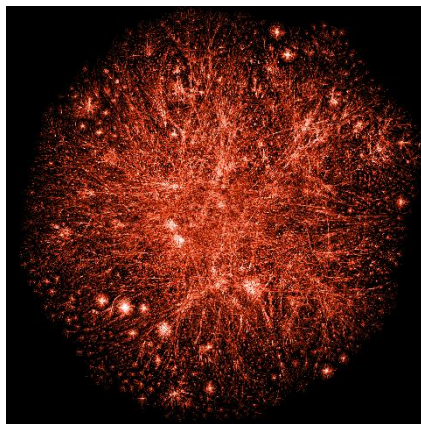
Bitcoin transaction graph from OXT

Lets say that the green dot in the centre was used to buy a book that is banned in the Czech Republic. BitFury would mark that Bitcoin as “tainted”. Six transactions are going out from the centre; that means *six addresses* are now tainted by the original transaction, and must also be marked red as “Bad

Coins". It doesn't take much imagination to see what comes next. The taint will quickly spread throughout the network until there are no Bitcoin left that do not have some sort of taint...



Eventually, **every Bitcoin will be tainted**. And if no one is allowed or is simply frightened to accept tainted Bitcoin, the entire system will collapse forever. This must be the “MUAHAHAHAHA” crazy thinking of the Statists who mistakenly believe this plan will be enough to slow down or even kill Bitcoin forever.



Better dead, than red.

These facts alone make the idea of marking Bitcoin with flags totally and absolutely unworkable. The only way around it is if flags expired, with a Statute of Limitations trigger. But this would defeat the purpose of marking the money, which is to exclude it from circulation **forever**. Obviously this idea has come from the mind of a nocoiner and anti-Bitcoiner, who has absolutely no clue about how Bitcoin works, and no idea of what its nature is or the law.

With one paragraph and a few images this idea is exposed for the farcical garbage that it is; the fever dream creation of an ignorant short-term thinker with no imagination or idea of the history of bank notes and their use in crime. No matter what these people do, **they cannot possibly win**.

Conclusion

This type of absurd, anti-Bitcoin behaviour will not last long, and will not have long lasting effects on Bitcoin. As I describe above, all Bitcoin will eventually become tainted in some way, and in fact, it will be the most tainted money in history because it is never destroyed. Furthermore, improvements to the Bitcoin protocol will make anonymity the default across the entire network, permanently blinding all anti-Bitcoin actors and killing their business models forever. Whether they succeed in marking all coins or are prevented, Bitcoin must eventually become super saturated with taint. This is not because Bitcoin is bad, but it is because man is bad, and he does bad things, and will never stop until the world ends. Bitcoin will survive these absurd and infantile attacks on its fungibility. What will not survive are the reputations of the very sad and misguided, anti-Bitcoin characters who are introducing these toxic tools to the world. History will look on them with total disdain, and their names, and the names of their companies will be a curse in the mouths of every Bitcoiner today. We are beginning to see this happen right now. **So sad!**

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



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](#)