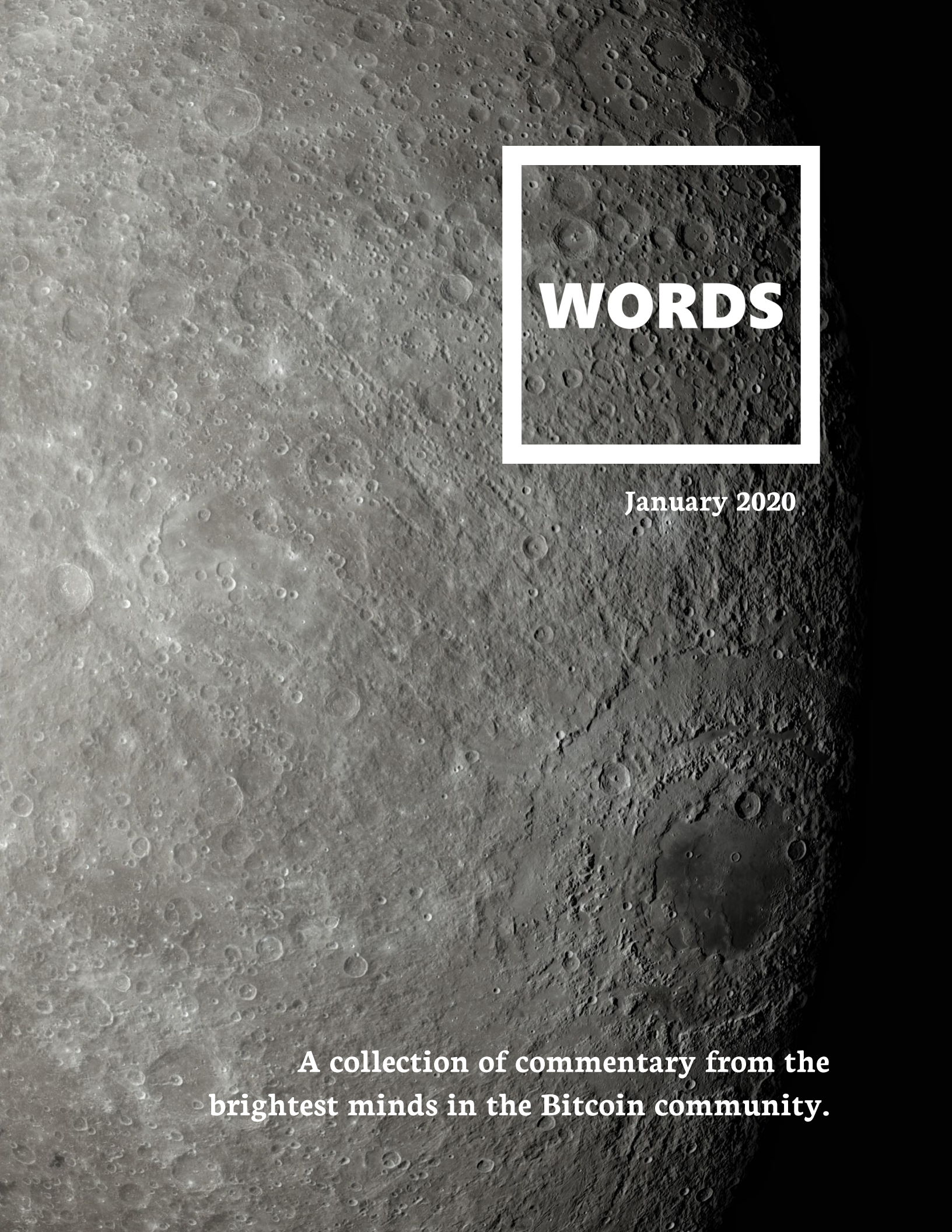


January 2020

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

Contents

Goals and Scope

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

History

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

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

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

Support WORDS

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

Support WORDS

Spread the word

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

Follow us on social media

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

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

Twitter

Subscribe to our newsletter

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

Subscribe

Our pledge

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

Bitcoin's increasing price resistance uphill, short- and long-term

By Harold Christopher Burger

Posted December 30, 2019

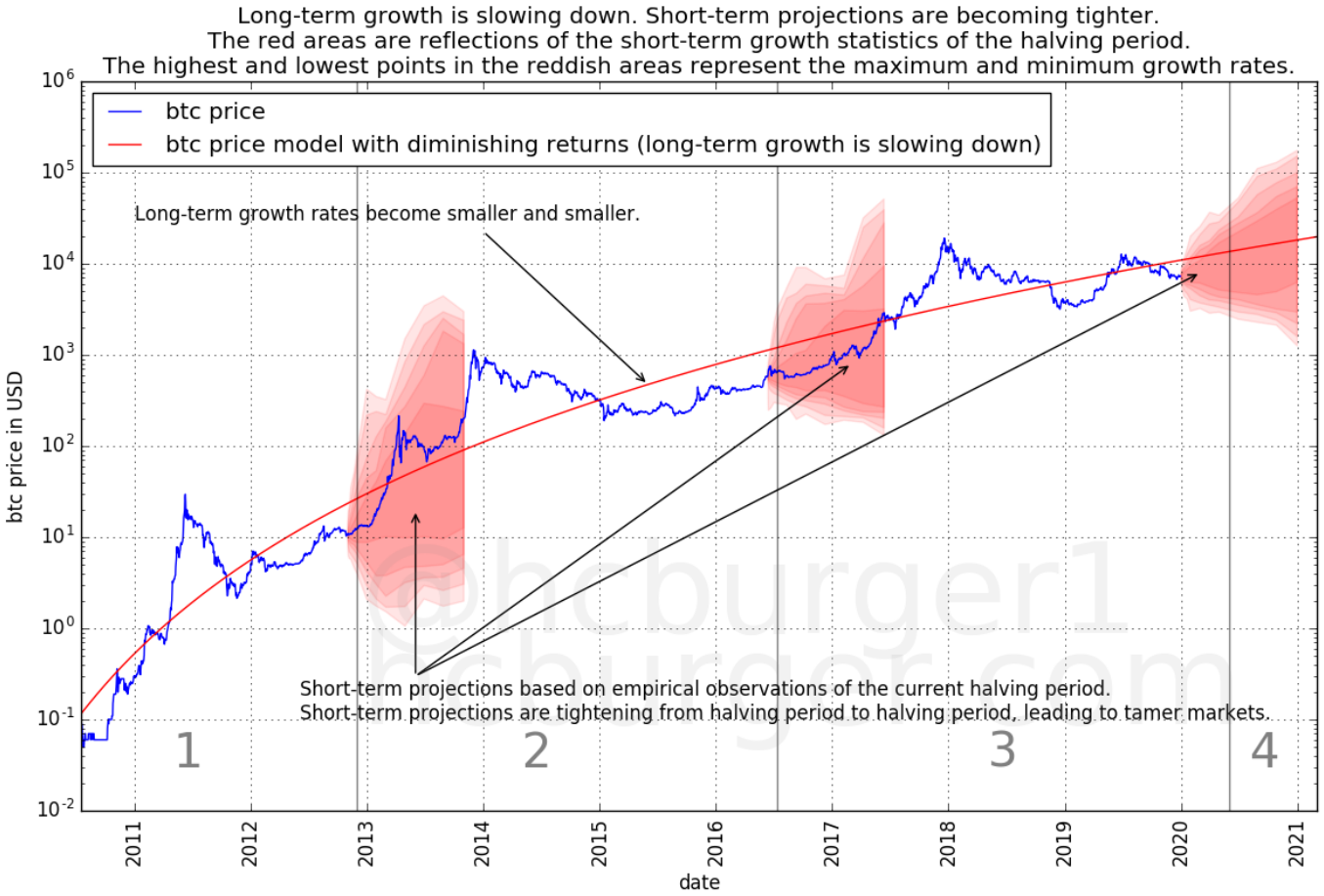
What can we say about bitcoin's future price? In "Bitcoin's natural long-term power-law corridor of growth" I have proposed a mathematical model for bitcoin's price evolution which uses a simple equation using only time as an input variable. This article will not use a precise mathematical model. Rather, we will make a number of empirical observations regarding bitcoin's price evolution. Two main observations are made:

- The case for the fact that bitcoin's price returns are diminishing over time (i.e. price growth is slowing) is strengthened.
- Bitcoin's shorter-term price movements are becoming tamer over time: Fluctuations are becoming less extreme in the short-term.

These two points can be explained by the fact that it takes more and more capital to increase the price of bitcoin, and that it becomes more and more difficult to find more capital. Moving the price of bitcoin from $0.1 to $1 was possible with relatively few dollars. Moving the price of bitcoin from $1000 to $10000 required much more capital. This effect slows the potential growth of bitcoin in both the long- and short-term.

The price of bitcoin is facing more and more resistance on its path upwards. To a lesser extent, the same is true for downward price movements.

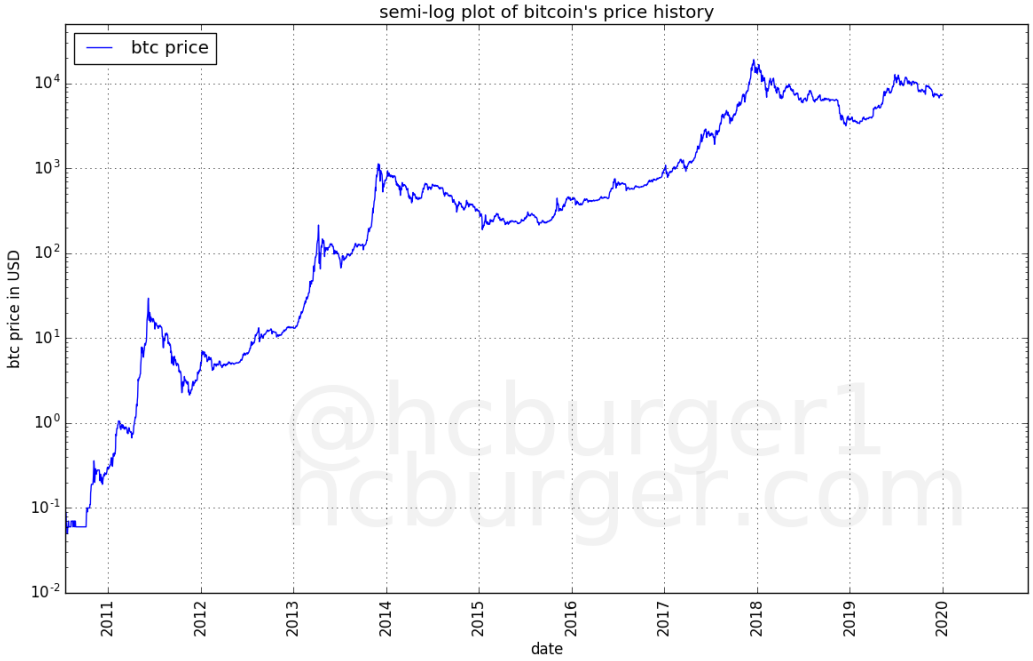
Investors should expect lower long-term gains than in the past, but also tamer and slower bull markets. Overall, bitcoin's price volatility indeed seems to decrease with time. Price growth here should be understood as being in percentage terms.



The red zones are reflections of the statistics of short-term growth rates observed within the halving period. The highest and lowest points in the reddish areas represent the maximum and minimum growth rates observed. The maximum and minimum growth rates are estimated over several hodling periods, represented horizontally. Darker areas indicate percentiles. The exact process is described further below in this article.

Diminishing or non-diminishing returns?

Bitcoin's price history is best looked at by using a logarithmic scale for the price, giving us as so-called semi-log plot, in which the x-axis represents time and is linear, and the y-axis displays the price of bitcoin, and is scaled logarithmically.



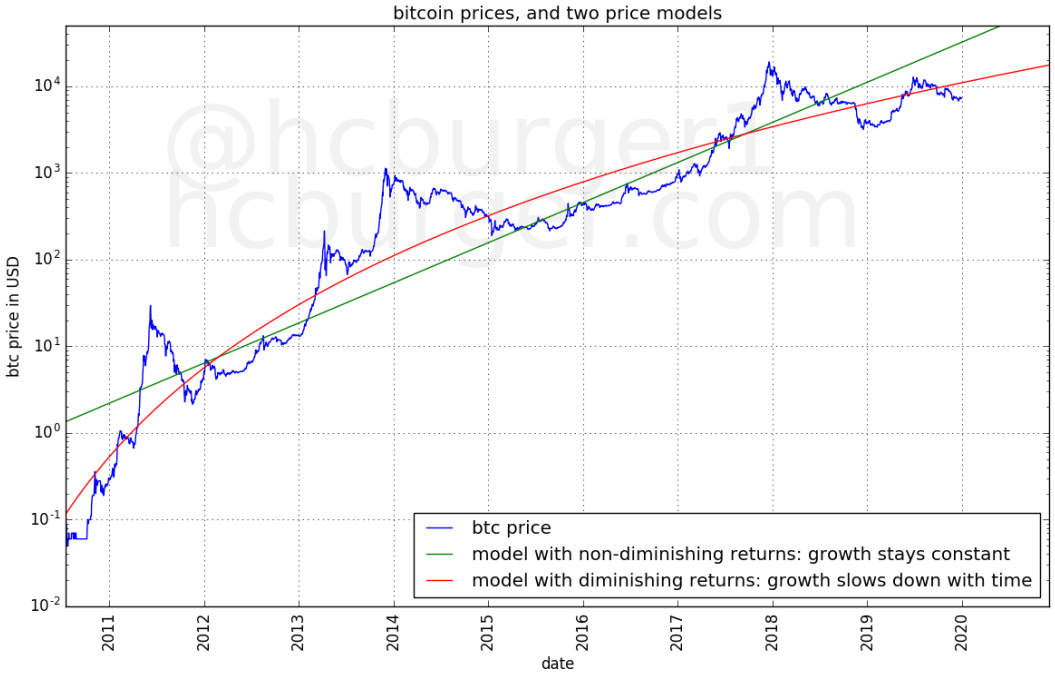
Using a logarithmic scale gives us the advantage of being able to observe bitcoin's full price history in a single plot. It also has the property that equi-distant movements on the y-axis indicate price changes that are identical in percentage terms. E.g. the price movement from $1 to $10 per bitcoin takes up the same distance on the y-scale as the price movement from $100 to $1000. This property is extremely useful but is not always perfectly understood.

To better understand the properties of a semi-log plot, let's look at two models:

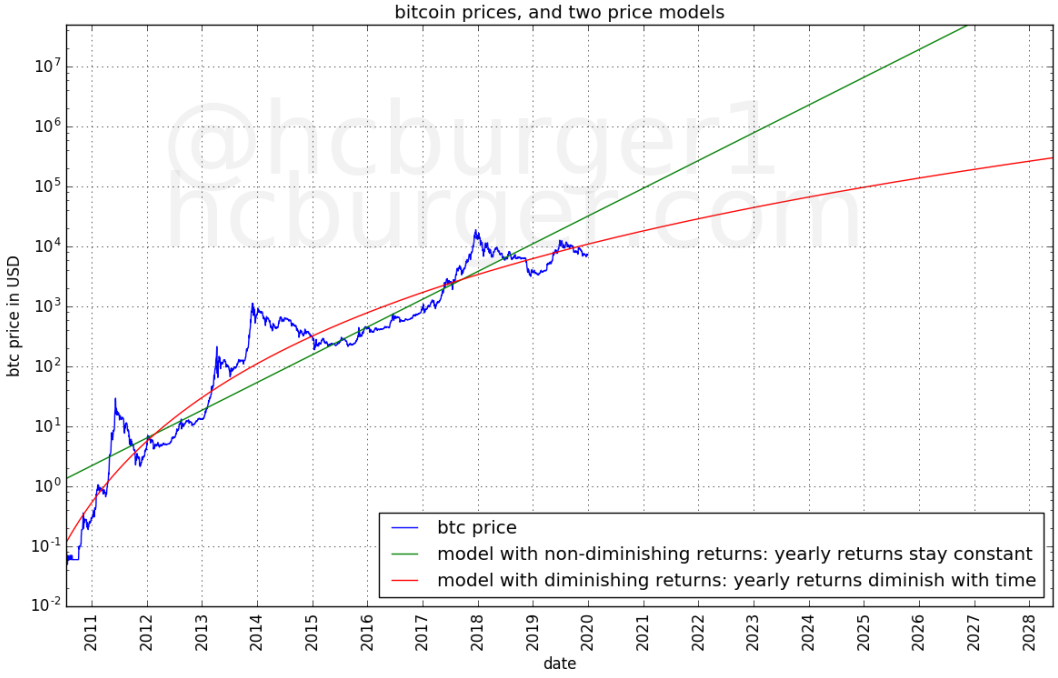
- one with non-diminishing returns (equal expected growth rates over time)
- one with diminishing returns (growth rates become smaller over time)

I used the equation described in the previous article for the model with diminishing returns, but a different model with slowing growth rates could have been used as well for the purposes of this article.

The model with non-diminishing returns displays like a straight line in the semi-log plot, whereas the model with diminishing returns displays like a curve that initially grows quickly, and then more slowly.



Which model should we prefer? The difference between the two is important, as the two predict wildly different prices in the future.



In the previous article, the choice for a model with diminishing returns was mostly motivated by the fact that the bitcoin price curve in the semi-log plot

appears to be slowing. Also, the regression error for the model with diminishing returns is "good": It is about 5.3 times lower than for the model with non-diminishing returns. The model with diminishing returns is therefore empirically better at modeling the data. This already tells us that bitcoin's long-term growth has diminishing returns, but in this article, we will make some observations that give additional weight to the conclusion that bitcoin's upward price movements face greater and greater resistance.

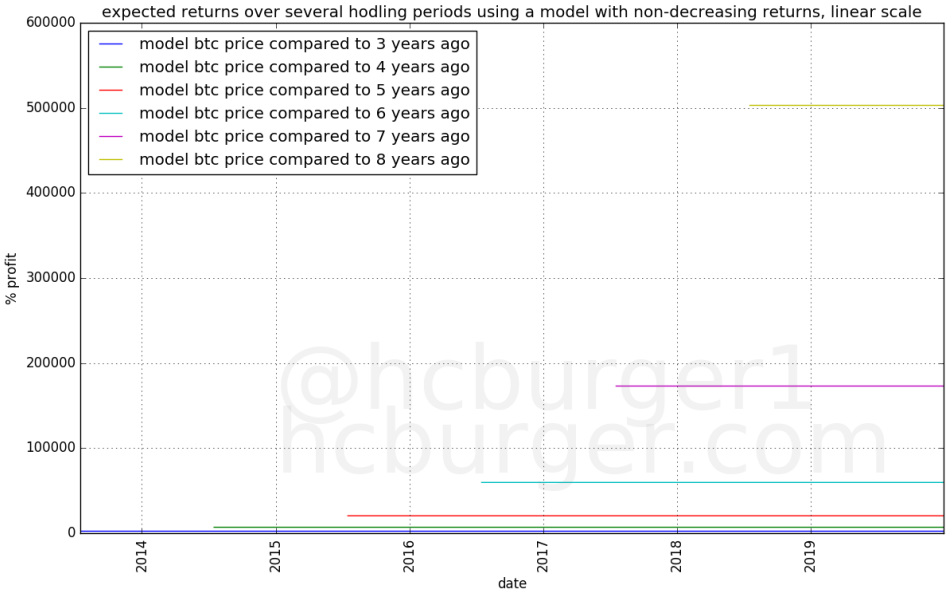
Expected returns, long term

Diminishing returns means that bitcoin's growth is slowing. Non-diminishing returns means that bitcoin's growth is not slowing down, i.e. the expected growth rate stays the same over time. To better understand the difference between the two, let's take the perspective of fictional investors.

A model with non-diminishing returns

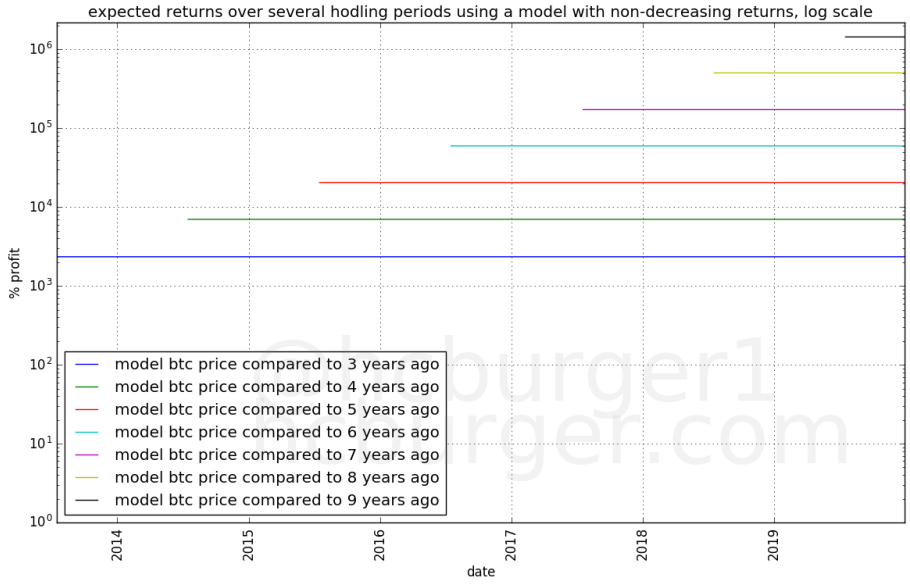
Let's assume that bitcoin's price follows a non-diminishing model. How much money can an investor expect to make? The answer depends on the amount of time the investor held his bitcoin before selling them (the "hodling period"). The longer the hodling period, the higher the expected return. What is interesting is that for the model with non-diminishing returns, the profit the investor can expect to make does not depend on when he invested.

This is demonstrated in the plot below. Each colored line represents one hodling period. The x-value of each point on the line represents the time at which the investor sold his bitcoin. The y-value represents the percent profit he made from his investment.



The longer the hodling period, the later the starting point of the line representing that hodling period. This is because bitcoin's price history is limited and we assume that it was not possible to invest in bitcoin before the 17th of July 2010. According to this, it is not possible to have held bitcoin for eight years before mid-2018, which is why the yellow line above starts in mid-2018.

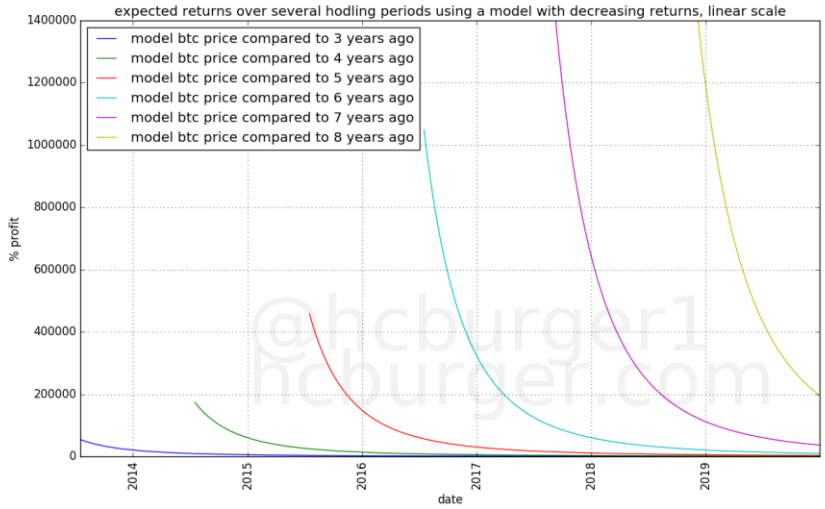
We can display the same data in a semi-log plot:



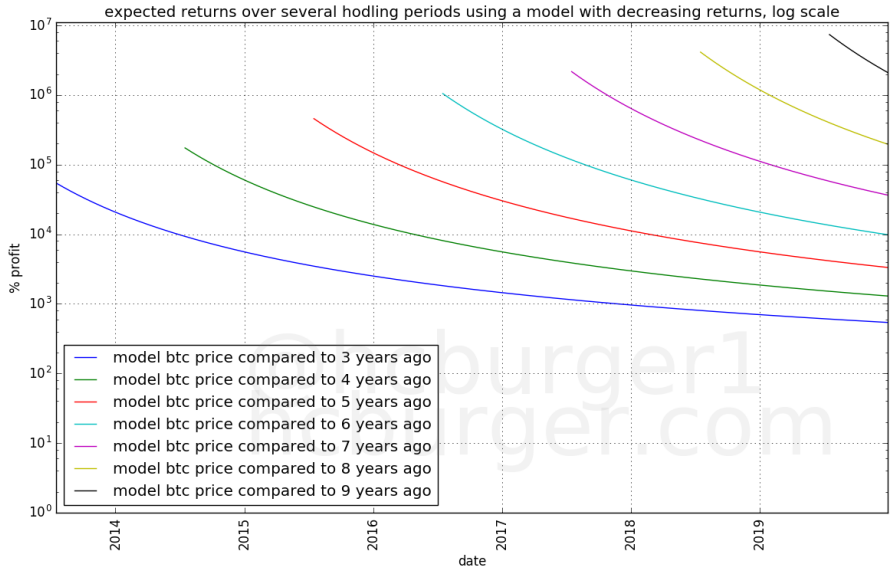
We see that according to this model, an investor who bought bitcoin and sold them 3 years later would have made a profit of approximately 2500% no matter when this investor bought his bitcoin. The same holds true for any other hodling period, but the returns are higher for longer hodling periods.

A model with diminishing returns

Using a model with diminishing returns, the situation is different: The expected returns depends on ***when*** one invested. The lines in the below plot drop sharply, which means that for the same hodling period, buying earlier gives higher expected returns.



A semi-log plot again makes the data easier to read:



Investor A who bought bitcoin in mid-2011 and sold them three years later in mid-2014 would have made about 10000% profit.

Investor B who bought bitcoin in January 2015 and sold them three years later in January 2018 would have made "only" about 1000% profit, or 10 times less than investor A.

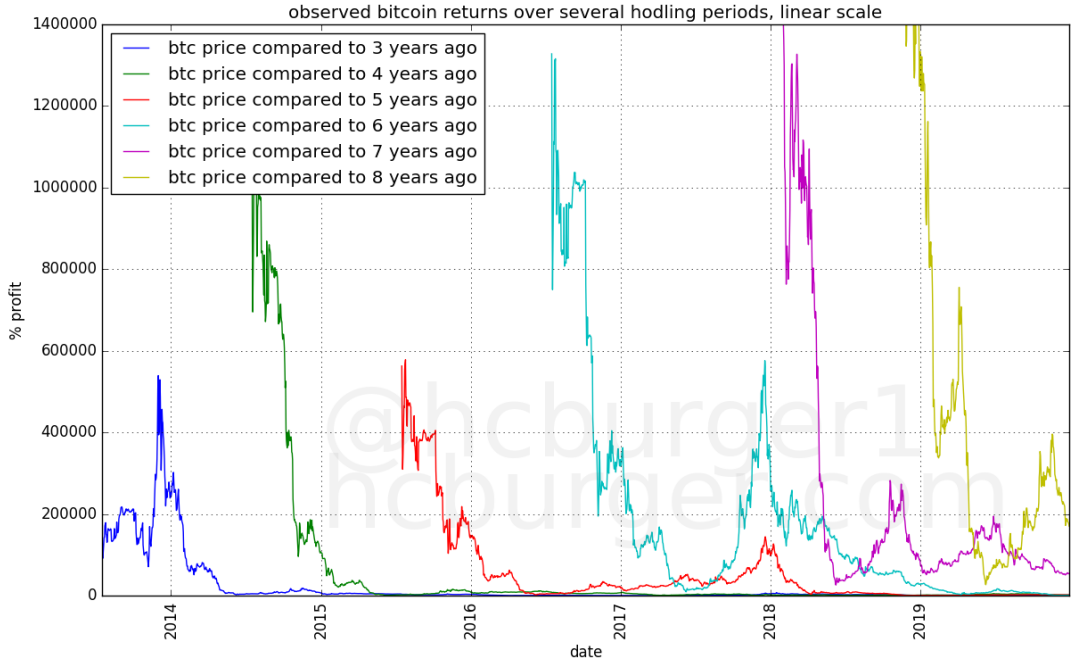
The situation is similar, but even more pronounced for longer hodling periods. A 10x decline in returns occurs faster. Investors A and B invested three and a half years apart, with a 10x difference in returns. For an 8-year hodling period, a 10x decline in returns occurs in about a year.

(Note: For the model with diminishing returns, I used the same model as in my previous article , but the exact choice of the model is not very important here, as the specific numbers are not as interesting as the principle itself.)

Actual returns

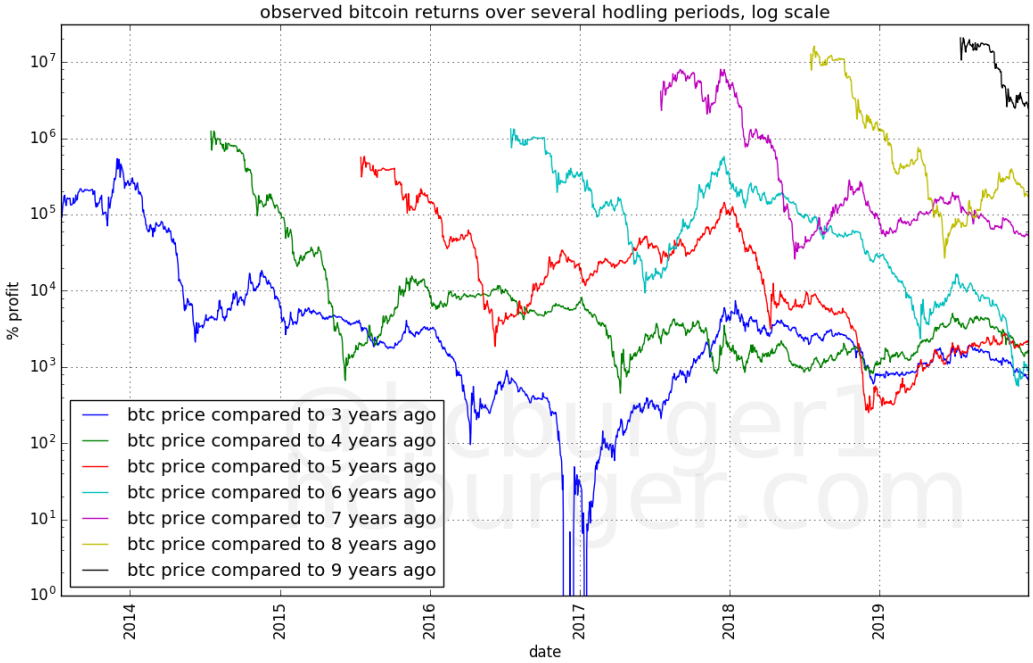
The profiles of the expected returns are very different for the model with diminishing compared to the model with non-diminishing returns. The difference is extremely important to anyone who invests in bitcoin. Which of the two models better reflects reality?

To answer this question, we will perform the same exercise as before, but using bitcoin's actual price history:

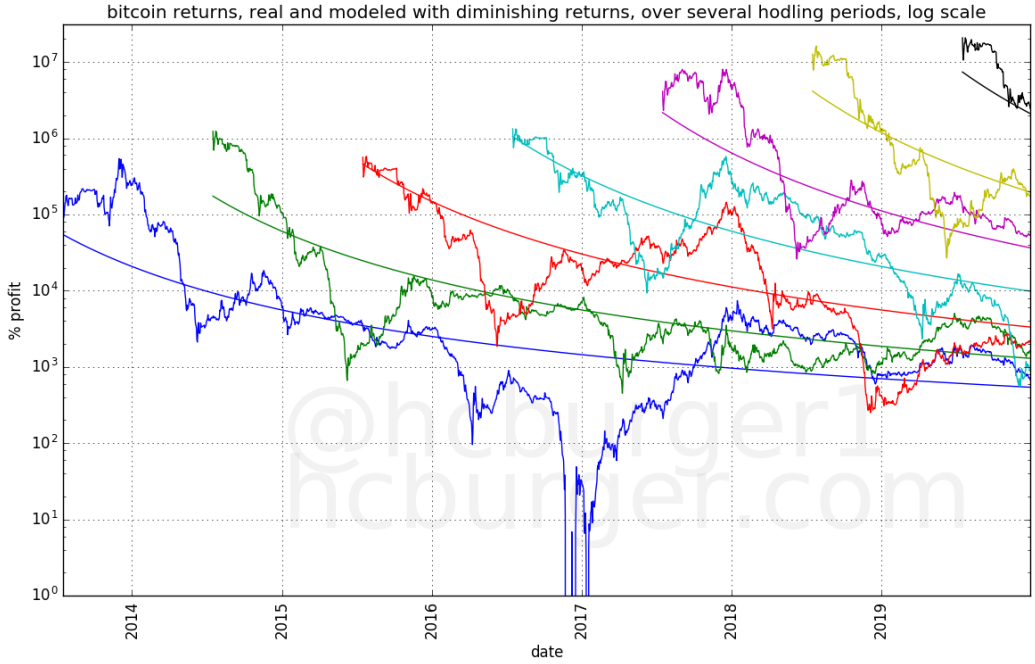


What is immediately noticeable are sharp drops in the return curves, which is in agreement with the model with diminishing returns. What is also immediately noticeable is that the curves are much more noisy than those based on model (i.e. simulated) data. The noisiness is due to the wild price swings for which bitcoin is so famous.

In the semi-log chart, we notice very low returns for the 3-year hodlers around the 2017 mark. This is because the price around 2017 was about $1000, approximately the same as during the previous all-time-high, around 2014. Someone who bought at that all-time-high and sold three years later could have made a small loss.

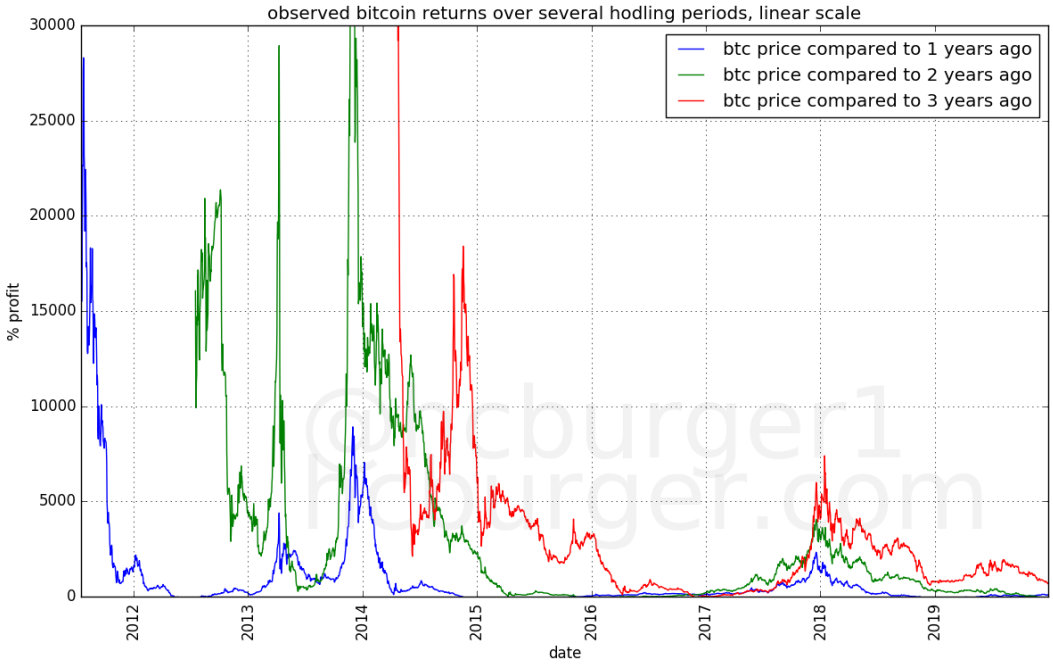


Let us now compare the real return curves to those based on model data using a model with diminishing returns. The same color-code is used for the length of the hodling periods:



We see that the real return curves are modeled adequately by the model with diminishing returns, but we have to take into account that there is quite a lot of noise.

We can also repeat the experiment for shorter hodling periods, and see a similar, but more noisy, pattern.



The return curves above show us that by the end of the year 2014 at the latest, the nature of bitcoin's diminishing returns should have become apparent. Later data confirmed that trend.

Conclusions regarding long-term trends

The return curves empirically favor a bitcoin price model with returns that diminish over time. Looking at the three- and four-year return curves, this effect would have been observed at the latest by the end of the year 2014. Newer data has only been confirming this conclusion.

The effects of diminishing returns, combined with price volatility, are:

- The expected returns for all hodlers diminish over time
- The expected returns for long-term hodlers become closer to those of shorter-term hodlers. Due to price volatility, this also means that short-term holders can sometimes have higher returns than long-term hodlers.

The conclusions regarding long-term diminishing returns were already drawn in "Bitcoin's natural long-term power-law corridor of growth" but we have looked at this effect in a novel way in this article, and have also seen that the effect would have been visible as early as 2014, or maybe even earlier. Also different from the previous article is that we arrive to similar conclusions without using a precise model. The general conclusions are therefore independent of the exact choice of the model.

Why is the price growing slower and slower?

Given the observation that bitcoin's price growth exhibits diminishing returns, can we come up with a plausible ad-hoc explanation?

Probably the simplest explanation is that increasing the price of bitcoin by a certain amount in percentage terms requires more and more fiat currency. To illustrate: Increasing the price of bitcoin by 100% took relatively little capital when the price of bitcoin was $0.1. It requires much more capital to move the price of bitcoin from e.g. $10000 to $20000.

Attracting ever more capital becomes ever more difficult, or at least, takes more and more time. Perhaps a single individual with modest funds could have moved the price from $0.1 to $0.2, but it would take a very wealthy individual to move the price from $10000 to $20000. Alternatively, the price could be moved from $10000 to $20000 by a greater number of individuals.

Attracting more and more people to invest in bitcoin, or finding a few exceptionally wealthy individuals takes more and more time.

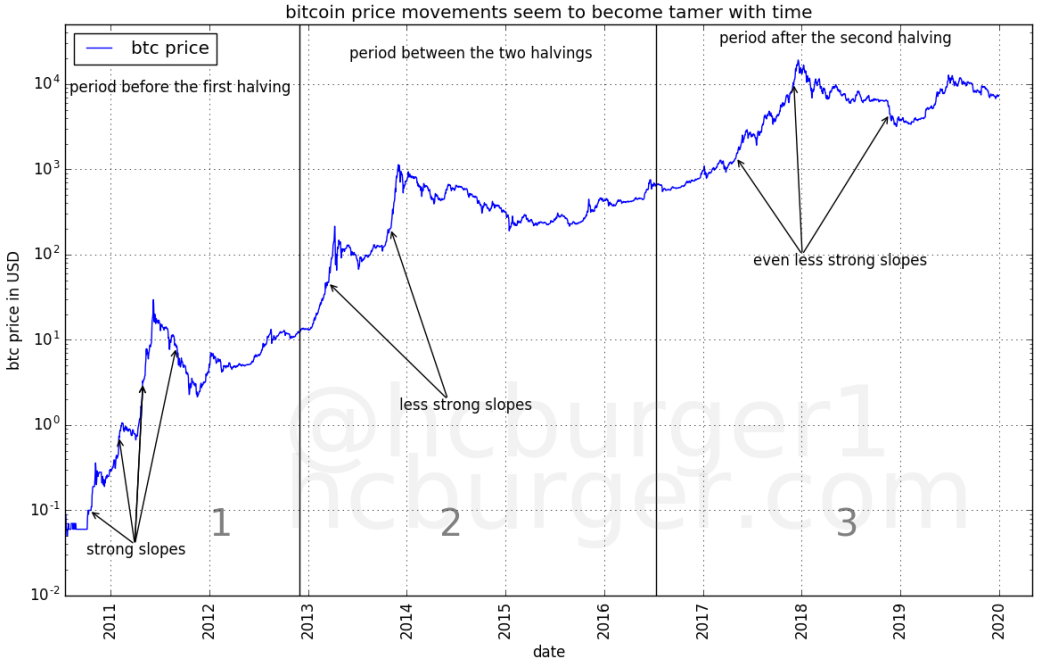
Short-term price changes

Does the above explanation for slower long-term growth rates also have an effect on shorter-term growth rates? This is something that has not been thoroughly considered in "Bitcoin's natural long-term power-law corridor of growth". Yet, higher bitcoin prices should make it more difficult to move the price in the short-term, too. This would mean that short-term price swings should become more tame over time, leading both to overall lower volatility and also potentially slower bull markets.

To answer this question, let's divide bitcoin's price history into three parts, one for each halving period:

- the period before the first halving ("halving period 1"),
- the period after the first halving and before the second halving ("halving period 2"), and
- the period after the second halving ("halving period 3").

We observe the strongest price swings during bitcoin's bull markets. The corrections following a bull market also have strong (downward) price swings. At first sight, it would appear that these shorter-term price movements become slower in the later periods, which also leads to bull markets taking longer and longer to develop:



Let's consider the slopes of the price curve. A given slope corresponds to a given price change in percentage terms, due to the nature of semi-log plots. Instead of talking about price changes in percentage terms, we can talk about differences in the log price. The two are completely equivalent.

In each period, let's consider the slopes of bitcoin's price movement over a particular timeframe, e.g. 180 days. For each 180 day timeframe, we will look at the difference between the log price at the beginning and the log price at the end of that timeframe. We then count how often this difference falls into a particular range. The result is a histogram of bitcoin log price growth rates over 180 days. The growth rates are equivalent to slopes in the semi-log plot of the price history. Negative log price changes mean that the price has been declining.

The histogram of the 180 day growth rates for the three halving periods can be displayed in a table:

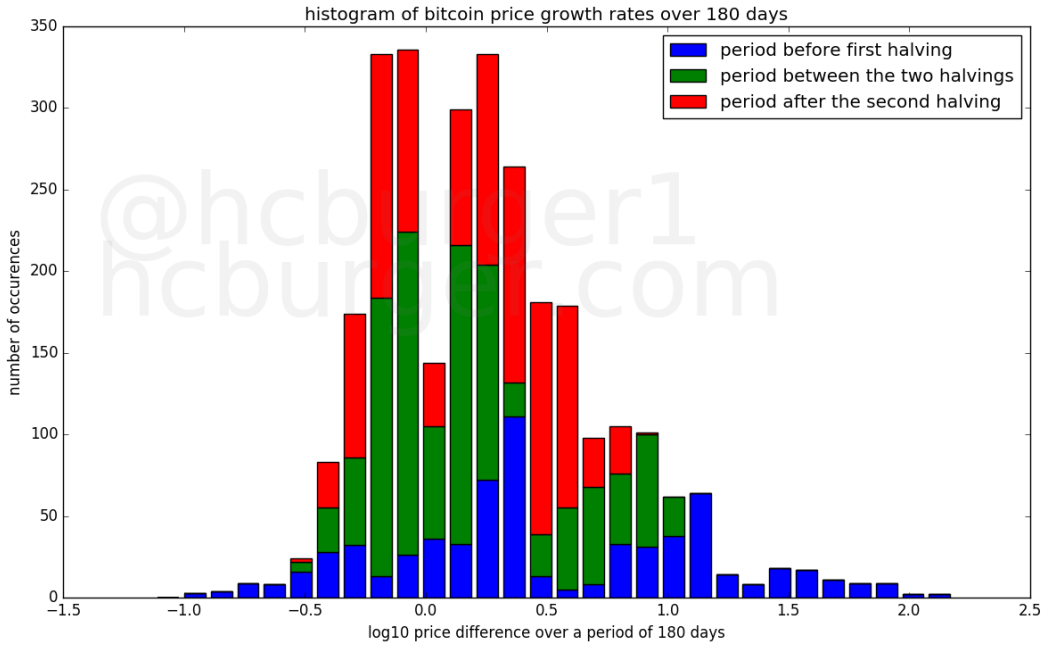
	-1.01 to -0.90	-0.90 to -0.79	-0.79 to -0.68	-0.68 to -0.57	-0.57 to -0.46	-0.46 to -0.35	-0.35 to -0.24	-0.24 to -0.13	-0.13 to -0.02	-0.02 to 0.09	0.09 to 0.20	0.20 to 0.31	0.31 to 0.42	0.42 to 0.53	0.53 to 0.64	0.64 to 0.75	0.75 to 0.86	0.86 to 0.97	0.97 to 1.08	1.08 to 1.19	1.19 to 1.30	1.30 to 1.41	1.41 to 1.52	1.52 to 1.63	1.63 to 1.74	1.74 to 1.85	1.85 to 1.96	1.96 to 2.07	2.07 to 2.18
counts for period 1:	3	4	9	8	16	28	32	13	26	36	33	72	111	13	5	8	33	31	38	64	14	8	18	17	11	9	9	2	2
counts for period 2:	0	0	0	0	6	27	54	171	198	69	183	132	21	26	50	60	43	69	24	0	0	0	0	0	0	0	0	0	0
counts for period 3:	0	0	0	0	2	28	88	137	111	39	83	129	132	142	124	30	29	1	0	0	0	0	0	0	0	0	0	0	0

(Period 1 corresponds to the period before the first having, period 2 to the period between the two halvings, and period 3 to the period after the second halving).

What becomes immediately apparent is that the earlier halving periods have more extreme growth rates, in both the positive and negative direction. For

example, the first period had 180-day growth rates of between -1.01 and -0.57 and also between 1.08 and 2.18, whereas the later halving periods do not. The second halving period has 24 instances of 180-day growth rates of between 0.97 and 1.08, whereas the third has none.

The same data can be displayed visually, allowing for easier inspection:



The blue bars representing the distribution of the growth rates of the first halving period are more spread out than the green and red bars representing the two other periods. A greater vertical size of a bar indicates a higher count in that bin. The earliest halving period is the most spread out, the second less so, and the third halving period the least.

Alternatively to the histogram, we can also consider the statistics of the 180-day growth rates for the three periods. The first number is expressed in log10 terms, whereas the number in parenthesis is expressed in percentage terms.

Halving period 1 (before the first halving):

- max growth rate: 2.156613 (14242 %)
- 90th percentile growth rate: 1.410404 (2473 %)
- 10th percentile growth rate: -0.352216 (-56 %)
- min growth rate: -0.996782 (-90 %)

Halving period 2 (between the two halvings):

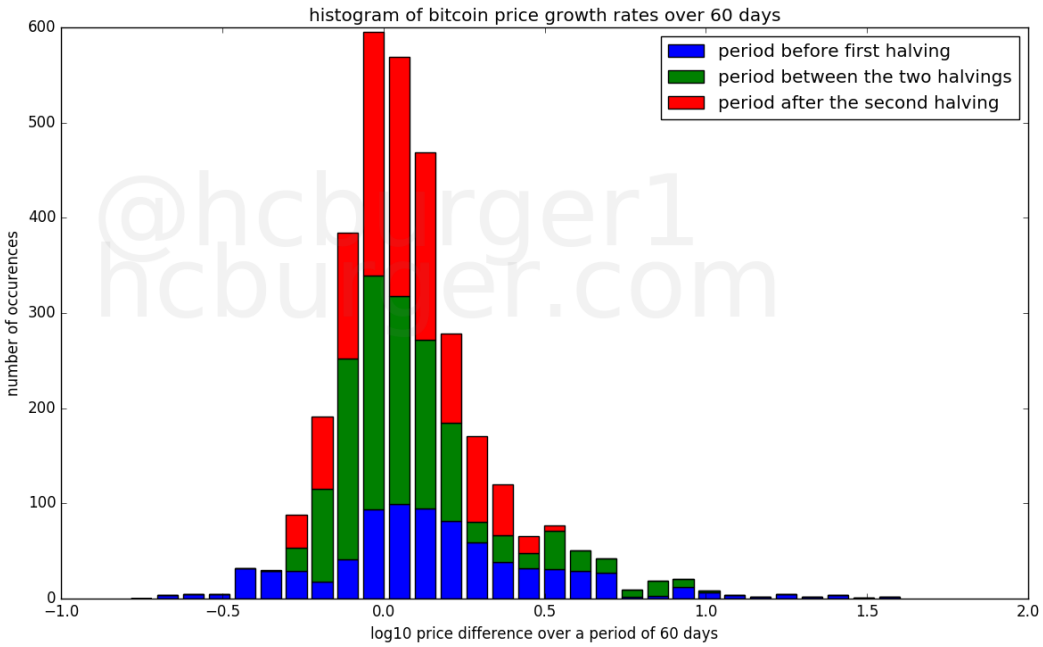
- max growth rate: 1.079093 (1100 %)
- 90th percentile growth rate: 0.810624 (547 %)
- 10th percentile growth rate: -0.225461 (-40 %)
- min growth rate: -0.518089 (-70 %)

Halving period 3 (after the second halving):

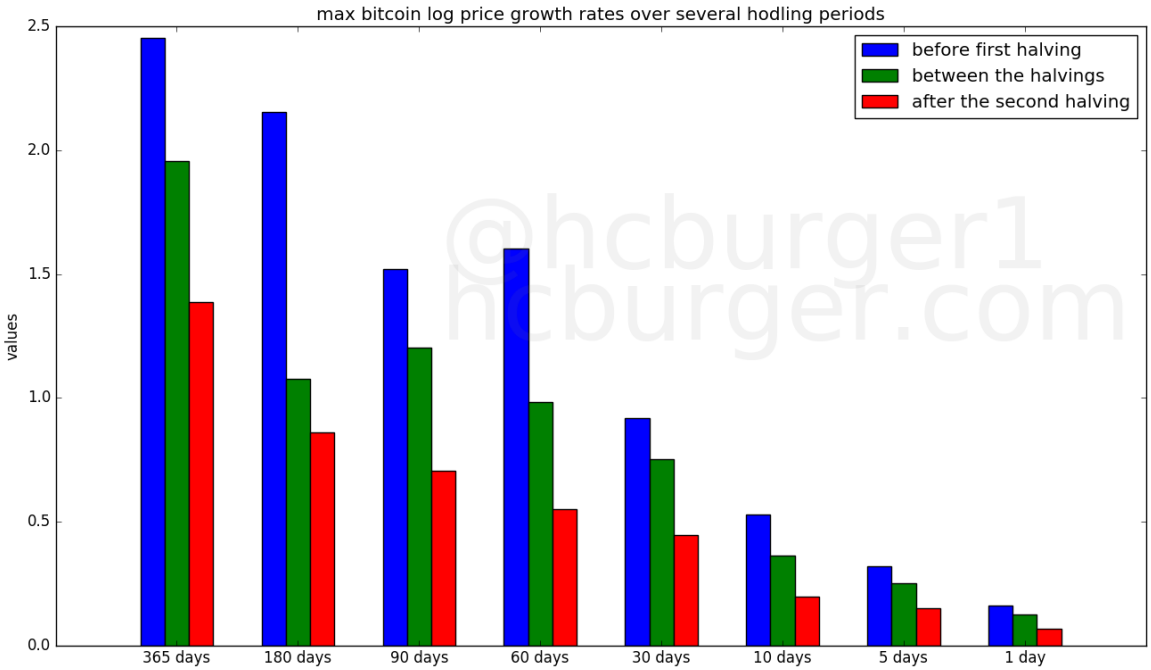
- max growth rate: 0.862816 (629 %)
- 90th percentile growth rate: 0.586342 (286 %)
- 10th percentile growth rate: -0.251239 (-44 %)
- min growth rate: -0.465312 (-66 %)

The maximum growth rate over a 180-day hodling period was 14242% in the first halving period, 1100% in the second, and 629% in the third halving period. The strongest negative growth rates over a 180-day hodling period was 90% in the first halving period, 70% in the second, and 66% in the third halving period, indicating that downward swings (over a 180-day span) have also become tamer over time.

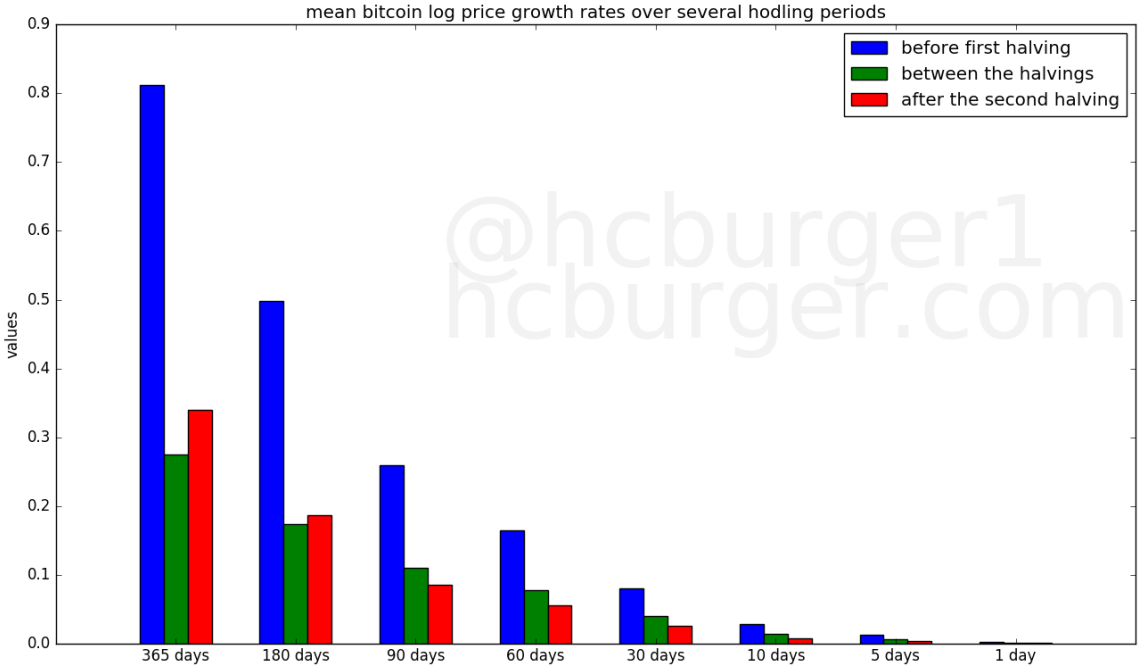
Similar observations can be made when the 180-day holding period is changed, e.g. to 60 days:



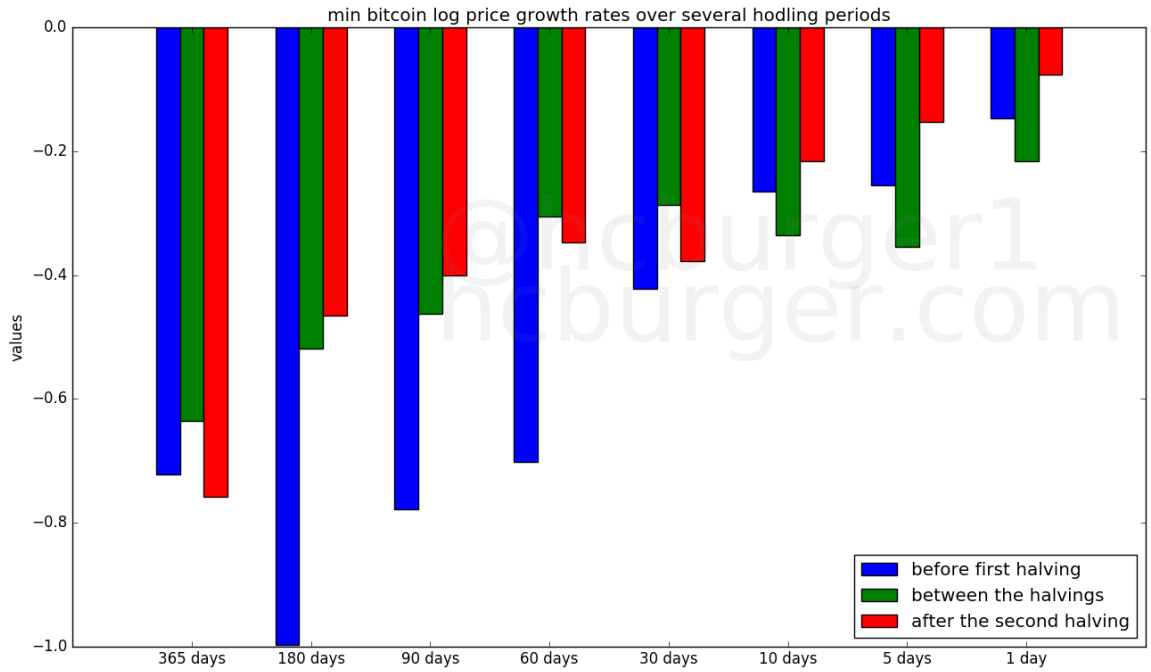
The maximum growth rate over several hodling periods systematically declines over the three bitcoin halving periods:



The mean growth rates over most hodling periods also declines over the three halving periods. This is just a reflection of the fact that the price of bitcoin has been increasing at a slower and slower rate.

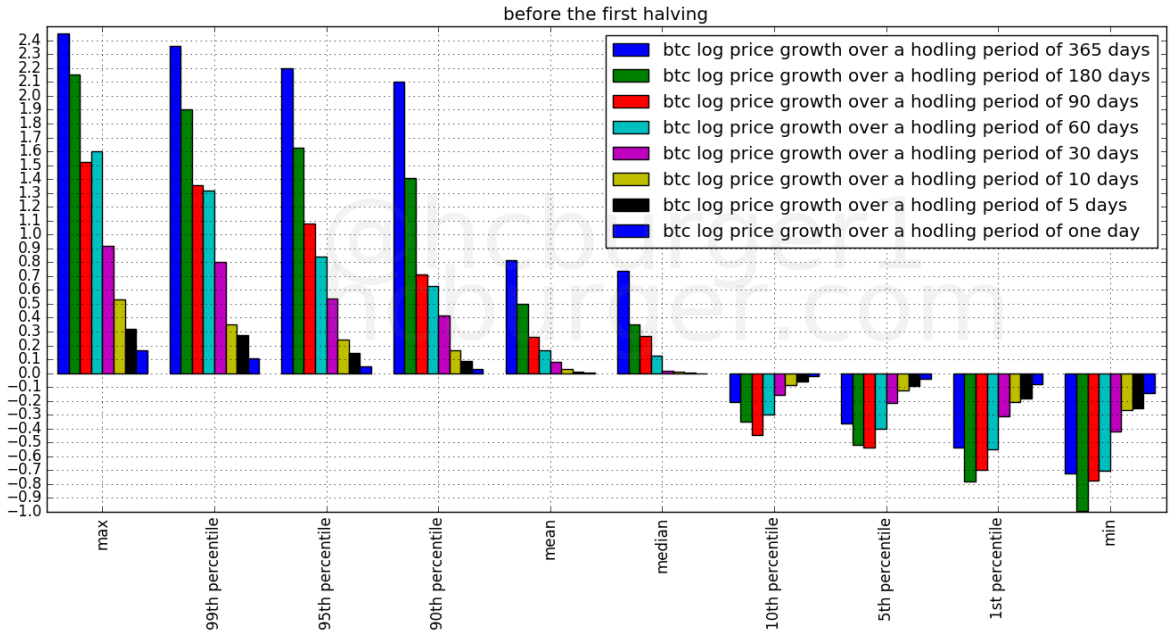


The value of the minimum growth rate over several hodling periods also tends to decrease over the three halving periods, though this effect is less marked than for the maximum growth rate.

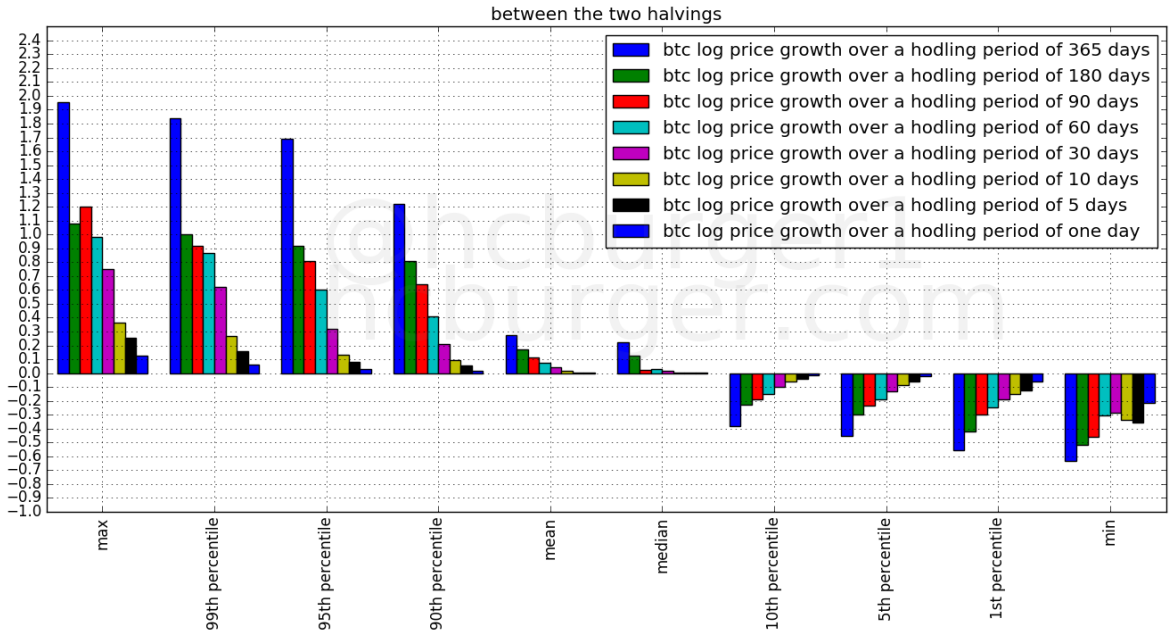


Let's now make one plot per halving period. Each plot contains several statistics over several hodling periods. The percentiles are statistics that lie between the min and the max, so that e.g. the 90th percentile can be used as a form of "attenuated max", or the 10th percentile as a form of "attenuated min". The 50th percentile is the same as the median.

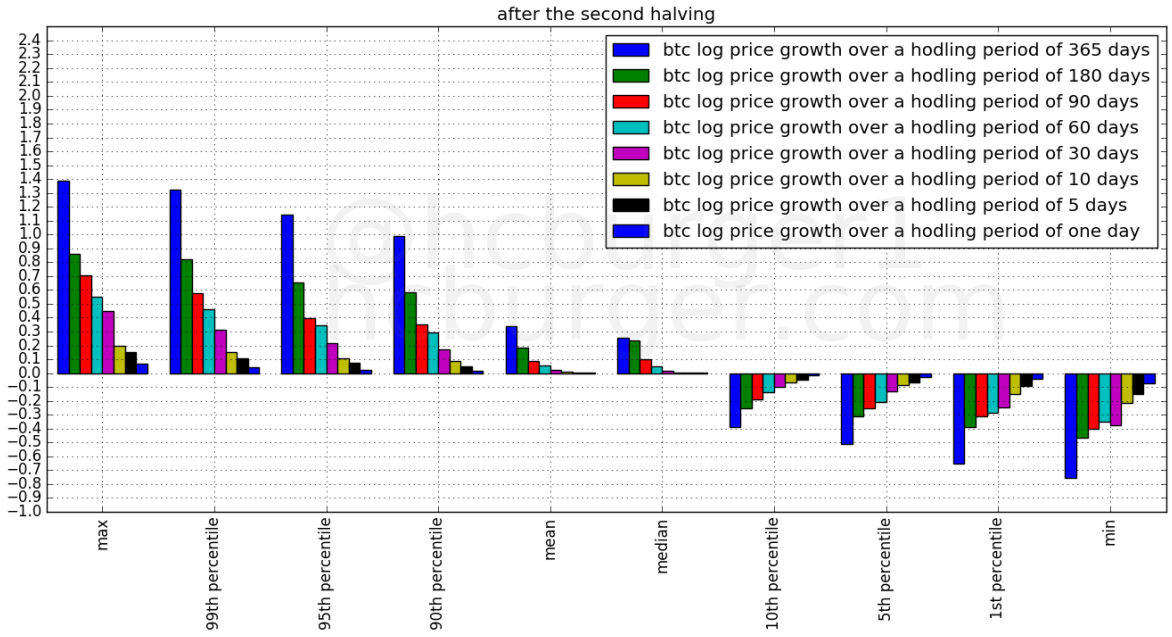
The following plot displays the statistics for the first halving period:



The next plot displays the statistics for the second halving period. The y-axis still uses the same scale. The fact that almost all bars have shorter length means that the statistics over most hodling periods have been attenuated.



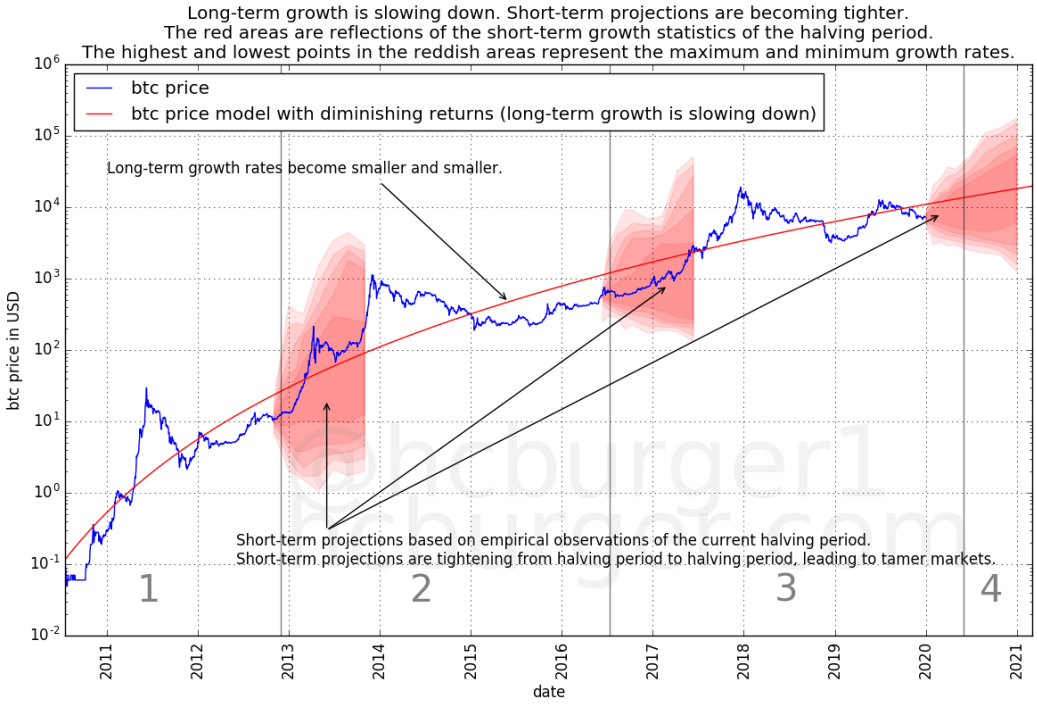
The statistics are further attenuated from the second to the third halving period:



These three plots confirm that the positive growth rates over relatively short hodling periods become smaller and smaller in each succeeding halving period. To a lesser extent, negative growth rates also become smaller over time.

These observations are in agreement with our explanation that it takes ever more capital to cause price fluctuations, and hence price fluctuations become tamer. We should expect this trend to continue in the future.

The statistics computed above can also be represented graphically. In the following plot, we display the statistics of each halving period at the end of that halving period, anchored at the price at that given time. The vertical width of the red regions represents the difference between the min and the max growth rates. The red regions have a horizontal width of 365 days because that is the longest short-term hodling period we have considered. Darker red tones just represent different percentiles.



This is another convenient representation showing that the statistics over the short term have become tamer in successive halving periods.

Future price developments

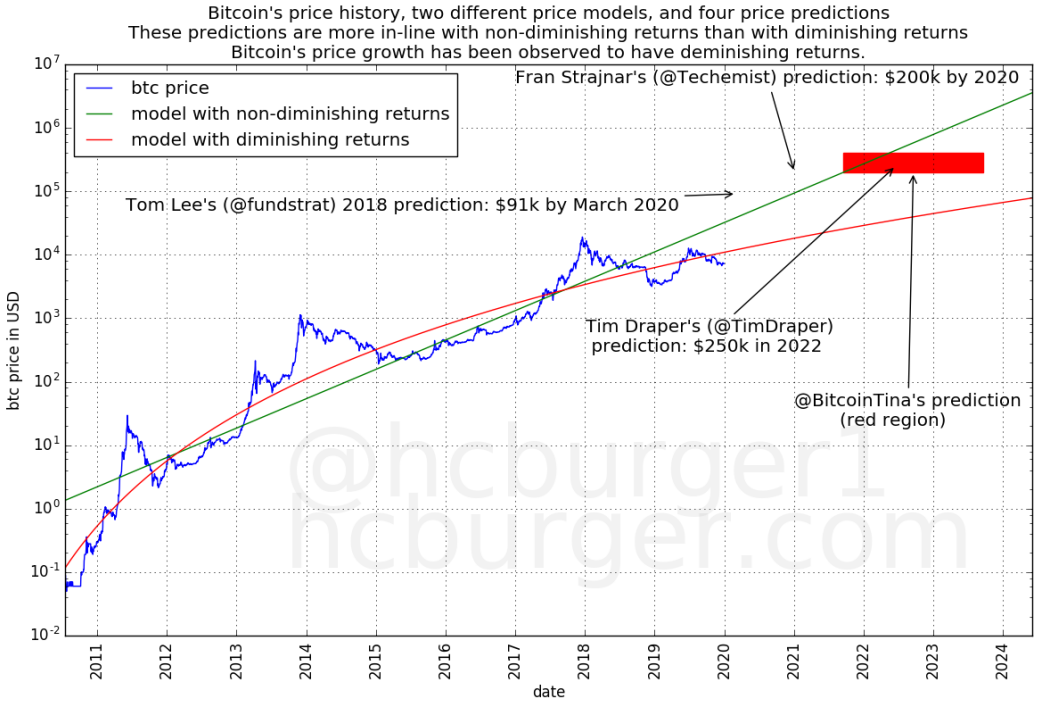
We have two ways of looking at price predictions and models. Assessing whether:

- the long-term projections are realistic
- the short-term projections are realistic.

Let's look at a few potential scenarios.

Predictions made by individuals

It appears that it is believed by some that bitcoin's price will grow with non-diminishing returns, leading to some price predictions being made that are more in-line with the model with non-diminishing returns than with the model with diminishing returns:



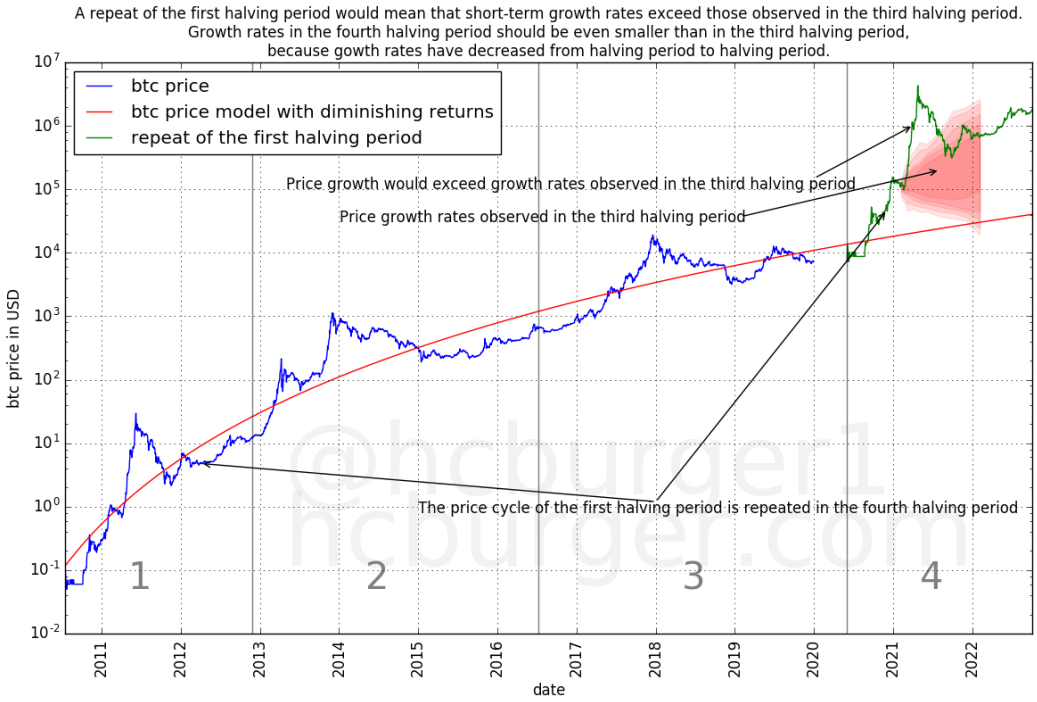
Source of the predictions for Tom Lee and Fran Strajnar, Tim Draper, and BitcoinTina.

Since these predictions are not in line with diminishing returns, and we have empirically observed long-term price growth to be diminishing, it would be surprising for any of these predictions to come true.

Cycle repeats

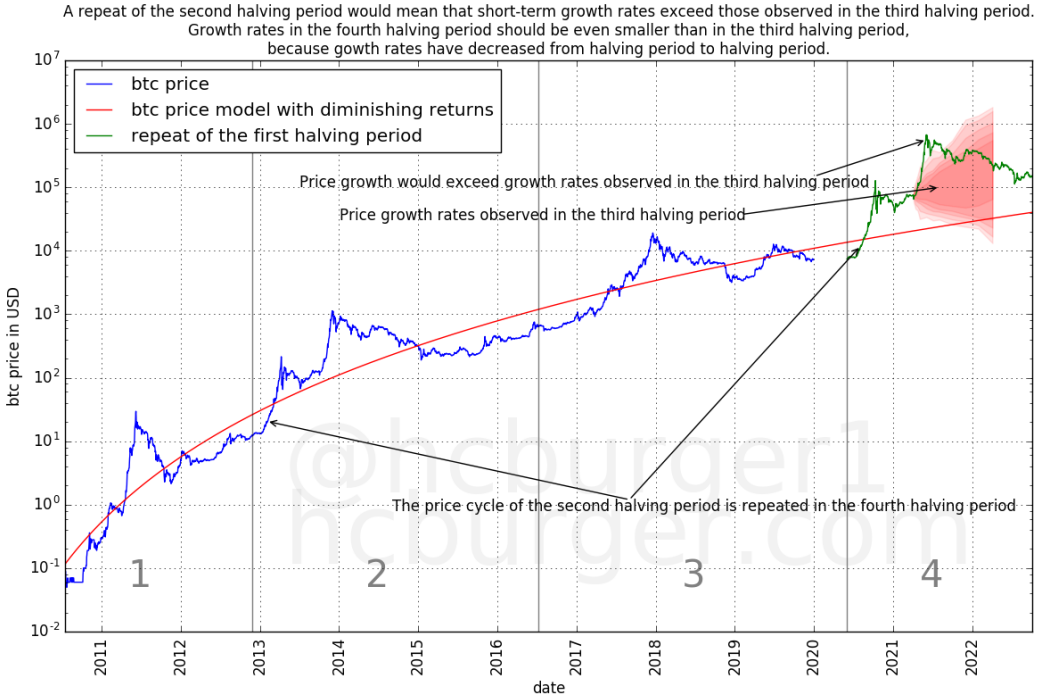
We can also ask ourselves if it is possible for history to repeat itself. E.g. could the price movements observed in the first halving period repeat themselves after the next halving?

For that to be possible, the hypothetical price movements should at least agree with the statistics observed in the third halving period. In fact, we expect the statistics of the price movements in the fourth halving period to be even more tame than those observed in the third period. However, we have not observed any statistics for the fourth having period, so we're going to work with statistics from the third halving period for now.



The above plot shows a repeat of the first halving period after the third halving. We see that price movements are too extreme and lie outside the range observed in the third halving period. We should therefore consider a scenario with such strong short-term price fluctuations as unlikely.

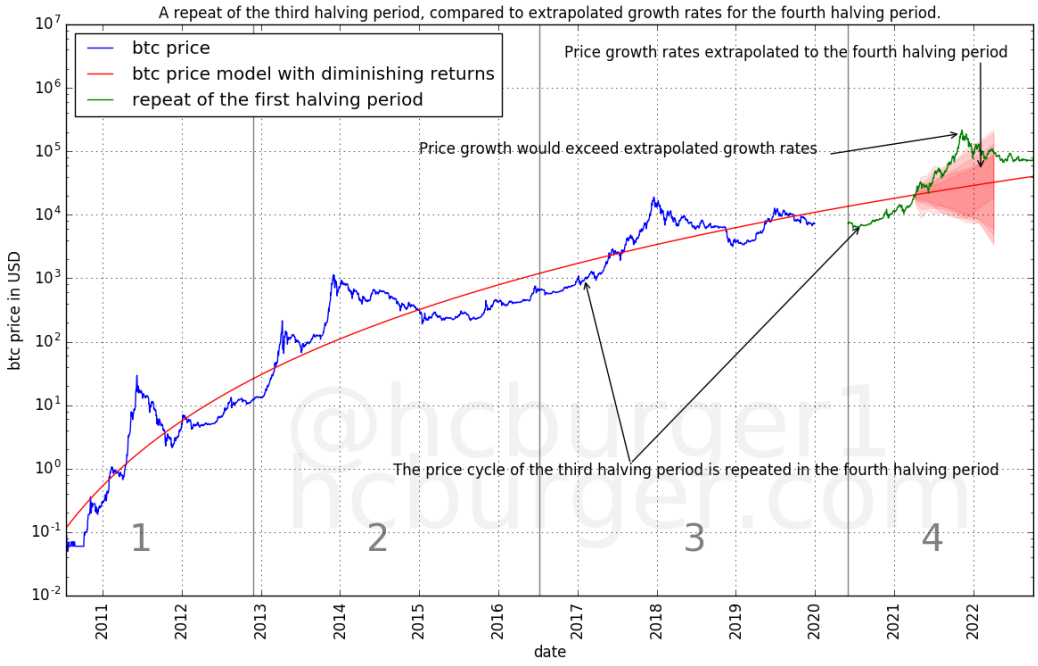
What about a repeat of the second halving cycle? The same conclusion holds: the short-term price fluctuations seem to be too strong.



Would a repeat of the third halving cycle be possible? The below plot shows that the price movements are (obviously) in agreement with the statistics observed in the third halving period.

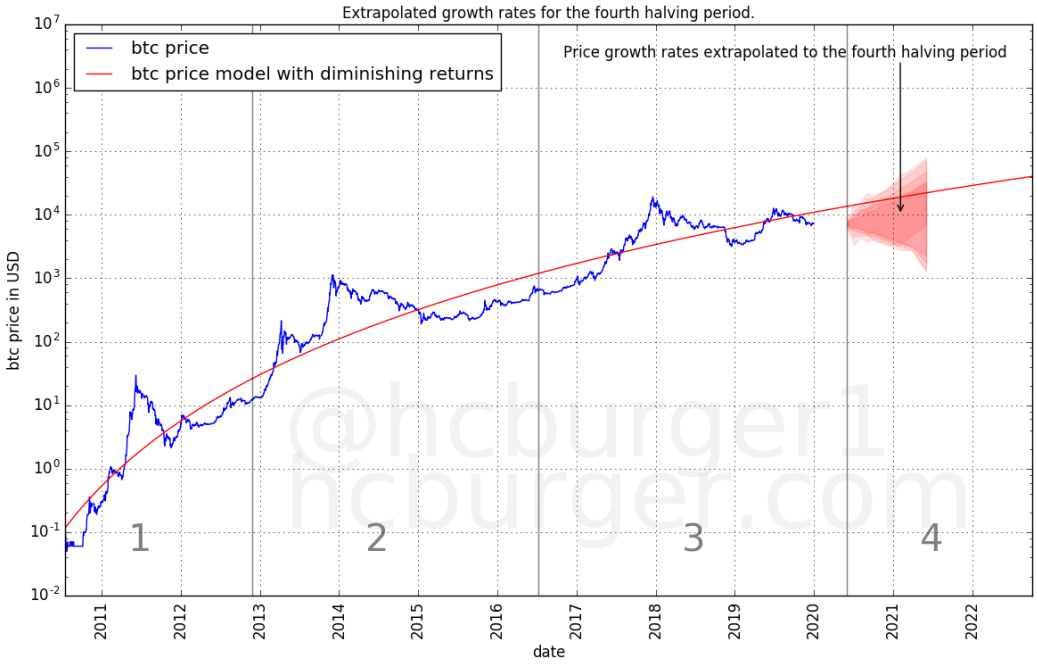
However, short-term price movement statistics should be tamer in the fourth halving period than in the third, for the same reason as statistics in the third period are tamer than in the second period.

We will use a simple method to obtain extrapolated statistics for the fourth halving period, and compare the price movements of the third halving period to those statistics. The extrapolation method works as follows. For a given statistic, it computes the reduction factors from: 1) the first halving period to the second halving period and 2) the second to the third halving period. This average factor is then used to extrapolate the statistic from the third halving period to the fourth.



Using this extrapolation method, the price movements of the third halving period would be too extreme.

Assuming 0 price growth until the third halving, and using extrapolated statistics for the fourth halving period, we get the following possible price movements.

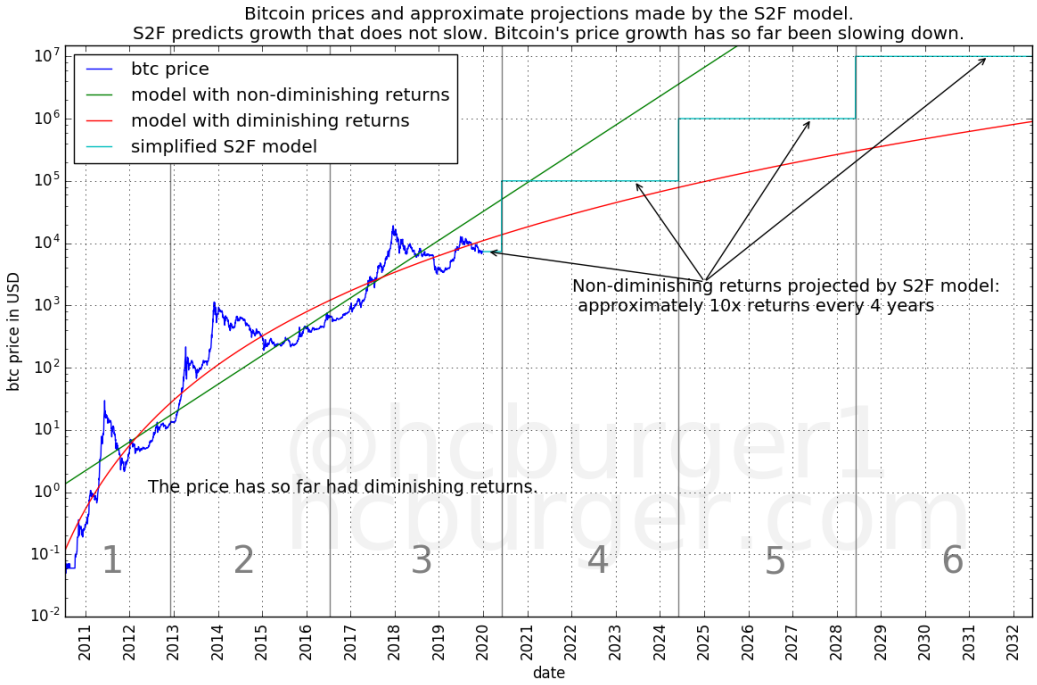


Stock-to-Flow model

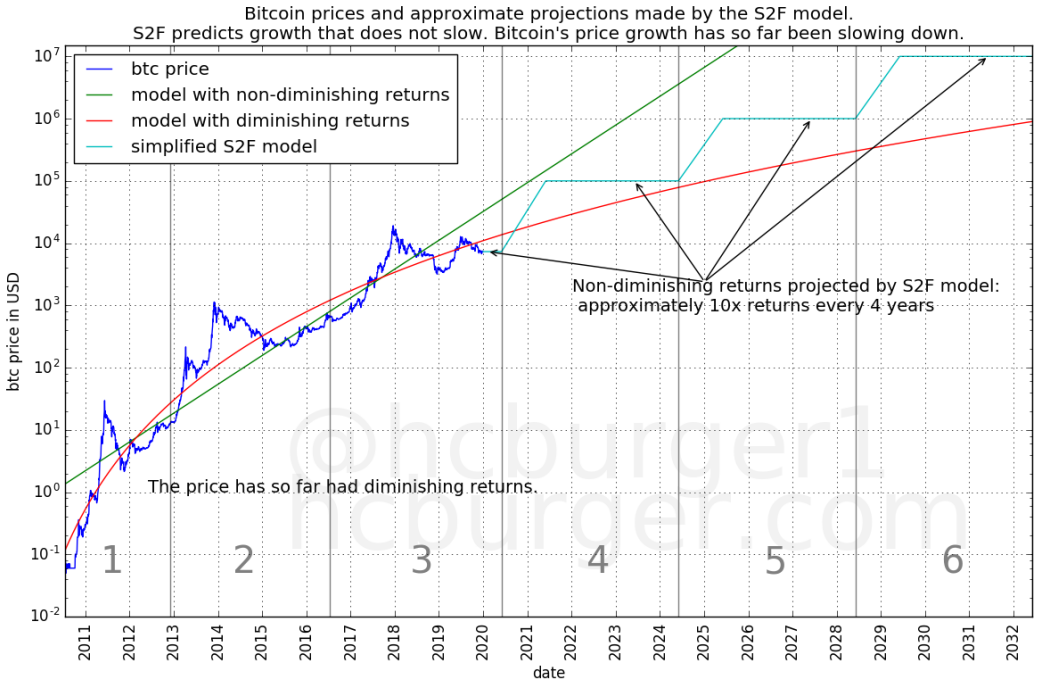
A model proposed by planB called the stock-to-flow model (S2F for short) models the price of bitcoin using its scarcity, defined as the newly created stock divided by the already existing stock. Price predictions made by this model predict prices in the $100k range for the next halving period, with prices increasing approximately by a factor of 10 for each subsequent halving period:

![](/assets/images/2020/m1/h30.png *source: 100trillionUSD*

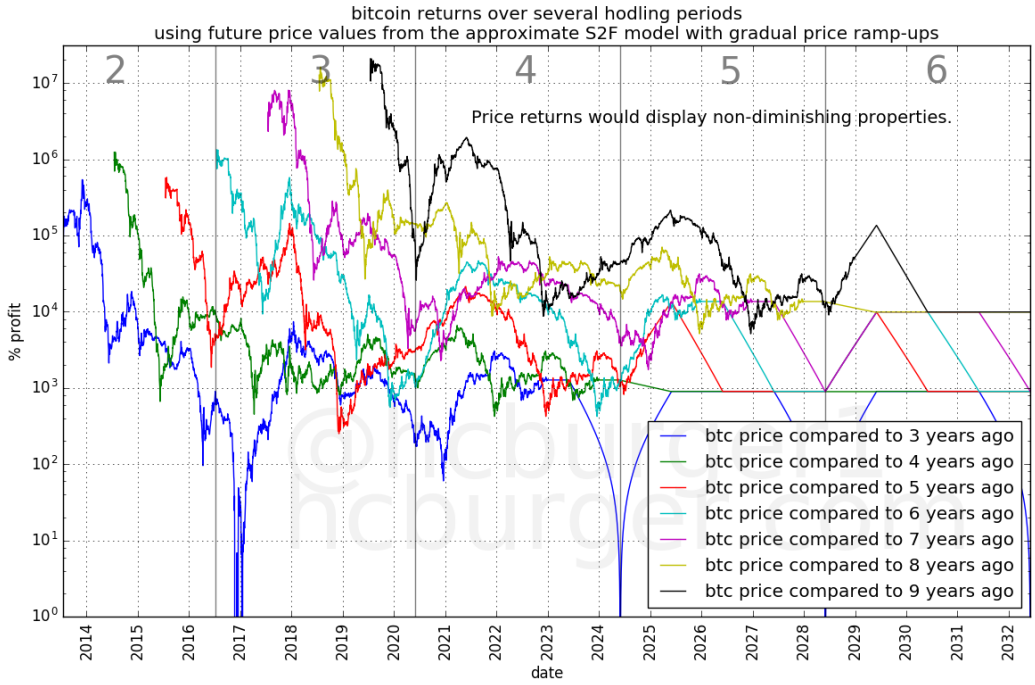
A model which has a constant growth factor (here: 10) for a given period of time (here: 4 years), is a model with non-diminishing returns. Such a model therefore makes claims about the future that are opposed to the observations of long-term diminishing returns we have made in this article, and the expectation expressed in this article that the trend of diminishing returns should continue.



In the short-term, we should not expect the price to move in a step-wise function as displayed by the cyan line (nor does the S2F model claim that the price should evolve in such an abrupt manner). As an experiment, let us consider the following smoother hypothetical future price curve:

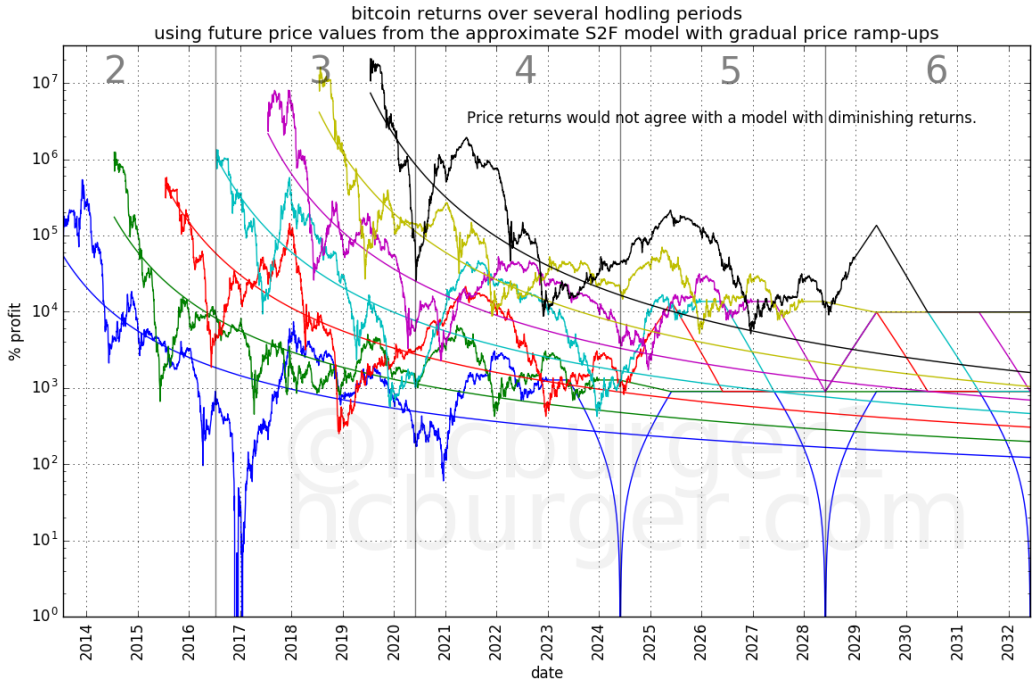


Looking at the return curves that such a price curve would generate, we see that returns at the beginning of the future halving periods (4, 5, and 6) tend to ***increase***. Increasing returns can happen, due to volatility in the price, but should not be expected to happen systematically. We also see that returns for e.g. the three- and four-year hodling periods are more or less flat, at 1000%, reflecting the 10x price increase between halving periods predicted by the S2F model.



Overlaying the return curves generated by the model with diminishing returns shows these disagreements more clearly:

- The S2F model has return curves that are partially ***increasing***, which is not expected in the model with diminishing returns
- The S2F model has return curves that are mostly flat for shorter hodling periods, which indicates non-diminishing returns, whereas in this article we have observed historically diminishing returns.

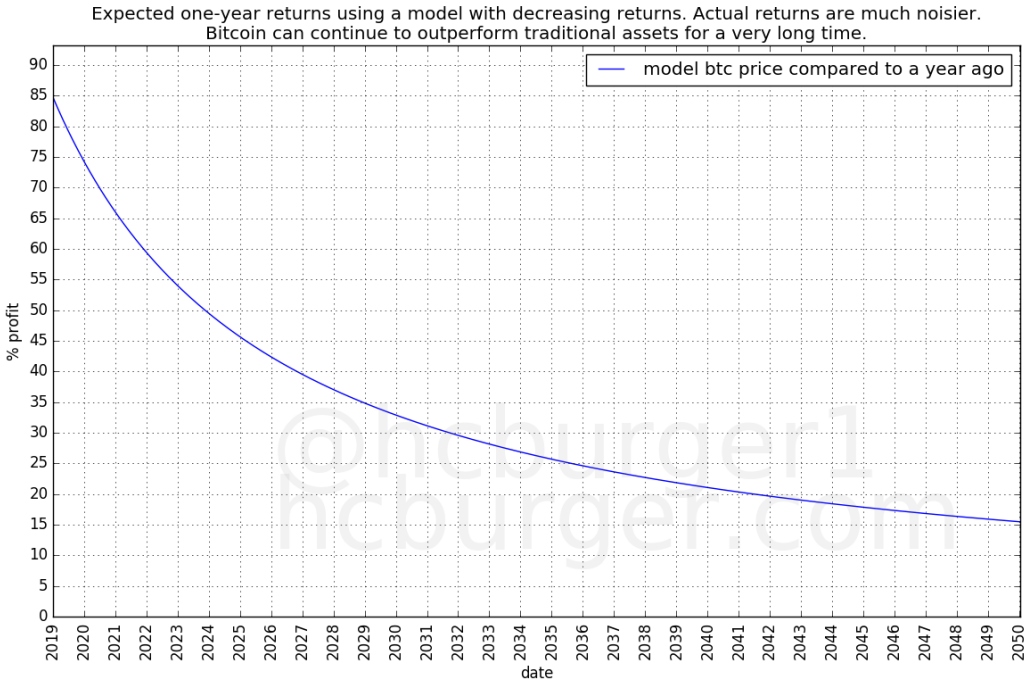


This is not a statement that the S2F model is incorrect, but it does show that for the S2F model to hold as currently formulated, return curves need to change compared to how they have behaved up to now: they need to transition from being diminishing to being non-diminishing.

Also, it is not quite correct to say that the S2F model has non-diminishing returns: In the early history, returns as modeled by the S2F model are indeed diminishing. The returns only diminish up to a certain point, though (approximately a 10x return every 4 years).

The future is still bright

Even though diminishing returns lead to predictions that are less optimistic than predictions based on non-diminishing returns, bitcoin can still have very strong growth for many years to come, and continue to outperform most traditional assets.



Discussion

What this article does not state

This article has made no numerical predictions. No predictions are made regarding the rate of decrease of the long-term price growth rate. Also, no prediction has been made regarding how much volatility is expected to decrease in the future. No statement has been made regarding whether both should tend toward 0 or not.

Potential counter-arguments

Bitcoin's price growth has at various times been described as being either:

- constant,
- accelerating, or
- resembling an S-curve.

We see no empirical evidence for any of the above. Bitcoin's price growth has been diminishing from the start.

Why would this property not hold anymore? One might argue that past performance is not an indication of future performance, and therefore that the fact that bitcoin's returns have so far been diminishing does not mean

that they will continue to be diminishing in the future. In other words: bitcoin's returns could become non-diminishing in the future. As arguments against this statement we can say that:

- We have so far seen no sign that bitcoin is starting to show non-diminishing returns.
- A new, as of yet unknown, mechanism would need to take hold in order to counteract the fact that it becomes ever more difficult to attract ever more capital.

Reasons for slowing growth

We have stated that an increased price of bitcoin leads to more capital being required for even more price increases. We took a shortcut in that explanation: What matters is not only the price, but also the number of bitcoins traded. If few bitcoins are traded, other things being equal, the price of these bitcoins is easier to change than if many bitcoins are traded. One could therefore say that the depth of orderbooks (in fiat terms) really matters, rather than the price itself. So far, orderbook depth has increased along with price.

An alternative way of looking at diminishing returns is the following. The price of bitcoin depends on supply and demand, like anything else. The supply is driven by the willingness of hodlers to part with their bitcoin for a given price. Initial investors were unwilling to part with their bitcoin for anything less than very high returns. These initial sky-high returns attracted more investors, some of which are willing to part with their bitcoins for lower returns ("good enough" returns).

Mathematically, bitcoin's price growth does not display memorylessness. Memoryless growth would mean that price growth does not depend on its price, which would mean non-diminishing growth. Memoryless/non-diminishing growth would be very surprising, as it would mean that bitcoin's price has no effect at all on its expected growth rate. We should therefore not expect non-diminishing returns in bitcoin's price growth, nor do we observe it empirically.

It is also not clear if higher price / deeper orderbooks is the only factor reducing price volatility in the short term. Another reason for reduced volatility might simply be time itself: as time goes by, traders find more and more profitably exploitable patterns. Exploiting these patterns leads to reduced volatility. Yet another reason might be the number of bitcoin traders. The more traders attempt to exploit patterns, the more stable the price is expected to be.

Conclusion

Bitcoin's price has faced increasing resistance when moving upwards, leading to diminishing returns. Long-term, the price has grown slower and slower. Short-term, volatility has decreased, and bull markets have taken longer to develop and pop. These observations agree with the logic that as the price of bitcoin increases, price movements require ever more capital. For this reason, these two trends are expected to continue in the future. If these trends continue into the future, it will invalidate predictions and models that are based on expectations of non-diminishing returns, which will prove to be too optimistic.

Disclaimer: This article is not financial advice.

Related work / Prior art

I am deeply grateful, and also apologetic, to dave the wave, for pointing out to me that he observed both long- and short- term diminishing growth patterns in bitcoin for more than a year.

In a first article, Dave noted:

"As Bitcoin becomes more liquid, it becomes less volatile. Given the principle of the growth curve, this increasing price stability should incrementally come into fruition, with subsequent cycles, as the real volatility of those cycles diminish. These subsequent cycles also see the law of diminishing returns coming into effect though at this relatively early stage of the curve, future returns are projected to remain on quite a different scale to that of traditional asset classes."

In a later article, Dave noted:

"And this is something you'd expect in a maturing, more liquid market — the general principle being that with more liquidity, comes less volatility. Also predictable, on the basis of the log growth curve model, is a longer base than previously — not only is volatility in the medium term reducing [hence a less volatile base], but so too is volatility reducing on the over-all long-term macro chart of Bitcoin."

The similarities in the conclusions in Dave's and this article are striking.

Acknowledgements

This article was inspired by two independent discussions I had. Once with BitcoinEcon, who was pondering whether future bull markets might

span longer timeframes than previous ones. This discussion led me to the idea of inspecting short-term growth rates in the various halving cycles. The other with InTheLoop, in which we were discussing how much faith one can really put into any predictive model. This led me to the idea of seeing how far we can go without any model.

Thanks IntheLoop and BitcoinEcon for the great discussions!

Follow me on Twitter

Slice The Pie

By 6102

Posted January 1, 2020

What even is orange pie? This dumb tweet inspired this short article...

“The carpenter can’t run out of inches The stadium can’t run out of points The airline can’t run out of FF miles And the USA can’t run out of dollar”
- Stephanie Kelton

Understanding

There is a common belief that the USA can just print as much money as it wants. Ignoring the complex nature in which money is actually created (debt, treasury notes etc) this is true, the USA can print as many dollars as it likes.

Misunderstanding

This is completely misunderstood by many to mean that the USA can buy anything it likes. This is categorically false. This misunderstanding comes from the fact that an individual acquiring more dollars sees his buying power increase, because those dollars come from his peers, and thus their loss is his gain. He does not increase the supply of dollars, he increases his holding of dollars. In contrast, when a country prints more dollars it is simply increasing the supply of dollars. This does nothing to increase the buying power of the country. As a result of this misunderstanding, many people mistakenly believe that the USA can’t default on its debts.

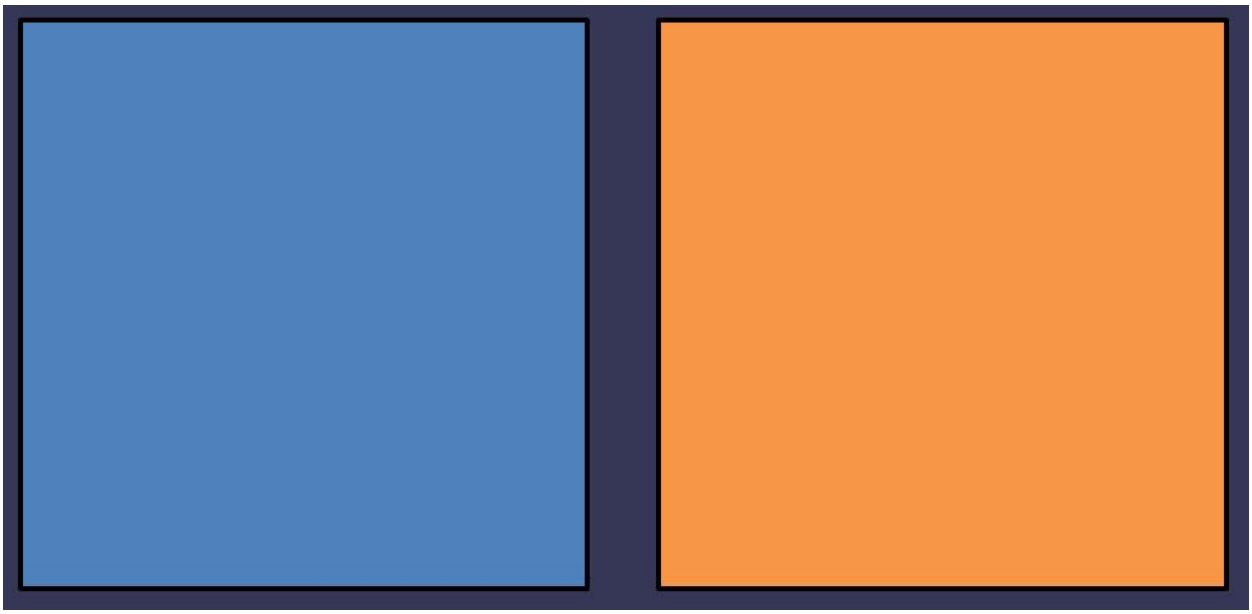
“This is the United States Government ... you never have to default because you print the money. “ - Trump

“The United States can pay any debt it has because we can always print more money to do that so there is zero probability of default.” - Greenspan

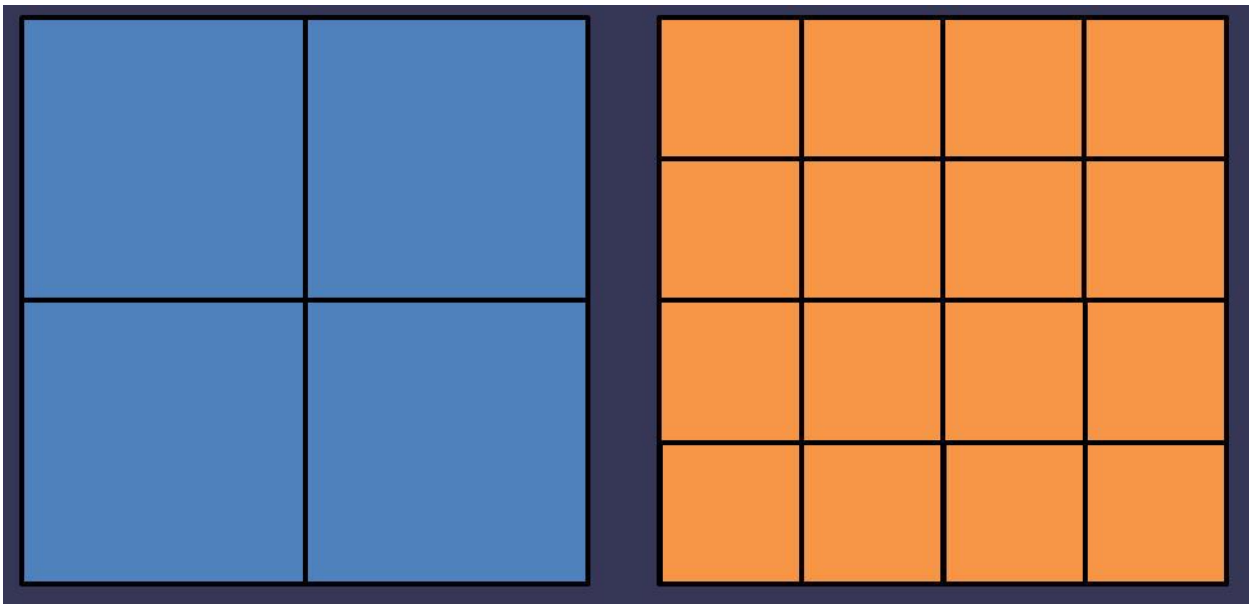
Why doesn’t printing money help?

. Like any useful measuring tool it should be reliable, if all else is constant then measuring the same thing twice should yield the same result twice. Increasing the money supply effectively distorts the measuring tool. If you double the money supply then you will simply half the value of each unit of money.

Consider two pies, Blue(berry) Pie Orange Pie (wtf)

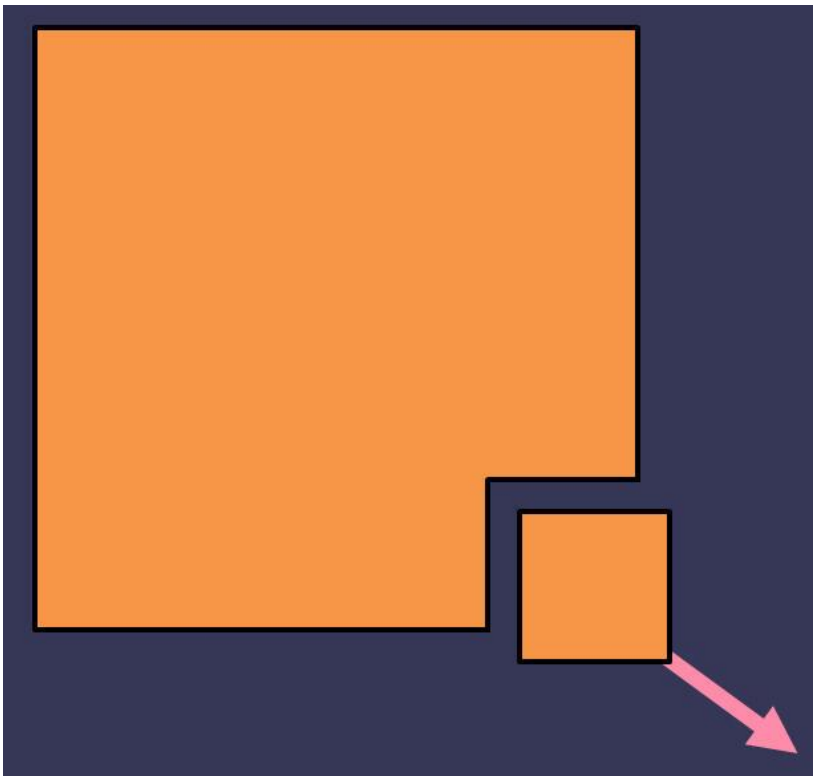


Blue(berry) pie is split into 4 equal slices, while Orange pie is split into 16.

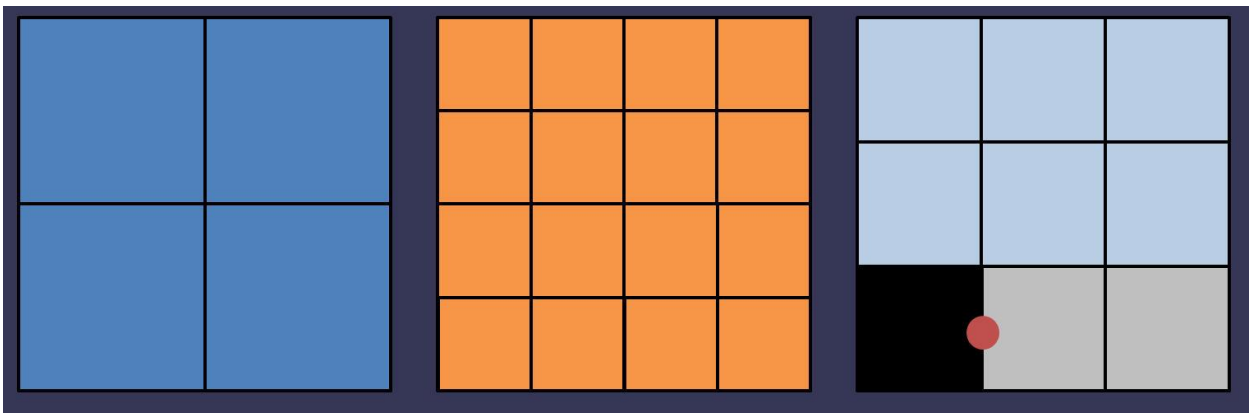


Assuming that both pies are equally delicious (this is unlikely, apologies to any orange pie lovers) what is the relative value of a slice of blueberry pie to a slice of orange pie? 4:1 (A slice of blueberry pie is equivalent to 4 slices of orange pie) Money is equivalent to the number of slices of the pie. You can slice the pie into more pieces, but the value of each slice will be worth less. To

complicate matters, governments have a tendency to continue slicing the pie while you are holding it! They call it ‘inflation’.



Remember, Money is a tool used to measure value. Like any good measuring tool it should be reliable, if all else is constant measuring the same thing twice should yield the same result twice. Inflation breaks the reliability of money. A dollar 50 years ago would get you a whole lot more than a dollar today. That is because the value of the dollar has decreased, and it has done so due to inflation (printing more money). Consider the policy of those who slice the pie you hold pieces of.



An Introduction to the Efficient Market Hypothesis for Bitcoiners

What the EMH does and does not say

By Nic Carter

Posted January 4, 2020

Curbstone brokerage on Broad Street in Manhattan, 1902 (Public domain image from the United States Library of Congress)

As we approach the Bitcoin halving due in May 2020, a heated debate has raged among Bitcoiners about whether the issuance change is being anticipated by the market or not. Those who downplay the purported impact of the issuance change tend to make references to market efficiency. This concept has thus become a source of great rancor and debate. The disagreements are often intractable, as strawman versions of the EMH are presented, and the parties cannot converge on shared definitions. Mutually understood concepts are a prerequisite to a useful debate. Since the concept is widely misunderstood, I thought I'd explain it from scratch, assuming little prior financial knowledge.

Origins of the EMH

The efficient market hypothesis has been attributed to several thinkers, among them Benoit Mandlebröt, Louis Bachelier, Friedrich Hayek, and Paul Samuelson. Hayek's *The Use of Knowledge in Society* is useful background reading for the concept, although it never makes reference to the EMH specifically. His seminal essay argues in favor of distributed, market-based economies, in contrast to centrally planned ones. The key insight: markets are information-aggregation mechanisms that no central planner, no matter

how skilled or well-resourced, can match. Consider the following passage (emphasis my own):

[T]here is beyond question a body of very important but unorganized knowledge which cannot possibly be called scientific in the sense of knowledge of general rules: the knowledge of the particular circumstances of time and place. It is with respect to this that practically every individual has some advantage over all others because he possesses unique information of which beneficial use might be made, but of which use can be made only if the decisions depending on it are left to him or are made with his active coöperation.

[...] And the shipper who earns his living from using otherwise empty or half-filled journeys of tramp-steamers, or the estate agent whose whole knowledge is almost exclusively one of temporary opportunities, or **the arbitrageur who gains from local differences of commodity prices, are all performing eminently useful functions based on special knowledge of circumstances of the fleeting moment not known to others.**

In the bolded section you can begin to see how Hayek views markets: as forces that aggregate a multitude of different views and expectations into prices. Hayek understands market-derived prices as information — a particularly high signal source of information at that. The beauty of markets, to Hayek, is that simply by selfishly acting according to their own interests, individuals participating in the economy create signals in the form of prices. The EMH orients this perspective specifically towards financial assets, holding that investors collectively surface relevant information which is incorporated into prices through the mechanism of trades.

Following a series of studies about stock returns like Samuelson's 1965 ***Proof that Properly Anticipated Prices Fluctuate Randomly***, the EMH was finally codified for good in 1970 by legendary finance academic Eugene Fama (you may have heard of the Fama-French model). In a paper entitled ***Efficient Capital Markets: A Review of Theory and Empirical Work,*** Fama defines an efficient market as "a market in which prices always "fully reflect" available information." If you were stop reading here, you'd already have a better understanding of what is meant by efficient markets than the caricatures presented on Twitter. The EMH is not a mystical claim. It's simply the view that market prices reflect available information. This is why academics often refer to them as 'informationally' efficient markets. The efficiency refers to information proliferation.

What does this actually mean? It simply means that if there is new information which is relevant to the asset being traded, this information tends to be incorporated into the price of that asset with rapidity. And if there

are future events which you might reasonably imagine would affect price, they tend to be incorporated into the price ***when known***. Markets don't wait for (knowable) events to happen — they anticipate them. This means, if a weather forecast predicts that a hurricane will emerge and wipe out sugarcane plantations next week, speculators will bid up the price of sugar ***today,*** anticipating the supply shock. Now, of course, when there are unpredictable exogenous shocks (imagine that the hurricane materialized with no warning), then price can only react in real time, as the information becomes known. The speed of information incorporation is one of the tests of efficiency.

While the EMH is a simple idea, it tells us a great deal about how markets operate. Markets are efficient if prices rapidly incorporate new information. Forecastable, market-moving events taking place in the future tend to be incorporated in price beforehand. Importantly, one consequence of the EMH is that, once all relevant information is incorporated into price, you are left with only random fluctuations, called 'noise'. What this means is that while asset prices will still jitter about, even in the presence of no new fundamental information, these fluctuations contain no information of their own.

And lastly, the difficulty of surfacing unique new information (not already included in price) tends to vary with the sophistication of market participants and the liquidity of the asset. This explains why you might be able to find an edge in an obscure micro cap stock, but probably not in predicting the price of Apple.

Since Fama's paper, and thanks to popular books on the topic like Burton Malkiel's ***A Random Walk Down Wall Street,*** a heated debate has raged over whether active management is worth it. Indeed, since efficient markets posit that consistent edges are very difficult to find, many investors have come to question whether actively traded vehicles like hedge and mutual funds make sense. In the last decade, trillions of dollars have flowed out of such 'active,' stock-picking strategies, and into passive vehicles, which simply seek to track the performance of the entire market, or a specific sector. This is one of the most critical debates happening in finance right now, and it's mostly due to the growing realization that markets are, indeed, generally efficient.

The EMH described

I take slight exception to the 'hypothesis' component of the EMH. If it were up to me, I'd call it the efficient markets ***model,*** not hypothesis. This is because it doesn't really contain a hypothesis. It doesn't really make a specific testable claim about the world. As stated, the EMH posits that **market prices reflect available information** (which, as we have noted, is the purpose of markets in

the first place). Interestingly, Fama in his 1970 paper calls it the efficient market model, not hypothesis. It seems he has the same intuition.

I would also go as far as to consider EMH somewhat tautological. Recalling Hayek, we know that (free) markets measure society's net informational stance over various assets. So if we replace 'market prices' with 'concentrated information outputs' in the EMH construction bolded above, we get the following:

Concentrated information outputs reflect available information

That certainly sounds tautological. But that doesn't make the model any less useful_._ Conversely, it means that contesting the EMH is to question the nature of markets themselves. And indeed, most critiques of the EMH (I will cover a few later in this piece) generally cover instances where markets are not clearing, for some reason or other. So if you accept that EMH is tautological, 'efficient markets' also starts to sound redundant. Indeed, the default state of (free) markets is to be efficient, because this is why we have markets. Markets compensate anyone for finding relevant information. If they weren't default-efficient, then we wouldn't bother with them.

Referring to it as a model makes it very clear that it's just an abstraction of the world, a description of the way markets should (and generally do) work, but by no means an iron law. It's just a useful way to think about markets.

Let me be clear! I do not believe in the "strong form" of the EMH. No finance professional I know does. It is generally a straw man. The strong form holds that markets reflect **all** information, all the time. If this were true, no hedge funds or active managers would exist. No one would bother poring over Apple's quarterly reports, or evaluating the prospects for oil discovery in the Permian basin. Clearly, given that we have a large active asset management industry, in which lots of very bright individuals constantly seek to surface new information about various assets, the strong form doesn't hold.

Truthfully, the EMH is not something you 'believe in,' or not. The choice is to understand markets as useful information-discovery mechanisms, or reject the usefulness of markets altogether.

There are of course conditions which lead to market inefficiency. Fama acknowledges as much in his 1970 paper, calling out transaction costs, the costs of acquiring relevant information, and disagreement among investors as potential impairments to market efficiency. I'll discuss two here: the costs of surfacing material information, and frictions inherent in actually expressing market views.

If the EMH generally holds, how are funds compensated for finding information?

So what explains the fact that there is a large (albeit shrinking) industry involved in active investing, despite the fact that markets are generally efficient? If market-relevant information is generally encoded in prices, then there is no profit from finding new information and trading against it. But clearly, many individuals and firms do actively attempt to surface new information. This presents a bit of a paradox.

This brings us to another one of my favorite papers, ***On the Impossibility of Efficient Markets***, by Grossman and Stiglitz. The authors point out that gathering information is costly, not free. They then note that since EMH posits that all information is immediately expressed in prices, there would be no compensation from incurring costs to surface new information under that model. Thus markets cannot be perfectly efficient: information asymmetries must exist, as there must be a way to compensate informed traders. Their model introduces the useful variable of information cost into the standard model of market efficiency. It follows from their model that if information becomes more costly, markets become less efficient, and vice versa. So whether or not markets reflect their fundamentals is at least partially a function of the difficulty of surfacing that relevant information.

The authors conclude:

We have argued that because information is costly, prices cannot perfectly reflect the information which is available, since if it did, those who spent resources to obtain it would receive no compensation. There is a fundamental conflict between the efficiency with which markets spread information and the incentives to acquire information.

A rather delightful implication of Grossman and Stiglitz is that, to render arbitraging prices back to where they 'should' be a profitable activity, there has to be a cohort of traders who are perennially knocking prices out of whack. Fischer Black (he of the Black Scholes formula) gives us an answer, with a lovely paper pithily entitled ***Noise*** in the Journal of Finance. He identifies unsophisticated 'noise' traders: those who trade on noise, rather than information. Noise can be found anywhere. Just mosey on to Tradingview and see the plethora of indicators that people swear by. Black divides market players into two cohorts:

People who trade on noise are willing to trade even though from an objective point of view they would be better off not trading. Perhaps they think the noise they are trading on is information. Or perhaps they just like to trade.

With a lot of noise traders in the market, it now pays for those with information to trade. Most of the time, the noise traders as a group will lose money by trading, while information traders as a group will make money.

Noise, in Black's view, "makes financial markets possible." The existence of noise traders gives professional firms like hedge funds liquidity, and valuable counterparts to trade against. In the poker analogy, noise traders are the fish. They make the game profitable for the sharks, even in the presence of a rake. Ask any former online poker player — as the scene became more competitive, and unsophisticated players left, it stopped being as profitable to play.

The noise theory resolves the 'apparent impossibility' of efficient markets as pointed out by Grossman and Stiglitz. The existence of noise as introduced by unsophisticated traders gives sophisticated traders a considerable financial incentive to introduce information into prices. So you can thank the degens overtrading on Bitmex — they are the ones compensating funds for allocating resources to Bitcoin and surfacing relevant information quickly.

If the EMH generally holds, how do you explain instances where markets do not clear?

This is another good question. There are copious examples of situations where arbitrage opportunities were easy to identify, yet where the arbitrage could not be closed for some reason. The most famous of these examples is arguably the trade which caused the demise of Long Term Capital Management. It was a pair trade on bonds which were effectively identical but were differently priced (partially due to the Russian default in 1998). LTCM was betting that the prices of the bonds would converge. However, many other hedge funds had made that same bet with leverage, and as the bonds failed to converge in a timely manner, LPs in some of the hedge funds redeemed, the funds faced margin calls, and were thus forced to liquidate this positions. This kicked off a feedback loop causing additional squeezes: the cheaper bonds were sold off, and the pricier instruments kept rallying as shorts were covered. LTCM was betting on market efficiency and the convergence of these instruments; but because of market stress and the winding down of pent-up leverage, they weren't able to complete the trade, and the fund blew up.

This phenomenon is examined in a 1997 paper from Shleifer and Vishny entitled ***The Limits of Arbitrage***. Shleifer and Vishny point out that arbitrage is not normally done by the market, generically, but rather is a task delegated to specialized institutions (funds, typically). As such, arbitrage is costly: requiring freely available capital. There's a paradox: great arbitrage

opportunities come about when the market is under stress (this is when you get many stocks trading at a low price-to-book, for instance). But during times of market stress, capital is ***least available.*** Thus the arbitrageurs, who require capital to operate, are worst equipped to perform the required arbitrage when they are most needed. These are the limits of arbitrage. As the authors state:

When arbitrage requires capital, arbitrageurs can become most constrained when they have the best opportunities, i.e., when the mispricing they have bet against gets even worse. Moreover, the fear of this scenario would make them more cautious when they put on their initial trades, and hence less effective in bringing about market efficiency.

Take the simple example of a value-based hedge fund which has raised outside capital. They will tell LPs (investors in the hedge fund) of their intention to pursue contrarian bets — buying value stocks when they are cheap, for instance. Let's say the market declines and they buy a basket of stocks whose valuations have contracted and have low P/E ratios. However, imagine that the market subsequently declines another 40%. Their LPs are now staring at a loss and ask to redeem. This is the worst possible time: the fund has to sell the stocks at a loss, even if they have a high conviction on making money on them in the long term. They would much rather be buying the (now very discounted) stocks, whose valuations are even more attractive. To make things worse, liquidating those positions forces them down further, punishing other funds making the same trade.

Shleifer and Vishny therefore find that:

[P]erformance-based arbitrage is particularly ineffective in extreme circumstances, where prices are significantly out of line and arbitrageurs are fully invested. In these circumstances, arbitrageurs might bail out of the market when their participation is most needed.

The limits to arbitrage caveat about EMH actually explains a lot of situations where people will describe market conditions and lament that information is not being incorporated. This is often taken as a slight against the EMH. But of course we cannot expect malfunctioning markets to operate properly. So when Dentacoin's multi-billion dollar putative market cap is touted as an example of market efficiency not holding, consider that it likely had a minuscule float, ownership was extremely concentrated, and obtaining a borrow for a short was impossible. This means that market participants cannot meaningfully express their views on the asset.

A fuller conception

Mindful of these constraints (issues of market structure, costly information, limits to arbitrage), we can devise a more complete version of the EMH which includes these caveats. You might therefore devise a modified EMH that sounds a bit like this:

Free markets reflect available information to the extent that price-setting entities are willing and mechanically able to act upon it.

- *Free markets:* because state-controlled markets may not clear (for instance, markets for currencies with capital controls do not give reliable signals, since selling is effectively constrained)
- *Price-setting entities*: because minnows don't ultimately matter most of the time. A small number of well-capitalized participants can suffice to incorporate material information into price
- *To the extent that they are willing*: this covers the 'costly information' caveat. If information is more costly to obtain than it is worth to instrumentalize (for instance, in the case of discovering accounting fraud in a micro-cap stock), then it won't be included in price
- *Mechanically able:* this covers cases where limits to arbitrage exist. If there is a liquidity crisis, or the markets are not functioning properly, for whatever reason, and funds cannot operationalize their views on the market, inefficiency may occur

So when most financial professionals talk about the EMH, they generally imply a modified, slightly caveated version like the one above. Almost never do they mean the 'strong form' of the EMH.

Interestingly, by caveating the EMH, we have stumbled on an alternative conception entirely. The model I have described here somewhat resembles Andrew Lo's ***adaptive market hypothesis.*** Indeed, while I am very happy to maintain that most (liquid) markets are efficient, most of the time, the adaptive market model far more closely captures my views on the markets than any of the generic EMH formulations. Many active managers that I know are at least familiar with Lo's work. The theory is fully developed in his book, but you can get a condensed version in his 2004 paper.

In short, Lo attempts to harmonize findings from behavioral economics finding apparent irrationality on the part of investors, with the orthodox EMH school. He calls it the adaptive market hypothesis because he relies on an evolutionary approach to markets. Taking Black's insight further, Lo divides market participants into 'species', giving us a view of market efficiency which departs from the mainstream:

Prices reflect as much information as dictated by the combination of environmental conditions and the number and nature of "species" in the economy or, to use the appropriate biological term, the ***ecology***.

Lo describes profit opportunities from information asymmetries as 'resources', leading to formulations like the following:

If multiple species (or the members of a single highly populous species) are competing for rather scarce resources within a single market, that market is likely to be highly efficient, e.g., the market for 10-Year US Treasury Notes, which reflects most relevant information very quickly indeed. If, on the other hand, a small number of species are competing for rather abundant resources in a given market, that market will be less efficient, e.g., the market for oil paintings from the Italian Renaissance.

The contextualism and pragmatism that Lo's model presents aligns it with the experience of most traders, who intuitively understand that market participants are quite heterogeneous, and understand the notion of 'table selection' (borrowed from poker). I won't dive too deep into Lo's take here, but I do recommend his book, and at the very least his paper summarizing his theory.

What this means for Bitcoin and the halving

As we have seen, most markets are efficient most of the time. This is not something markets just happen to do; this is their purpose. I have discussed a few exceptions: the limits to arbitrage situation, non-free market situations, situations where behavioral biases apply, and situations where market participants may not be sufficiently motivated to surface relevant information. The question is, do any of these conditions apply to the Bitcoin markets? Right now, this doesn't seem to be the case. We are not in a liquidity crunch. There are no apparent limits to arbitrage. In the pre-financialized era for Bitcoin (I'd say anytime before 2015), you could have convincingly made that case. There truly was no easy way for a well-capitalized entity to express as positive view on Bitcoin. But today there is.

As for free markets, Bitcoin is clearly a very free market, one of the freest on earth (since the asset itself is highly portable and easily concealable, and traded around the globe). Unlike most currencies, it is not backed or guaranteed by a sovereign, and there are no capital controls impairing selling. Participants also have the abundant ability to place large short positions on Bitcoin, so they can express a diverse set of views. So we can check the 'functioning markets box'. Now, is Bitcoin sufficiently large for there to be a significant number of sophisticated funds devoting concerted effort to surfacing material information? At a $150b market cap, I think that's

absolutely the case. The final test of market efficiency is whether or not market-moving information is incorporated into prices right away, or with a lag. An event study covering the effect of exogenous shocks like exchange hacks or sudden regulatory shifts on price would be welcome.

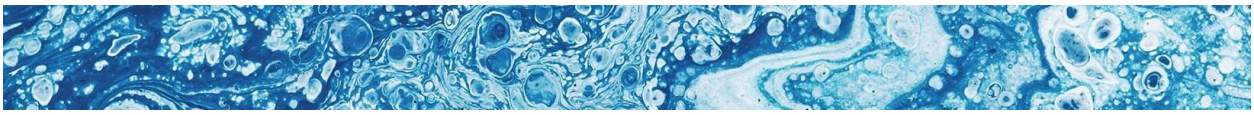
The only necessary conditions for efficiency for which Bitcoin still has question marks have to do with disagreement among market participants (i.e. the lack of a shared valuation model that price setting entities converge on), and the development of more financial plumbing. There are still a few classes of entity for which Bitcoin exposure is rather difficult to obtain. Of course, surmounting these challenges will render Bitcoin's prospects sunnier.

So is the halving "priced in" or will it be a catalyst for appreciation? If you've read this far, you will understand that I consider it patently absurd that a change in issuance would have been overlooked by the price-setting entities. Anyone with an interest in Bitcoin has been aware of the supply trajectory from inception. Supply was encoded in the very first implementation that Satoshi released to the world in January 2009. Long-scheduled changes in the rate of issuance do not constitute new information. Any presumed demand-side reactions to the 'halving catalyst' can also be anticipated by sophisticated funds who have a strong incentive to frontrun investor optimism.

Now, can Bitcoin appreciate from here onwards? Absolutely. I don't believe appreciation, if it occurs, will be due to the entirely foreseeable changes in the rate of issuance (the forthcoming halving will take us from 3.6% to 1.8% annualized issuance), but of course I feel that there are other factors which could positively affect the price, most of which are hard to predict. Is that consistent with the EMH? Very much so. EMH permits informational shocks (for instance, imagine if we suddenly had rampant inflation in a major world currency). It's also possible that the price setting entities are taking an overly conservative view of Bitcoin's future, or that they are acting on a weak fundamental model. These are consistent with weak form EMH.

I'll leave you with this parting thought. Regulated securities markets have structural barriers to efficiency in the form of prohibitions on insider trading. As Matt Levine likes to say, insider trading is a form of theft in which someone trades on information which does not belong to them. They have not discovered the information from public sources, but rather were privy to something like a merger discussion and acted on it. Since insider trading is banned, stock prices generally don't reflect pending catalysts like acquisitions until they are publicly announced. However, in a market for a virtual commodity like Bitcoin, insider standards don't typically apply. If a catastrophic bug is found, you can expect that this information might be incorporated into price right away. So in that sense, it's quite possible that the

market for Bitcoin is ***more*** informationally efficient than markets for U.S. equity are.



Common objections

I will consider some objections here. Odds are, your responses are covered.

I found an instance of inefficiency. This is evidence for the inefficiency of markets generally

This is a bit like throwing a baseball in the air and claiming that its temporary departure from the earth disproves gravity. Few or no finance practitioners believe that all markets are efficient all the time. If information is unevenly distributed, or information-owners lack the means to instrumentalize their views, then the prices may not reflect information. Short term instances in which markets do not apparently reflect information are just invitations to query why market participants were unable to price in relevant information. These failures aren't evidence of the weakness of the EMH, but rather reinforce its usefulness as an explanatory tool.

Behavioral biases exist, so market efficiency doesn't hold

A number of persistent behavioral biases have indeed been found by researchers, and I find it plausible that they systematically affect asset prices to an extent in the medium term. However the question here is whether they are relevant to the matter at hand — the putative effect of a change of the rate of supply on the price of the asset — and whether these purported biases can actually affect the price formation of a highly liquid $150b asset. You might respond: 'well Bitcoiners have a bias which causes them to bid up the price of assets with sharply decreasing issuance rates, even if this information is already known.' If you can prove, Kahneman and Tversky-style, that this is a universal human bias which affects asset pricing, and contradicts dominant market models, not only will you win the argument, but you will also likely collect a Nobel. In this situation I'd also refer you once again to Lo's adaptive markets.

Efficiency is impossible in Bitcoin because there are no fundamentals

Some people hold that sentiment drives everything in crypto markets, and that fundamentals do not exist. This is a convenient fallacy. There are obvious

fundamentals which everyone would agree matter. Here is a short, non-exhaustive list:

- the quality of financial infrastructure enabling individuals to get exposure to and hold Bitcoin. In 2010, it was virtually impossible to buy Bitcoin, and your only option for custody was the Bitcoin QT 'Satoshi Client' or a homebrewed paper wallet. Today, you can get a billion dollars of Bitcoin exposure, and you can self-custody it or rely on some of the world's largest asset managers and custodians. This is a fundamental change
- the quality of the Bitcoin software (compare the current version with Satoshi's first client). The protocol itself and the tooling surrounding it has been improved, refined, and made more useful
- the actual stability and functionality of the system — imagine a case where Bitcoin failed to produce blocks for a month. That would surely impair the price. If you concede this, you admit that there are 'fundamentals' beyond mere sentiment
- the number of individuals globally that are aware of and demand Bitcoin. This is 'adoption'. This not mere sentiment; this is a measure of which sources of capital, worldwide, are actively seeking exposure to Bitcoin

There are many other fundamentals which I won't cover here. Funds which trade Bitcoin seek to track the trajectory of these variables, and ascertain whether Bitcoin is too richly or modestly priced relative to their growth. This is "fundamental analysis".

Again, if you aren't persuaded, just think about the contrast between Bitcoin's state in 2010 and its state in 2020. It's many orders of magnitudes easier to use, acquire, buy, sell, and store. That is a change in fundamentals. Granted, these aren't 'fundamentals' of the sort that apply to stocks with cash flows, but Bitcoin isn't a stock. A unit of Bitcoin is a claim on ledger space which gives you access to the particular transactional utility of the network. I'll concede that the fundamentals aren't quite as explicit as those present in a stock. But, the notion of 'fundamentals' isn't just restricted to equity or instruments with cashflows. Global macro investors consider currencies based on macro variables or assessments of political risk. Commodity traders look at production rates and the ebb and flow of supply. There are analogies here.

All of this to say that funds have meaningful market-relevant information to trade against, not just sentiment or hype. It's just that it's hard to obtain a precise fundamental assessment of Bitcoin.

Efficiency is impossible in Bitcoin because it is volatile

It's entirely possible to have volatile and efficient markets. Recall that all efficiency requires is that available information is incorporated in price. Think about the value of a call option close to expiry, with the underlying fluctuating around the strike price. One minute the option is in the money, the next it is worthless. This would be both a volatile and efficient situation.

Alternatively, consider the value of Argentine government bonds in response to political turmoil. The fundamental here is the Argentine government's willingness to honor their debts. Efficiently functioning markets would continuously reevaluate the prospects for creditors being repaid. In a period of flux the fundamental is volatile, and so too consequently is the value of the bonds.

Bitcoin's volatility derives in part from market participants rapidly re-assessing its prospects growth, both in terms of pace and trajectory. Even small changes in future expectations of growth rates have significant effects on the implied present value. (Indeed, in DCF models for equity valuation, the outputs are very sensitive to long term growth rates.) Market participants revise their growth expectations frequently, and expectations differ (because there is no single dominant model of Bitcoin's price), giving rise to the elevated volatility (especially against the backdrop of a inelastic supply). If future expectations of growth ***are*** the fundamental, then the rapid revaluation of those expectations creates consequent volatility in price. So volatility does not disqualify efficiency.

If the EMH were true, Bitcoin would have just started life at its current valuation

This isn't how the world works. As I explained above, Bitcoin didn't start life with mature, rock solid fundamentals like it presently has. It had to grow into its valuation. In its earliest days, there was considerable uncertainty over whether it would achieve any success whatsoever. It had to actually go through all these trials and tribulations to get to where it is today. So it wouldn't have made sense for large funds to allocate to Bitcoin on day 1 (although, it clearly makes sense in hindsight), because they didn't know it would grow, and in many cases, because they structurally couldn't invest in it. Think about how you would have acquired Bitcoin in 2012, two years into its existence. You would have had to use something like Charlie Shrem's BitInstant, or the (already insolvent) Mt Gox, which we know now was run shambolically. You could have mined Bitcoin, but this was a difficult and deeply technical task.

This returns us to the "limits to arbitrage" point. Many investors that ***wanted*** to buy Bitcoin from 2009 through to present day simply couldn't, due to regulatory reasons, operational risks, and a lack of functional market infrastructure. Even if they did believe that Bitcoin would be worth north of $100b at some point, they wouldn't have had the ability to instrumentalize that view. Moreover, investors didn't start out with rock solid conviction. They needed to see Bitcoin work, successfully, in the wild, without being shut down, before choosing to store wealth in it. If you believe that Bitcoin's continued success represents new information being brought to market, then you understand that the EMH does not require it emerging from the womb, fully formed, at an initial >$100b valuation.

Something which is influenced by ponzi-related buying like Plustoken cannot be efficient

I'd agree that investors in Plustoken buying (and then selling) about 200,000 BTC was a major driver of price action in 2019. However, this doesn't impair efficiency. If it had been known in the West that Plustoken had all those coins, and were just about to sell them off, and the price of Bitcoin did not move, then I agree — there would have been questions about efficiency. However, it wasn't until much later, after much of the coins had been sold off, that information percolated through the West about the Plustoken BTC. Remember, efficiency doesn't require that prices ***never move***; rather, it suggests that prices move on new information.

Small cap assets pump on by hundreds of percent on dubious news. This is evidence of market inefficiency and disproves the EMH

Again, local, or temporal evidence of perceived irrationality does not invalidate the EMH. You either believe markets are good information clearing mechanisms or you do not. Granted, many of these small cap altcoin markets are very poor, from a structural perspective. These assets may trade on unregulated or illiquid exchanges. This means the prices you see do not necessarily reflect reality. Thus temporary pumps and dumps in illiquid assets don't prove much in either direction, aside from the poverty of the market environment in which they trade.

Generally speaking, most adherents to the EMH will concede that efficiency varies positively with the size of the asset and the sophistication of the participants. It will be very hard to find an edge in large, publicly traded stocks. Odds are, if you find some market-relevant information about Apple or Microsoft, someone else will have found it as well. But in smaller, less liquid asset classes, the returns from surfacing relevant information are far less, so there are less analysts actively inserting information into assets, meaning that

opportunities may well exist. This is because large, multibillion dollar funds simply cannot operationalize strategies trading in microcap assets.

This is simply to say that there are scale effects with efficiency. Bitcoin is not a microcap; it's a globally traded traded asset worth over $100b. This ensures that there are high returns from surfacing relevant information and expressing it in the form of trades. Thus there is a significant disanalogy between the inefficient microcap altcoins (where returns from finding information are low, and markets are weak), and a mature asset with lots of analysts looking for an edge.

When small cap cryptoassets get 51% attacked or suffer bad news, they don't decline. This demonstrates that crypto markets are not efficient

I'll defer to Lo here (seriously — read Adaptive Markets!). The adaptive explanation would be that small cap assets are generally held by hardcore believers, or better yet, closely held by confederates of the founding team. In those conditions, cartel-like behavior can easily emerge. You have likely seen these conversations on Reddit and Telegram: coin owners urging each other not to sell, especially not in the presence of bad news, since the crypto community is briefly paying attention to the project. Renewed buying in the face of bad news is a way that issuers seek to blunt the effect of a negative catalyst. This only works in small markets were ownership is not widely distributed, though.

Also, it's worth considering that virtually no one holds these assets because they like the underlying technology or find that particular flavor of code ripped off from Bitcoin Core or Ethereum that interesting. Small cap cryptoassets are held in expectation of a possible future pumps. Thus, impairments relating to the actual protocol itself are not the ***fundamental***. The fundamental is the issuing team's willingness to procure "adoption," or at the very least, feign adoption by securing favorable press releases and partnerships. As long as the underlying protocol doesn't totally dissolve, the 'fundamental' — the ability of the issuing team to create hype — can remain intact.

Since some bitcoiners mechanically buy Bitcoin on a regular basis (think: tithing) and less new supply will exist, this will mechanically cause appreciation

This is an example of first order thinking. The EMH lives on the second order. The key insight of the EMH, to me, is that any information you have, a sophisticated market participant also has. Since sophisticated market participants are strongly incentivized to find relevant information and trade

against it, you can bet that they will have expressed that information the moment they acquired it. If this were indeed a plausible hypothesis (that static buying pressure would have a positive effect on price as issuance is cut in half), then these funds have already expressed this positive view in the form of a trade. This is what is meant by "priced in." If something material is discovered to be due to happen tomorrow, it will be incorporated into price today. This is one of the most tricky features of the EMH, and it genuinely takes a bit of effort to get your head around it.

The question then becomes, not "is this information which, in a vacuum, would move the price?" but rather "**do I have information which the smartest and best-resourced hedge fund analyst does not have?**" If the answer is "no," you can expect that this information is presently incorporated into price (to the extent that it is actually material information).

Why the focus on funds? The reason is that they are specialized firms which aggressively seek out information and express it in the form of trades. They are the entities which keep price in line with the "fundamental." You need to recall that you are not operating in isolation. You are operating in the digital equivalent of a jungle with predators lurking around every corner. These predators are skilled, fast, and well resourced.

In equity markets, we're talking about funds that have personal relationships with CEOs and CFOs, have dinner with them, and interpret whether they are optimistic about the next quarter. Funds that have dozens of analysts crunching datasets you weren't even aware existed. They will track corporate private jet movements to suss out whether an acquisition is likely to take place. They will run a machine learning model to assess the emotional state of Jerome Powell from his eyebrow twitches as he announces Federal reserve actions. They will take satellite data imagery from parking lots to predict whether Walmart will beat quarterly earnings guidance. Public markets are incredibly competitive. They are where some of the most talented individuals make their careers, and there's no real restriction on being able to act on information (outside of insider trading). Anyone who believes they have an edge is free to express their view in a trade.

So if you feel you have information which is market-relevant (like this expectation that a supply contraction would drive up the price), the most sophisticated participants have it too. And they've already evaluated it and acted on it.

Additionally, you need to recall that markets are not democratic. They are weighted by capital. A whale can express a far stronger opinion than a minnow. Hedge funds simply have more capital (and they tend to have access to cheaper leverage!). Then, when they develop a view on some stock,

they have the means to express that view. This is how the "pricing in" takes place. Thus it's really only price-setting entities that matter most of the time.

Plustoken amassing 200k BTC (~1% of supply) and selling it was a major driver of price action in 2019. Why wouldn't the halving (affecting 1.8% of issuance) do the same?

First of all, the rise and fall of Plustoken wasn't anticipated. It was genuinely new information — so much so that most investors only learned of the magnitude of the ponzi until **after** it was mostly done selling off. Also, as far as we can tell, the Plustoken BTC wallets were liquidated over a relatively short period; about 1–2 months far as I can tell. That's a lot of BTC for any market to absorb. The change in issuance adds up to a decline in 1.8% annualized — but that's annualized. What it means mechanically is that ~24,800 fewer BTC will be mined every month. That's a large number, but it's not the same as 200,000 BTC being liquidated in a short period. And, unlike Plustoken, the reduction is known well in advance.

The halving will affect Bitcoin from the demand side, by causing excitement among investors and getting press coverage. Thus the halving will still be a positive catalyst for Bitcoin

The same logic as found in the response directly above holds here. If you look at the Litecoin case study, the price was clearly bid up in anticipation of the halving, and then it collapsed after the halving itself. This may well have been a case of investors hoping that the halving would be a positive catalyst. You can see how investors positioning themselves (making bets on how they think other investors might react) affects price. You get into a recursive game where everyone is watching everyone else, and they all try and anticipate what the other is doing. Thus even if there is a highly-anticipated demand-side shock on the date of the halving (either through press coverage or simply investor ebullience), it will have been anticipated by a price setting entity and likely incorporated into price months prior.

If markets are efficient, there's no point investing in Bitcoin

This isn't the case at all. There are some informational facets of Bitcoin which are entirely known and transparent, like the supply schedule. However, as I mention above, a lot of the fundamental drivers of the Bitcoin price are not easily quantifiable or even knowable. No one quite knows how many Bitcoin owners there are worldwide, for instance. If you are able to forecast these factors better than others, you will be able to find an edge. Additionally, there are plenty of un-forecastable shocks which might have a positive effect on

Bitcoin in the future, such as currency crises. Critics of the EMH fail to see that it only stipulates that markets express ***available*** information. Obviously, unknown future catalysts are not available. They haven't happened yet.

Ultimately, if you are better at forecasting Bitcoin's growth than other price-setting entities, you might want to trade on your superior knowledge. I think this is an entirely plausible prospect. So I am absolutely not discounting Bitcoin potentially being attractive for an active allocator, even in the presence of the EMH. Indeed, I personally have a positive outlook on Bitcoin. So clearly I believe there is alpha in having specific domain expertise on Bitcoin. If I were a staunch strong-form EMH believer, I wouldn't be in active management! In fact, active managers have a very strong incentive to find ways to repudiate the EMH. So it should be rather telling that I am defending it here.

For an example of what a demand-oriented fundamental model of Bitcoin might look like, here's an attempt courtesy of Byrne Hobart:

Investing in Bitcoin: The Asset Allocator's Perspective

Off and on, friends ask me why I'm not working at or running a crypto hedge fund. I'm interested, worked in the...

medium.com

Under the presence of weak-form EMH, fundamental analysis is possible, and indeed necessary. After all, someone has to do the analysis to surface the information that ultimately is expressed in prices. This job is left to active managers. So maybe those nasty hedge fund investors are useful for something, after all.

Thanks to Allen Farrington and Leigh Cuen for their helpful review and feedback.

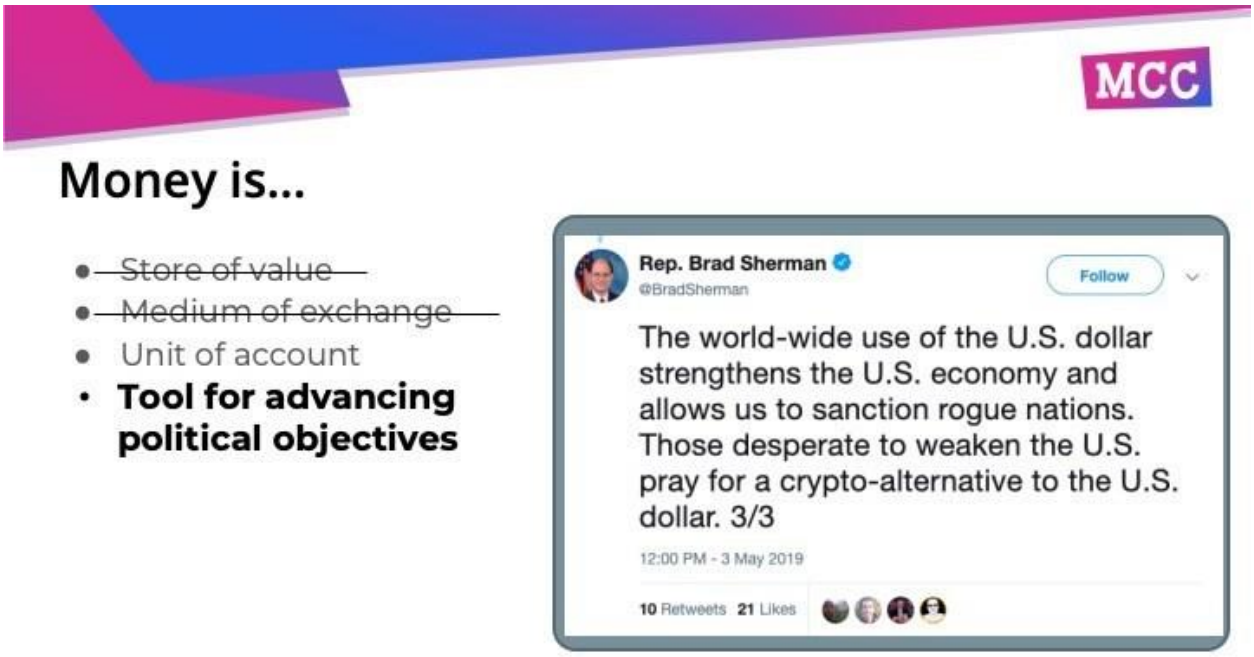
How to Resist Censorship with Bitcoin

By Elaine Ou

Posted January 4, 2020

This is an excerpt from a presentation I gave at the 2019 Magical Crypto Conference.

Some time ago, I was arguing with a nocoiner on the internet, and he brought up the usual FUD, with the Nazis and North Koreans and global warming. But then he said something that made me think. He said, any defense of bitcoin is morally bankrupt. And I thought, that's **exactly right**. Bitcoin is completely devoid of morals. **Good.** Because money shouldn't have morals. We're building a global currency, not roleplaying Model UN. And that's everything that's wrong with fiat money today.



Money has suffered from **feature creep**. Economists like to define money as filling three roles – store of value, medium of exchange, unit of account — but the function of money has changed over time. The US dollar hasn't been a store of value for decades; in fact it's designed to depreciate at 2% a year to encourage consumerism. And exchange is now mostly done on credit. What we do have is the standard unit of account for international finance. If everyone's using the dollar, we can weaponize it to coerce certain behavior. Advancing political objectives, is the dollar's most important use case. Congressman Sherman gets it.


COMMENTARY

Don't Like an Industry? Send a Message to Its Bankers

With Operation Choke Point, the Justice Department's targets have included vendors of firearms and fireworks.

Mostly we do this by economically isolating a group of people we don't like. This can be anything from embargoing a whole country to Governor Andrew Cuomo and his sanctions against the NRA. As a result, the NRA lost their insurance and banking services in New York. Then there was **Operation Chokepoint**, a 5-year program where the Justice Department investigated banks for doing business with politically incorrect customers like gun dealers and payday lenders. An investigation isn't the same thing as a ban, but by imposing extra requirements to serve these customers, it ends up having same effect.

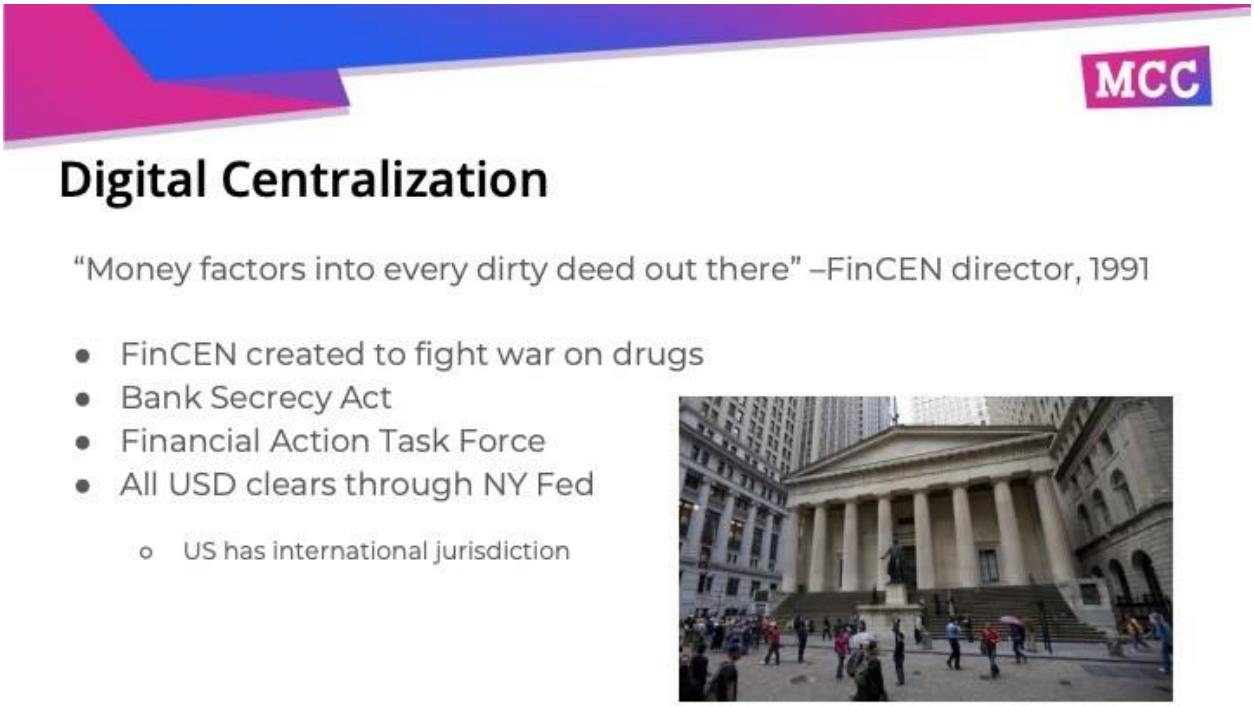
MCC

If a Law Cannot be Enforced, Does it Exist?

Here in the US we have the 4th Amendment, which says the cops can't come search your home without a warrant. It protects us from having cops randomly barge into our homes, but more importantly it limits the state's power to regulate. Even if the government did want to overreach and make rules about what we do in the privacy of our homes, there's no way to enforce those rules. So we can invite some friends over for drinks and cigars and play a game of poker with real money. In theory that's illegal. In practice, the cops can't do anything about it unless I invite them in. The government effectively has no say in the matter when it comes to peer-to-peer cash. Decentralization may not limit regulation, but it limits the **enforceability** of regulation.

A lot of the laws we have are self-enforcing. And by that I mean, most of us go through life without ever shoplifting or murdering anyone, and we manage

to do this without cops on every street corner. We do this because there's a societal consensus about what we shouldn't do. On the other end of the spectrum you have something like speed limits. Technically it's illegal to speed, but everyone speeds and mostly no one gets caught. In fact if you stay below the speed limit you're probably pissing off a lot of people behind you. The government can't put a throttle limiter in every car. So if a speed limit is unenforceable then a speed limit sign is basically fake news. Same with money laundering. It's the world's third largest industry after oil and agriculture. This is exactly what happens when you have laws that are **too dumb to enforce**. The only thing you can do to stop it is make more rules that everyone will go on ignoring.



Our self-regulating ways started to change in the 80s and 90s. Banks began storing account information in IBM mainframes instead of filing cabinets. Not only do computers make it easier to report suspicious activity, but they make it really easy to create **blacklists**. When the government realized it was losing the War on Drugs, they didn't say, "Wow I guess this rule is too stupid to enforce," like they did with Prohibition. They made FinCEN, which is basically a big data agency. FinCEN collects data from banks, credit bureaus, all the different law enforcement agencies. If all our transactions go through regulated financial institutions, then it's suddenly really easy to enforce stupid rules that no one would otherwise follow. And we can do it to anyone on the planet with an international bank account.

MCC

Permissioned Money

The end result is that there might as well be cops permanently stationed in your living room. Or an Amazon Echo, same thing.

MCC

Trusted Third Parties are Sanction Holes

- Any centralized system can turn into a general purpose regulatory tool.

ShapeShift failed? It may be due to geo-blocking

Unfortunately, our partner, Shapeshift, has enabled geo-blocking for Iran, North Korea, the states of New York and Washington. ShapeShift services in Jaxx will be unavailable for IP addresses that originate from the above locations.

If a third party service presents an easy way to enforce dumb rules, of course regulators are gonna take advantage of it. Regulators are lazy; that's why they invented sanctions in the first place.

MCC

Maduro Stymied in Bid to Pull $1.2 Billion of Gold From U.K.

By Patricia Laya, Ethan Bronner, and Tim Ross
January 25, 2019, 11:11 AM PST *Updated on January 26, 2019, 6:24 AM PST*

- U.S. lobbied U.K. officials to cut off the Maduro regime
- EU takes sides against Maduro in Venezuela's power struggle

LIVE ON BLOOMBERG
Watch Live TV >
Listen to Live Radio >

Even gold isn't safe anymore. Well it's safe if you hold your own gold, but this is why you don't store your gold with the Bank of England. Venezuela kinda screwed itself with the whole socialism thing, but here they're trying to fund imports to feed their citizens and the US lobbied the Bank of England to cut them off.

MCC

DECEMBER 17, 2018

Thanks to US Sanctions, Iranians Are Turning to Bitcoin Mining

BY MAZIAR MOTAMEDI

You can't enforce sanctions if you can't deputize the banks.

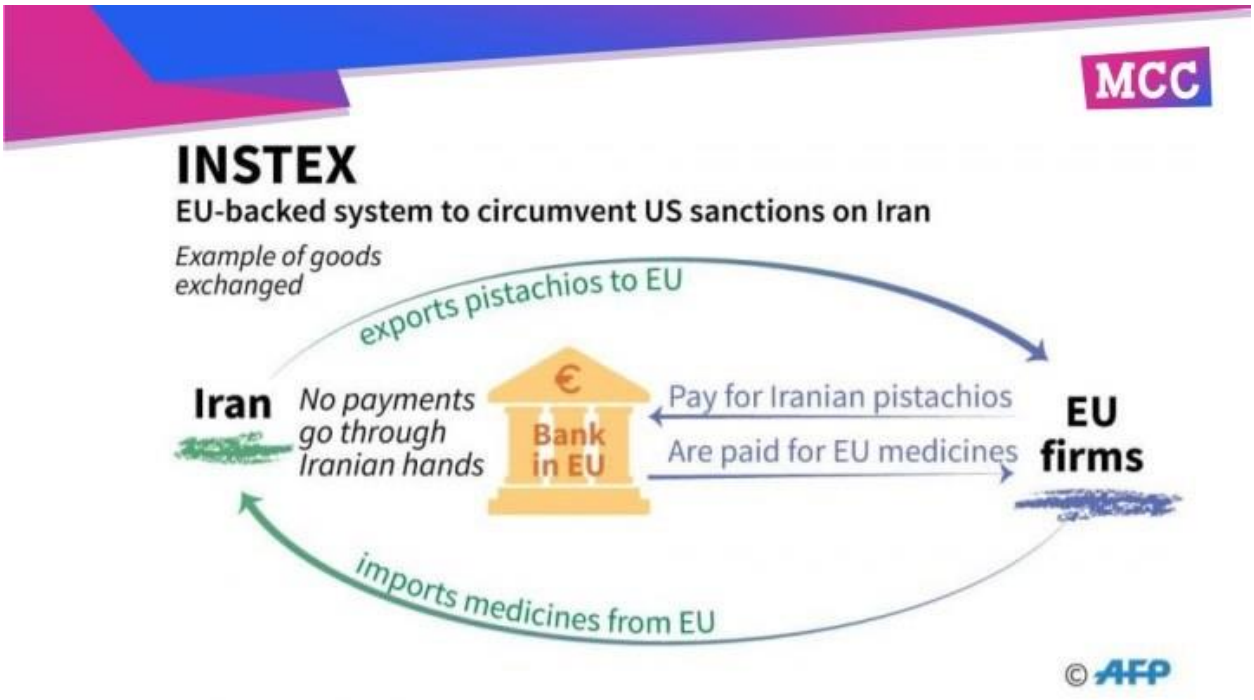
Herd Immunity

- Decentralize all the thingz
  - Run your own economic node
- Use privacy tools even if you don't have to
  - FinCEN: Bank fraud comes through Tor
  - If privacy tools are common, then the assumption that only criminals need privacy is invalid

We already know to run our own node, be our own bank. Even if Coinbase meets your needs, decentralization gives us **herd immunity**. If no one uses Coinbase, then Coinbase can't be used for law enforcement. Same goes for privacy. Right now, most bank websites won't let you log in if you connect through Tor. A few years ago FinCEN did some analysis on IP addresses logged in the suspicious activity reports filed by banks, and found that a lot of sketchy stuff came through Tor. Now anyone who uses Tor is treated like a criminal. Next they'll be looking at VPNs. If everyone speeds, no one gets busted just for speeding. If everyone uses privacy tools, then no one gets flagged as a criminal just for using privacy tools.

Blockchain analysis companies have gotten really good at tracing the provenance of Bitcoin through inputs and UTXOs, and convinced the Treasury Department that a good way to sanction Iranian hackers is to blacklist a couple of bitcoin addresses. The guy controlling these addresses already generated a new wallet and bragged about it to the New York Times, so even they know not to reuse addresses. Bitcoin developers have come up with better ways to improve transaction privacy. CoinJoin combines multiple Bitcoin payments from multiple spenders into a single transaction. Another proposal is pay-to-endpoint (P2EP) where both the Sender and Receiver contribute inputs to a transaction. The goal is to break the ability to identify the sender and receiver of a transaction. If enough people create transactions where senders can't be identified from the inputs, then blockchain analysis tools will become like those old-school polygraph tests, where they generate so many false positives that they completely lose credibility and are regarded as **junk science**, no longer admissible in a court of law.

We can also learn from financial institutions. Over the last decade, banks have paid something like $20 billion in fines for sanctions violations. OFAC sanctions, they're like ransomware for banks. Most of these are international banks serving international customers. They don't always appreciate it when we recruit them to further our foreign policy.



In Europe, banks set up a special purpose vehicle so European companies can transact with Iranian businesses without violating sanctions. A business in Paris might want to buy oil from Iran, and a pharmacy in Berlin might want to sell medicine to Iranians. **Instex** is a clearinghouse that matches credits and debits for these businesses, they settle their payments locally, and specific cycles are formed so no money ever transfers across the border.

It looks a lot like **Lightning**. As a network, Lightning serves as a clearinghouse where payments are routed all around the world, but actual settlement only happens when two nodes close a channel on the blockchain. This map shows public nodes and channels, but there are tons of non-public nodes and channels and no one needs to know what happens in the clearinghouse. We can create specific cycles in the Lightning network where we spend and stack sats and only rarely return to the main settlement layer.

Earlier this year we had **LNtrustchain**, which went all over the world to Iran, then Israel, and ended up in Venezuela. We have a map of the Lightning torch journey, but if participants hadn't advertised themselves on Twitter, no one would have been able to trace the torch.

The goal is not to use Bitcoin to evade sanctions or break the law, cuz we should all be law-abiding citizens. The goal is to make it so that financial censorship is no longer a thing. If no one can be forced into economic isolation, then announcing sanctions will be about as silly as thinking you can stop people from playing poker in their living rooms.

Dear Libertarians: Bitcoin Fixes This

By Rollo McFloogle

Posted January 5, 2020

As libertarians, we know that the emperor is not wearing any clothes. It's brutally obvious to us that the state is not only evil but also unable to realize a peaceful, productive society for all to enjoy. We can rigorously arrive at this conclusion through any number of ways: from pure consequentialism to deontology to ethical intuitionism. The logic, economics, and ethics all make sense on their own, but what strengthens their conclusions is that they all compliment each other in a wonderfully elegant way. A rock-solid case can be made for libertarianism and is worlds better than even the best steelman of any of the state-centered alternatives.

Unfortunately, many of those around us don't see this. Can they not actually see it? Or maybe they just don't want to see it. It's difficult to know because humans are complex creatures whose experiences and environments create an infinite amount of biases and perceptions. You can walk someone through each logical step of your libertarian justification, and he will nod in wholehearted agreement, but when you tie all the steps into their logical conclusion, he will undoubtedly reject it. And he won't have a good reason. The conclusions of libertarianism are so far outside of the paradigms of polite society that it's just too much for most people accept.

So we look for various strategies and methods to do our evangelization. Some work better than others. Memes, for example, have proven to be a wonderful way of delivering messages. Many, myself obviously included, have taken it to the blog and podcast world. But unless these things are truly a passion that you like doing, it can get very discouraging because the ratio of changed hearts and minds to the overall effort exerted is just so low. I'm not saying that it never works, but that this strategy working on a large scale is simply impractical.

For the majority of people, it takes too large of an investment of time and focus to grok the information well enough to not only unlearn years of misinformation but also absorb everything else that needs to be learned. As

such, we should not hitch our hopes and dreams to the culture change wagon.

Meanwhile, there are a number of libertarians who hope that a collapse of the state (and/or economy) will shake up society enough for at least some areas to splinter off as libertarian communities. I wrote about the problem both approaches face in a previous article:

If the state were to collapse tonight, what would happen tomorrow morning? We'd probably end up with something that is pretty close to what we had just before. Of course, it wouldn't happen that quickly, but the point is that in order for the structure of society to have a major shift towards liberty, a huge paradigm shift would need to occur in the minds of the people in that society. If a stateless society were to come out of the collapse of the current state, the collapse would need to affect the mindset of a significant portion of the people in a way that they would come to reject the state. Maybe that would happen for some people. But based on history, the result of collapses and revolutions has been to try the state again but in a bit different way. People just try it with different rulers. This means the root cause of the problem is not solved. Rinse and repeat. This is why the incremental replacement of state institutions by private markets is superior in an effort to have the market make the state obsolete. This slow approach makes people change without them even realizing it.

There is room to optimize this strategy to avoid some potential issues. While services like Uber and Lyft can disrupt the legacy taxi system, these markets tend to get corrupted because governments still have a central point to attempt to influence. Furthermore, they won't stop the state from waging endless wars and doing the other terrible things it does. Progress is very slow as the government plays Whac-A-Mole with entrepreneurs who search for and exploit loopholes in regulations. The hope is to make the state die by a thousand cuts and just give up after being overwhelmed. The better tactic against the state, however, is not aimed at avoiding its control but rather in destroying its ability to control.

In a 2014 interview, Cody Wilson had the right idea when he presented this strategy against the state: "Give it something it can't shoot with firepower and we'll see what it does." This is great, but what do we attack and how?

Enter Bitcoin.

Bitcoin is a decentralized digitally scarce and censorship-resistant medium of exchange. It provides people an alternative to the central bank fiat system where governments enjoy the benefits of seigniorage, the profits made by inflating the money supply. Seigniorage is instrumental in their ability to finance tremendous amounts of debt as they pay for programs and wars of

infinite scope. They could never directly tax their subjects to fund all of this—the necessary taxes would be far too burdensome for everyone to accept. Instead, inflation is the insidious devaluing of wealth while everyone gets drunk on the easy credit and money that become available instead of noticing what's going on.

But if there is a harder alternative money available, it will monetize in place of the incumbent money. We all know how much the US dollar has lost in purchasing power; meanwhile, Bitcoin has a hard supply cap of 21 million that will be reached around the year 2140. Want to change the monetary policy of Bitcoin? You're going to have to convince enough of the individuals running their own full nodes to change the consensus to run your ruleset. Given that they chose Bitcoin to avoid this sort of thing, it's nearly a nearly impossible task. Want to censor transactions or manipulate the status of the ledger? Be prepared to spend huge amounts of money on capital equipment to run a mining operation that would be so expensive to run, you're likely to bankrupt yourself before you're able to achieve your goals.

Forget "End the Fed." Let's make the Fed obsolete.

As more people start to hold Bitcoin and demand it as payment because they prefer the currency that appreciates over time, governments will be pressured to abandon their fiat systems whose values plummet to zero. They will be losing their most productive workers to private industry who woo them away the promise of pay in hard money while the government still tries to convince people to accept their value-hemorrhaging fiat. With no other option than to adopt Bitcoin, they will no longer be able to simply print money to fund their ventures. Direct taxation and service fees will be their options for income generation, which means they will have to drastically reduce what they do in their size and scope. They will be left with performing the "essential" services, while entrepreneurs will have the room to solve problems in the much freer markets that governments simply do not have the resources to attempt to regulate.

In the meantime, cheap credit and easy money will be a thing of the past as prices begin to actually reflect the conditions of the markets. Resources will be directed to the places where they are most needed, reducing inefficiencies and waste, which provides a huge shot in the arm to overall economic output. Business cycles will cause less harm across economies. As capital is accumulated and wealth is transferred from those favored by the government to those who truly deserve it, entrepreneurs can focus on more directly competing with whatever services that the state is still providing.

People won't adopt Bitcoin because they buy into some cypherpunk or libertarian ideology. They'll adopt it because it provides them with a better

tool to transport wealth across time and space to deal with future uncertainty. It won't even have to be a conscious decision.

The prevalence of sound money also permeates society with other positive benefits. Under an inflationary monetary system, people are incentivized to spend their money today because it will be worth less tomorrow. This creates a very short-sided, or high time preference, mindset. People care more about instant gratification than building things that last in their lives. Bitcoin fixes this because it reverses that incentive. With money being worth more tomorrow than it is today, people will tend to delay gratification in the short term in an effort to save their money to maximize its impact, thus lowering their time preferences. People will become more future-oriented, taking great care not to take actions today that would have harmful future consequences. This builds the necessary momentum for changing societal cultural preferences for the better.

When the security markets mature enough that people stop paying taxes for police and courts, government agents sent out to extract money from people will finally be seen as the marauders and pirates that they are. The private security agents will be too well equipped with too much market share at stake to let their clients be robbed by the government; the government agents will see trying to fight back as useless. This will be the final death blow of the state. Anything worth being done will be done by private industry and the state will have lost the monopoly of violence that kept the spigots of funding open.

"Libertarianism" as we know it will die off because it will simply become the ***status quo***.

Bitcoin and the Primacy of the Digital World

By Pascal Hügli

Posted January 8, 2020

As a fervent bitcoin enthusiast, I frequently come across the following objection: In contrast to physical, analog things, bitcoin and similar crypto assets are completely virtual and digital. As such, they are neither tangible nor graspable and would thus lack any real basis of value.

Because of their digital nature, many people still object to bitcoin, refuse to take it seriously or consider it altogether too scary. Some even lump the crypto asset in with other eerie and unsavory developments in tech and the ongoing digital transformation.

Be Not Afraid of the Digital World

Among greatest digital threats seems to be the phenomenon of “deepfake” media. This is a term that has been in common use since 2017 for the technology used to create deceptively authentic-looking images and videos. Many politicians, actors and other celebrities have already fallen victim to this practice. Deepfake videos put words into their mouths that they never said or make them perform actions they never did. What is real and what is not?

Some technophobes fear that because the capabilities of the digital world are increasingly blurring our notions of reality and what is artifice, political as well as societal life could become ever more confused and agitated. Democracy hinging on the fact that civil discourse and public debate happen among educated and enlightened citizens is very much in danger because the “fake” will become indistinguishable from the truth.

Within the reactionary mistrust of all things digital, bitcoin is getting its share of blowback as well. If this sort of mistrust resonates with you, I am here to tell you — some of these hazards associated with an increasingly digital world are certainly true. But Bitcoin is your ally, not your foe in this.

When looking at bitcoin, the juxtaposition of analog and digital might seem obvious at first glance — dissecting it further though reveals some interesting twists. Although bitcoin is virtual and non-corporeal, as a new manifestation of money it has actually overcome many characteristics of what is typically associated with the digital realm.

Bitcoin as an Asset

Interestingly, bitcoin as an asset does experience increasing marginal costs in production, a feature that can be seen in conjunction with gold, a tangible asset of the corporeal world. The more gold is produced, the more expensive it becomes. In the case of bitcoin, the production of new units is algorithmically set to a maximum per block/time interval. In other words, no matter how hard one tries, one can never produce more bitcoin within a period of approximately 10 minutes than the amount specified by the code. It is this digital scarcity imported via the real world that makes bitcoin potentially valuable.. The potentiality of value is being actualized as more people are persuaded of its absolute digital scarcity, since any realized value is always the result of subjective value judgements by individuals.

Bitcoin as a Digital Bearer Instrument

A bearer instrument refers to an instrument that is payable to anyone possessing the instrument and is negotiable by transfer alone.
Source: https://definitions.uslegal.com/b/bearer-instrument/

Bitcoin is not only digitally scarce but, by its very nature, is similar to a bearer instrument — another feature where bitcoin contradicts the usual notion of digital goods. Because bitcoin resembles a bearer instrument, it can be held independently and apart from any third party. While holding bitcoin does not give a bitcoin holder any rights against any tangible issuer, possessing bitcoin does indeed entitle a bitcoin holder to have them spent univocaly — that is, the bitcoin protocol automatically and undeniably executes a bitcoin transaction once initiated by a rightful owner. This goes to show that having bitcoin is associated with some sort of underlying right against some sort of issuer, the bitcoin protocol.

Thus the crypto asset has proved for the first time in history that bearer instruments no longer have to be printed on paper to have these characteristics. Bitcoin has solved the double-spending problem and cannot be copied. It's the perfect combination of the advantages from the analog as well as the digital world.

An Idea Whose Time Has Come

Many still do not appreciate the ingenuity of this combination. However, it is important to recognize that it is based on a way of thinking that is

increasingly losing its validity. For more and more people, the digital has become a matter that is taken for granted. While older generations may still make excursions into digital spheres as "tourists" of an analog world, Gen-Z, millennials and even the slightly older Gen-Xers have long been at home in a digital world where bits dominate atoms.

Having grown up mostly as digital natives, they have cultivated a digital lifestyle from the ground up. This gives them a completely different attitude toward the digital world than people who have been socialized knowing only the analog world. One of the most impressive examples of this development is the video game Fortnite.

For so-called Google kids, Fortnite is much more than a video game — it is the reality of their lives in which they socialize and spend more time than in the "real" world. February 2019 was the biggest moment in Fortnite's young history: The American electronic music producer DJ Marshmello gave an in-game concert. His performance took place completely virtually on a stage within the computer game. Fortnite players could participate only as their virtual avatars. And that's what they did: Almost 11 million mostly young people danced as their game characters in the digital concert.

Such events may seem surreal and curious to older generations, but for these Google kids, they are completely normal. Similarly, V-Bucks, the currency within Fortnite, are valuable assets for them. From this famous in-game currency, it is only a small step to bitcoin and other cryptocurrencies. This digital mindset also explains why some female millennials may be just as happy to receive a digital bouquet of flowers on their smartphones on Valentine's Day as they are to receive roses that have grown in the soil. Similarly, the day is soon approaching when digital gold will seem more "real" to this generation than physical, precious metal.

An Exponential Way of Thinking

As a species, we are in the process of digitizing our reality. This is probably just another iteration, not the last, of a cultivation process that humanity has been going through since time immemorial. We learn to think in gradually more abstract categories and tap into new potentials again and again. The process of cultural adaptation to fully adopt digital values has only just begun.

What makes it more difficult with bitcoin adoption, however, is the fact that it is an ***exponential phenomenon***. Our brains, on the other hand, are designed for ***linear interpolation***. We instinctively understand that if we take 30 one-meter steps, we can travel 30 meters in total. If we could somehow not take linear but exponential steps, the situation would be completely different. The same 30 steps, exponential in nature — translating to 2^30 steps — would take us around the world 26 times, a fact that we can hardly picture rationally.

Because our thinking is not one of an exponential mindset, exponential technologies have always overwhelmed us. One only needs to think of the internet or the smartphone: These technological advancements seemingly appeared all of a sudden, but shortly afterward, they had conquered the world. Bitcoin is now the next exponential technology to thrive on the back of these two (and other) exponential technologies. Just like the internet or the smartphone before it, the crypto asset is likely to produce second-round and third-round effects which will fundamentally change the world.

With each passing day, it makes less and less sense to perceive the virtual and physical worlds as separate spheres of human action. Our reality is getting evermore digital and, with it, physical atoms might be more and more dominated by digital bits. If you are intimidated by this, this is totally fine. But let me reiterate what I said in the beginning: Because bitcoin is a digital thing without the problems inherent to the digital world, it is your friend and not your foe.

Valuing BTC as a commodity

By Acrual

Posted January 8, 2020

After reading Fernando Nieto's comments (Fernando Nieto) about his cost of preservation, I have been digging into the models used to value commodities which have to do with assesing the cost of transportation and storage mainly and so far it is the best framework I've come across to value Bitcoin.

If you think about it, the potential demand for Bitcoin is stratospheric, as there is nothing more valuable than the utility of exchange.

Nobody in his right mind doesn't demand the ability to exchange utility over time. We want to make sure that whenever a need arises, we will be ready to satisfy it.

It doesn't make sense to acquire all the goods and services now, as they deteriorate over time and the need doesn't happen at the same time as the availability of a good or service that satisfies it. As a result, having the ability to postpone that utility of exchange at whatever time, is extremely valuable.

You can do two things:

- Preserve a good into the future that satisfies a need inmediately
- Exchange a good inmediately that satisfies a need in the future

The former is a present good and the latter is credit.

As Nick Szabo explains the Selfish Gene theory in his "Shelling Out" paper:

> cooperation between non-kin, which evolutionary psychologists call reciprocal altruism. As Dawkins describes it[D89], unless an exchange of favors is simultaneous (and sometimes even then), one party or the other can cheat. And they usually do. This is the typical result of a game theorists call the Prisoner's Dilemna – if both

If the exchange of favors (or the exchange of utility) is not inmediate, and even then, either party can cheat and as it turns out, they usually do.
That's why it is so important that for money we use present goods, and not credit. With credit of the Central Bank, as fiat money is, we are trusting strangers that don't pay the consequences of their mistakes.

As Fernando Nieto puts it, the cost of friction of owning a commodity is something like:

CoE1 + CoP*t + CoE2

where CoE1 is the cost of buying (acquiring) it and CoE2 is the cost of selling it whereas CoP*t is its cost of preservation as a function of time, which includes its deterioration, inflation, cost of storage and custody, transaction validation, ability to remain safe from thieves, etc...

Note: Fernando has kindly corrected an error, as the cost of transaction validation is obviously a CoE and not a CoP as I stated above

Whether the CoE or CoP of a medium of exchange are high or low, determines the time frame you will be eager to keep it for.

For example, for how long do you tend to keep your USD or EUR paper notes with you? What % of your wealth is into this? USD paper notes have very low CoE yet very high CoP because of its inflation mainly even if they are in the form of deposits. That's why we keep small amounts of it and that's why its actual value is on the order of a couple trillion dollars.

On the other hand, what % of your wealth is into real estate, or financial products or even gold? Its CoE is way higher but its CoP is way smaller than with paper notes, so you tend to keep them with you for really long periods of time.

If its kept (hodled) over long time frames, its value is very high and indeed it is as the real estate market is worth $210tn (even if only 10% of its demand is as a medium of exchange, we are talking about $20tn), $70tn for financial products and $8tn for gold, not to mention the estimated $20tn-$30tn in offshore money.

This means that given Bitcoin's extremely low CoP, Bitcoin is meant to be kept for very long periods of time. In really long periods of time it is a good idea to invest a small allocation of your portfolio, as an insurance for very bad events.

If it's meant to be kept for really long periods and it is a small allocation of your portfolio, volatility won't be a problem.

The more people understand this, the more Bitcoin becomes a self-fulfilling prophecy, the more it appreciates creating upwards volatility which is an even smaller problem than volatility itself and the more people are attracted to what in my opinion is the best form of money we have ever seen.

More people will decrease volatility and that small allocation will turn into a larger one.

With that in mind, if we add those $21tn + $70tn + $8tn + $20tn and divide them between the 21million btc — 3million lost, we will have a rough number of $6m-$7m per bitcoin

Bitcoin has already succeeded

By Acrual

Posted January 12, 2020

I frequently come across, like I guess most of you, people who repeat the mantra of “Bitcoin has failed” or “Bitcoin is going nowhere”, blah, blah, blah.

As I recently said in twitter, I find it hilarious; when I hear/read this, I have the same feeling as if someone told me my home or my computer have failed.

If value is subjective, **who do you think you are to tell me something that I find useful has failed for me**?

I can agree with you that my house or my computer may suck to your standards, but how can you know if it is not good enough for me? Isn’t that extremely arrogant?

Let me tell you a really brief story:

Something like 10 years ago, I got a speeding ticket yet I didn’t find out until it was very late because notifications from the authority were going to a former address of mine. So I was getting those notifications there but I had already moved somewhere else. Apparently I have the obligation to notify this authority in my Country, that I was actually moving, but I didn’t know.

Given the constant delays in payment, the ticket was getting larger with extra penalties.

Then one day, I can’t remember how, I found out that my bank accounts were about to be blocked. I was not married and didn’t have kids at the time, but the mere possibility of running out of money was one of the most scary experiences I’ve been through. **I don’t think I have ever felt this powerless**. Now married and with kids and with a communist regime in power which believes my individual well being is secondary to their ideology, it is as scary as it gets. It was me against bureaucrats on the other side of the phone that were simply following orders and for whom I was a mere ID number.

Until then, I thought this kind of things only happened to people that didn’t pay their taxes or criminals...

I don’t live in Afghanistan but in an EU country, so I can only imagine the number of problems people in that kind of countries may go through regularly.

If you think Bitcoin’s volatility is a problem, you are likely to have never experienced full volatility, that is, seeing your money going down to zero.

This is what many pundits don't see. If there are some initial use cases for Bitcoin in developed countries, just think of the potential eventual demand elsewhere. If the cost of storing this part of my wealth is both microscopic and censorship resistant compared to any other form known to us, then there is definitely a gigantic potential appreciation, becoming a good investment idea too. I'm as a result both a user and a speculator.

It all comes down to what you consider a success for Bitcoin. For me the fact it is already useful for me and many others is a complete success. Whether there is a tiny chance of it being attacked is irrelevant. My government could ban wine tomorrow and that wouldn't make wine useless or a failure overnight.

When did the iPhone succeed? When it reached $1m in sales? $10m? $5 billion? Or maybe 20 million users? or 100m?

For the same reason, has Bitcoin succeeded? If you can enjoy its utility already, I think it has. If not, what defines its success? And what defines its failure?

Whether you have not discovered its utility yet, that's an entirely different matter

Bitcoin Is Magic Internet Money

By Rhythm

Posted January 13, 2020

There may not be a more perfect representation of Bitcoin and its early community than this drawing created in Microsoft Paint, portraying a wizard in a blue cloak holding a staff with the slogan "**Magic Internet Money**". The illustration was created as a promotion to entice users on Reddit to learn more about the currency and join the Bitcoin specific forum.
Its reception was overwhelmingly well-received, and in part, helped build Bitcoin's brand awareness. When the advertisement went live, the community consisted of a little over fifty thousand subscribers and the price of bitcoin was still under three hundred dollars. For reference, the same forum is currently 1.2 million users strong. There were even almost 600 comments discussing the promotion and drawing itself. The thread is filled with Bitcoin users tipping other users with the "magic internet money". It was an example of a true grassroots and community-driven marketing campaign for, which at the time was still an incredibly niche community.

A subreddit moderator for r/Bitcoin made a post asking the community to help create and brainstorm ideas for a promotion. Within the hour, the user /r/mavensbot submitted the iconic image. He later went on to say it supposedly only took five minutes to illustrate it. For those unfamiliar with the Reddit website, this is what the promotion looked like to visitors:

Source from a write-up done by Paul Bars

The slogan describing the currency as “magical” however, was first used on a relatively obscure BitcoinTalk.org post. A poll had been created to pick a slogan for this new internet native currency. With only a few dozen voters participating, the infamous meme was born. “Magic Internet Money” won the poll, with “In Crypto We Trust” and “You Asked for Change, We Gave You Coins” not too far behind it.

edit 2013-03-03 / -03-06:

Hall of Fame

2013-05-05
Magic Internet Money - 17 (11.3%)
In Crypto We Trust - 16 (10.6%)
You Asked For Change, We Gave You Coins - 16 (10.6%)
The Fastest Way To Pay Around The World - 8 (5.3%)
Money Changes Everything. Bitcoin Changes Money. - 6 (4%)
The Future of Money. - 5 (3.3%)
Banking without Banks - 4 (2.6%)

Bitcoin users embraced the nerdy and near whimsical characterization given to it by the media and countless individuals in power. Even with the constant

doom and gloom predictions of the currency's future, "magically" the network has continued to operate.

- "The Rise and Fall of Bitcoin" – Wired at $2.37
- "So, That's the End of Bitcoin Then" – Forbes at $15.15
- "The SEC Shows Why Bitcoin Is Doomed" – Bloomberg at $93.57
- "Bitcoin Sees the Grim Reaper" – NY Mag at $105.7
- "Fool's Gold" – Slate at $131.95
- "Bitcoin revealed: a Ponzi scheme for redistributing wealth from one libertarian to another" – The Washington Post at $182.00
- "Bitcoin Is a Victim of Disinflation" – The New York Times at $208.50
- "Bitcoin is headed to the 'ash heap'" – USA Today at $208.50
- "Bitcoin's upcoming capital crisis" – Financial Times at $290.51
- "Bitcoin's defects will hasten its demise in 2015" – Reuters at $327.20
- "Can Bitcoin survive 2015?" – AOL at $332.63
- "Where did Bitcoin go wrong?" – CNN at $333.58
- "**Bitcoin Is A Joke**" – Business Insider at $433.57

Bitcoin was seen as a fringe phenomenon, even just a joke. With almost a decade of price making higher lows along with its seven network effects growing exponentially, the narrative is starting to shift. We are seeing Bitcoin go from "nerd money" to every corporation, government, bank and institution attempting to leverage it for themselves. There have been multiple attempts to package Bitcoin into something "compliant" or more digestible for the legacy system it ironically itself challenges. The creation of new digital currencies has been one of the more recent attempts. This only strips away everything about the network that makes it interesting to begin with. Blockchain has become the latest buzzword to fit this purpose. It is the most pervasive means of using one of the technologies that underpin the Bitcoin Network. As an exercise, take any company that comes to mind and do a quick internet search of its name along with the word "blockchain". There will be at least a few pages of results. Now do the same again, except replace "blockchain" with "bitcoin" and the results will only be a fraction of the prior search.

It may be news to some, but the term "blockchain" in the literal sense just means a "chain of blocks", a list of records, called "blocks"- quite similar to that of spreadsheets. The pages are cryptographically linked together, one after another. This concept goes back nearly thirty years in cryptography and computer science, but the term and technology have been made popular recently due to the way the Bitcoin Network has emerged. A ledger is not interesting in and of itself. What makes Bitcoin's ledger unique is that no single entity controls how or which transactions are recorded in the structure. Strip away the permissionless nature of the system, in which anyone can

access and innovate upon, and you are left with a database. In other words, just an excel spreadsheet.

A talk by Andreas Antonopoulos discusses this phenomenon of digital gentrification and corporatization of cryptocurrencies along with why we should be fighting to preserve the "weirdness" that Bitcoin brings to the world.

When someone tells you, "I'm interested in blockchain but not Bitcoin", what they mean is "I don't understand." - Andreas

That has not stopped numerous attempts to control it. As of today, several of the world's largest nations are actively developing digital currencies with the same "underlying blockchain" structure that Bitcoin leverages. They are taking the cypherpunk ideals of Bitcoin and removing the "punk" aspect while keeping the financial privacy for themselves. Last year, 2019, will be remembered as the year governments stopped laughing at bitcoin and entered the "then they fight you" stage with these digital currencies being announced:

- DCEP (China)
- EUROChain (EU)
- Libra (Facebook)
- e-Dinar (Tunisia)
- Petro (Venezuela)
- Aber (Saudi Arabia)
- Turkcoin (Turkey)
- e-Krona (Sweden)
- PayMon (Iran)

Less extreme attempts to conform Bitcoin has been occurring though "financialization". It is the inevitable process of Wall Street getting control of bitcoin. That is only a joke, of course. Financialization is when the value between multiple parties is facilitated using a financial instrument - this includes derivatives like futures and options.

There is a case to be made that Bitcoin's financialization and these financial products serve to complicate the market which requires a skill set out of reach for most market participants. Bitcoin is the first time the average person has had a head-start on Wall Street, and many do not want to give that up. Increased complication can also end up concealing bitcoin creation 'out of thin-air' if auditing the onchain metrics is not done. Rehypothecation, or creating more claims to the Bitcoin Network than there are Bitcoin is likely and could already be happening. Debating whether or not this is a negative development is a moot topic, as it will continue. Market participants and

Bitcoin users need to be aware of this process and leverage the audibility of the network to maintain confidence. **Verify, don't trust.**

Even from within the very community that rejected the status quo and embraced the memes of "Magic Internet Money", it has experienced attempts of "corporatization" with a past proposal called SegWit2x. This post is not meant to teach about the specific details and intricacies of the changes to the network or call out any actors on either side of the debate. Bitcoin may end up needing all of the supporters and advocates it can get, and re-opening old wounds seldom benefits anyone at this point. That is still to say though, those who do not learn history are doomed to repeat it. It would be a waste of months of debating and spent resources to not take anything away as a learning experience.

For a brief background, an agreement was formed in New York City mid 2017. This was to be known as the New York Agreement (NYA) where several individuals with a corporate focused mutual interest agreed to implement Segwit if a 2 Mb hard fork followed it. You can learn more about the details of Segwit here and more about block size here. This proposal and hard fork of Bitcoin's network was called SegWit 2x. It meant a doubling of the block size, and what the proponents saw as a compromise between those who still wanted even larger blocks after Segwit itself was implemented. If you would like more of the details and backstory to this implementation, Aaron van Wirdum has a well-documented article on it here.

It is important to note that not a single member of the Bitcoin Core development team, the most used implementation of Bitcoin, was invited to this select meeting. While Bitcoin's strength is in its permissionless properties, the exclusion of those most trusted by the community in implementing new changes to the network in favor of corporate CEOs, does send a message. The announcement was made via a blog post on Medium by Digital Currency Group. The proposal was backed by 58 of the largest companies in the ecosystem and 83.28% of the Bitcoin Network's hashing power initially.

In the grand scheme of attacks that Bitcoin will end up facing in its lifetime, this block size increase may appear to be relatively minor. The proposed hard fork of SegWit2x was eventually cancelled after only a few months. Bitcoin users voiced their concerns loudly. Similar to the initial announcement, a joint statement was later made by only six individuals to cancel the hard fork. This highlights how few were actually involved in the decision-making process versus the traditional governance of Bitcoin, or lack of governance I should say. To their credit, they included this in part of that decision:

Our goal has always been a smooth upgrade for Bitcoin. Although we strongly believe in the need for a larger blocksize, there is something we

believe is even more important: keeping the community together. Unfortunately, it is clear that we have not built sufficient consensus for a clean blocksize upgrade at this time. Continuing on the current path could divide the community and be a setback to Bitcoin's growth. This was never the goal of Segwit2x.

To reiterate, those who do not learn from history are doomed to repeat it. The point I'm trying to make in this write-up is to embrace what makes Bitcoin unique. Giving up the permissionless nature of the technology with government-issued stablecoins, the decision making process of protocol changes like with SegWit2x, or even just financialization of Bitcoin as an asset should be looked at with skepticism to say the least. Challenging the status quo has got Bitcoin this far already, why stop now?

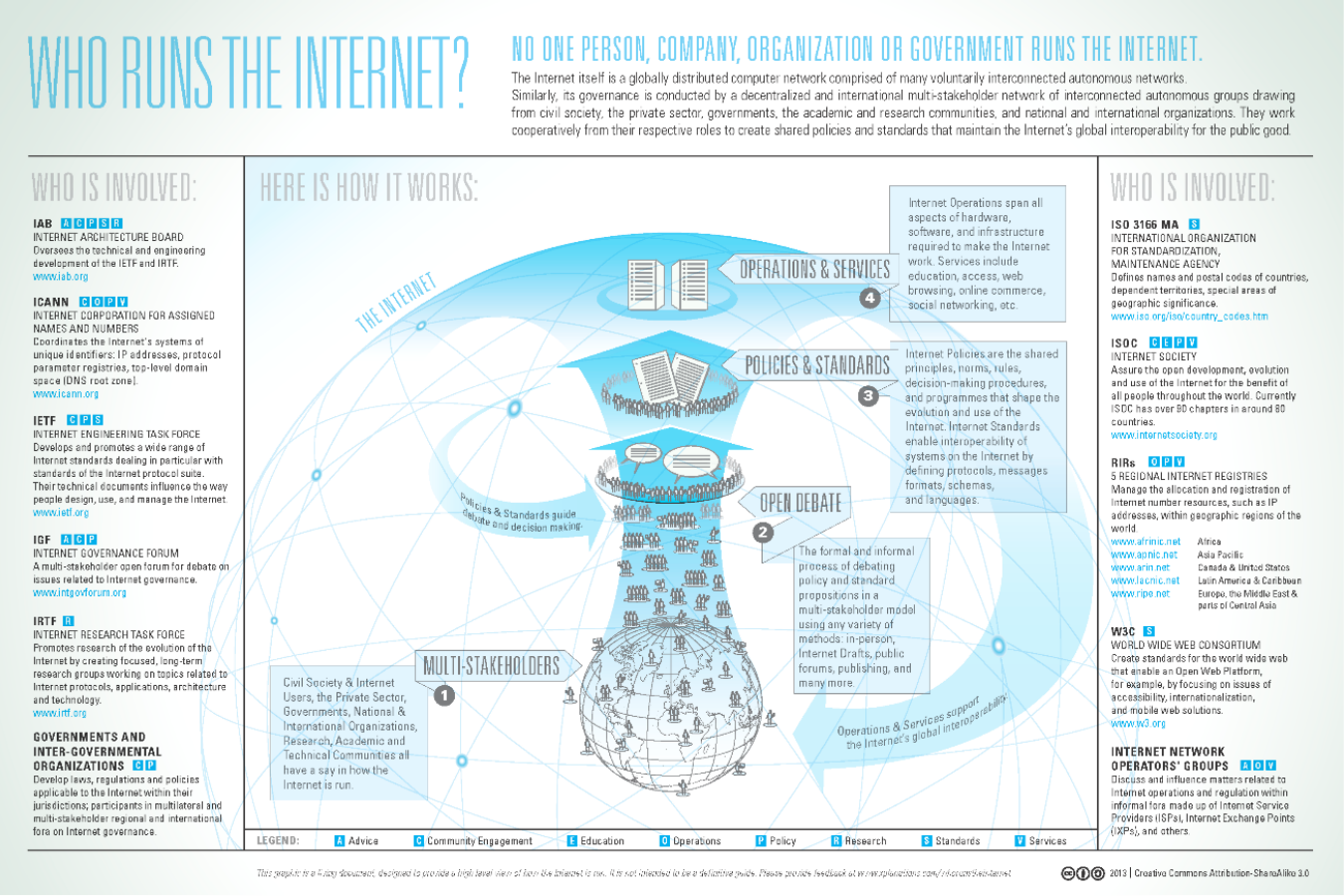
Keep Bitcoin weird.

Tweetstorm: No one person runs the internet

By Wiz

Posted January 13, 2020

No one person, company, organization or government runs the Internet. It's a globally distributed network comprising many voluntarily interconnected autonomous networks. It operates without a central governing body with each constituent network setting/enforcing its own policies.



Its governance is conducted by a decentralized and international multistakeholder network of interconnected autonomous groups drawing from civil society, the private sector, governments, the academic and research communities and international organizations https://en.wikipedia.org/wiki/Internet_governance

This means if you run your own ISP (i.e. an Internet "full node"), you get to decide how traffic flows across your own network, and you can also participate in Internet governance... but that's just boring stuff like how IP addresses and domain names get allocated and delegated.

The "link layer" control (your ISP's physical connections are Layer 1 and Layer 2) and "Internet layer" governance (ie TCP/IP protocol is Layer 3 and Layer 4) aren't super interesting. But, using P2P networks and cryptography, anyone can create their own Layer 5 ***virtual network***

For example, a centralized VPN, a distributed network like Tor, or Bitcoin's P2P network are all Layer 5+ protocols, that each have their own governance models. But because of the cryptography used they have security and privacy which allows for freedom and censorship resistance.

This is how Bitcoin is self-sovereign, how you can pirate movies over Bittorrent protocol, how darknet markets exist, etc. Layer 5 virtual networks can make their own rules - P2P networks + cryptography gives everyone freedom and allows anyone to be a self-sovereign "virtual ISP"

So the real power of the Internet isn't in the "base layer" of running your own ISP with fiber, routers, and servers, it's all in the upper transport and application layers - Bitcoin is both of these, combining cryptography with a P2P mesh network so everyone can run a full node.

Then! Once we consider the Bitcoin P2P network as a "transport layer", and start building on top of Bitcoin, the Internet really starts to get interesting. Bitcoin gives us a base settlement layer for freedom of financial transactions and BTC, soon to be the world's hardest money

The most important application stack in our generation will be built on top of the Bitcoin middle layer. Simple apps like Lightning, Bisq, and BTCPay, all routed over Tor, allow you to become your own ISP, your own bank, your own exchange, and your own payment processor. Fuck KYC

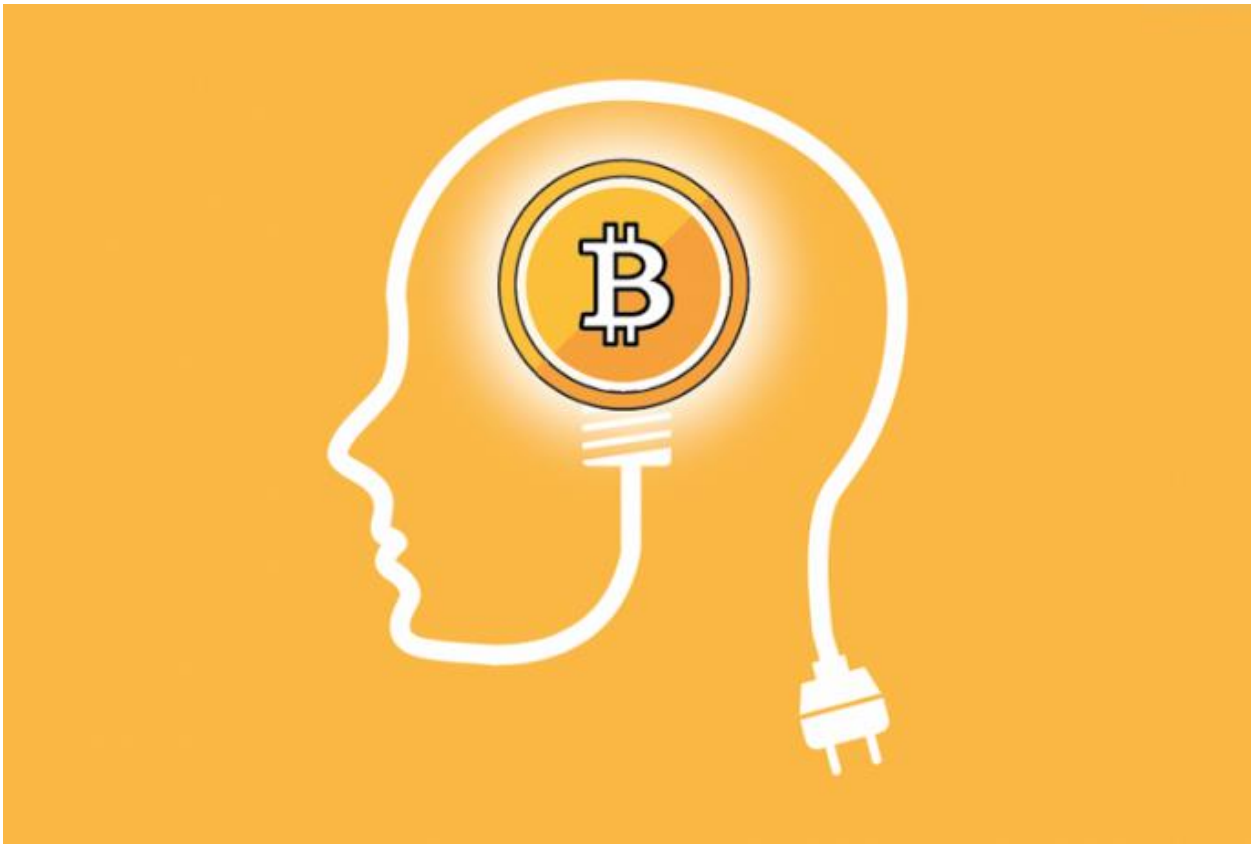
With just a few simple free apps running on a humble Raspberry Pi, anyone can be completely anonymous, have perfect privacy, and ultimate freedom. This means anyone can bypass all governance rules, including your favorite country's government as well. Internet + Bitcoin = Freedom

---

Bitcoin: The Blockchain for Truly Smart Contracts

By Conner Brown

Posted January 15, 2020



Smart contracts sound enticing. The allure of cutting out attorneys, endless paperwork, and exorbitant legal fees is what drew me into learning about cryptocurrency in the first place. Unfortunately, my dreams were shortly crushed. It was clear that reality didn't live up to the advertising hype and "smart contracting platforms" had fundamental problems with the nature of contracts.

Many have encountered these problems and decided smart contracts are something that can never work, I disagree. In fact, Bitcoin has made the proper design choices to make smart contracts possible where others have failed.

In this essay, I will cover the basics of contracts, explain the problems with naive "smart contracting platforms", and finally show how Bitcoin is keeping the dream of smart contracts alive.

Part One: Contract Basics

First, let's cover the basics of a contract. A contract is *an enforceable agreement between consenting parties*. Here is an example:

Alice agrees with Bob to purchase $1000 dollars of coffee beans from him per month for the next 3 years. Alice will pay Bob on the first of each month.

The contract is the agreement between the two parties (Alice and Bob) for the transaction (coffee beans for dollars) and can be digital, written, or even verbal.

The key difference between a contract and a mere promise is that a contract can be enforced by a third party. This third party is often an agent of the law, such as a judge, but can also include private arbitrators, mutual friends, mob bosses, etc. In the event of a_ breach_ (i.e. Alice misses a payment), the injured party can take the contract and evidence to their enforcement authority who will use their abilities to make the injured party whole under the terms of the contract.

Contracts are a necessary part of a functioning economy as they allow individuals to rely on actions of others. Therefore, an entrepreneur can operate a business knowing that the components needed for their product will arrive on schedule. This forms the basis of predictable trading, planning, and specialization. In this sense, contracts are socially scalable as they "overcome shortcomings in human minds . . . that limit who or how many can successfully participate." [1] As more people can rely on the efforts of others without trusting them personally, the entire network of possible economic interaction grows exponentially.

The key feature that makes contracts socially scalable is that **a contract can be entered and executed without supervision.** A merchant may engage in thousands of trades and contracts with others and never need to see a judge to resolve the conflict.

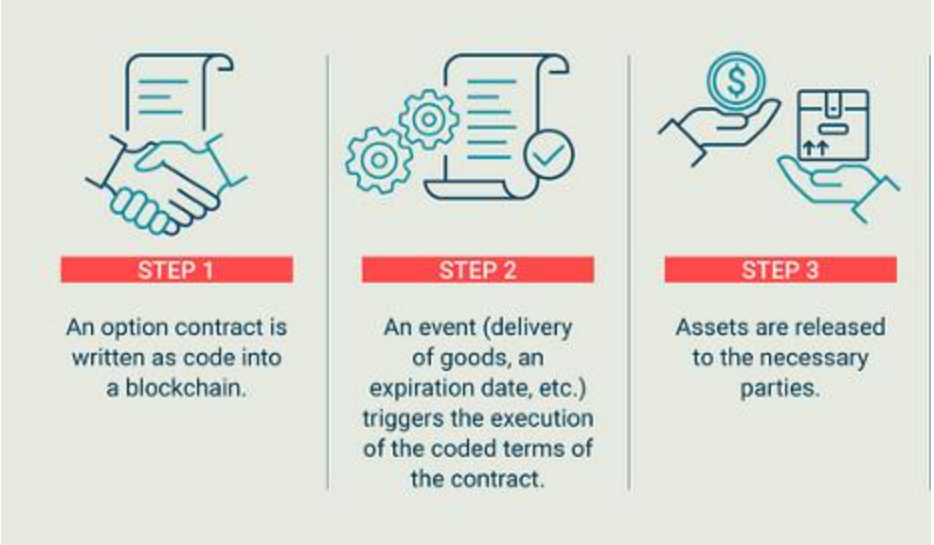
On the contrary, imagine a world where every contract you entered into (i.e. every time you sat down at a restaurant or purchased something from amazon) there had to be a third party overseeing the entire transaction to ensure that everything went according to plan. That would be ridiculous. Transaction costs would be so high that no one would ever use contracts in the first place. The beauty of contracts is not that a third party is present at all times, but that **there can be a third party if needed.** That fallback option is sufficient to generate trust between strangers.

With contracts, we improve the division of labor and add reliability to our world, the cornerstones of economic progress, by replacing the element of trust with enforceable guarantees.

Part Two: The Naive "Blockchain" Approach

Lately, there has been a lot of buzz around contracts. With the blockchain boom of the past decade, the meaning of the term "smart contract" has evolved in reference to the many distributed networks that have sprung up. For the purposes of this article, I will define a smart contract as the enforcement, verification, and performance of an agreement between two parties over a distributed protocol.

If only it were this simple.



The stock image above represents the naive vision for smart contracts. The theory is that one can simply take real world contracts, "put them on the blockchain", and somehow end up with an agreement that is more trustworthy. In this view, (1) there is a contract coded into the network, (2) data from the real world event is then processed by the network, and (3) lastly the network performs an action based on that information.

However, there are major problems with this approach.

1. The Oracle Problem

If your smart contract system is based on information from the physical world, (i.e. title to land, the price of a good, or the delivery of an item) then it must rely on a service known as an oracle that can feed that information to the smart contract system. This is a problem because there is no objective way to know if the physical world corresponds to the internal databases. As a result, services require trusted third parties to supply the information for their contracts — defeating the purpose of using a decentralized network in the first place.

Additionally, problems arise when something happens with a piece of property, but the blockchain is not properly updated. For example, imagine you are storing land titles on a blockchain. What happens if the land is meant to be passed on to family members but the private keys to the land are lost or destroyed? In that scenario, there are two options. Either the ledger is immutable and title is permanently issued to the wrong person, or the ledger can be changed by a third party (i.e. government agent or customer support) to reflect what occurred.

The first scenario means over time the ledger will become increasingly incorrect, and the second demonstrates why a blockchain is unnecessary to begin with . Problems like these are fundamental to their respective networks and demonstrate why smart contracts are not suited for physical world property rights.

2. The Inflexibility Problem

Contracts are never perfect manifestations of the drafters will. Often confusions and misunderstandings occur between parties when drafting. However, when drafting in a smart contract language, there is no room for error. Each word must be drafted from fully-defined computer terms which can be processed by the smart contract platform.

Jeremy Sklaroff explores this problem in a fantastic paper titled ***Smart Contracts and the Cost of Inflexibility.***[2] Smart contract platforms claim to reduce “inefficiency” by removing traditional language; however, Sklaroff demonstrates this removal unfavorably increases transaction costs. Hard coded contracts must be rigid and purely self-referential. This means that both parties must **fully and precisely define all expected and possible future states of the contract without traditional language.** The possibilities for even a simple contract of coffee bean delivery are dizzying.

It is also common when drafting contracts to reference conventions, customs, and terminology specific to a certain trade, significantly reducing the time required in drafting contract. These commonly understood substitutes would also not be recognized under a smart contract and would need to be entirely defined.

In sum, human activities require human constructs. Natural language has an interpretive richness and flexibility that cannot simply be replaced by computer logic.

3. The Breach Problem

Contracts are often complex agreements with a variety of terms and requirements. Many times whether or not the terms of an agreement have

been breached is up for debate. Bob may believe that he acted in accordance to the terms of the contract, however Alice may interpret things differently. For example, what happens if the coffee beans being delivered are the wrong size or type? Should this constitute a punishable breach or a negligible difference? Hopefully this would be negotiated ahead of time, but these problems are often difficult to anticipate.

To make matters worse, breaches are not always intentional or harmful. With standard contracts, a counterparty can give an explanation of their mistake and the injured party can choose take the case to the courthouse, or simply let it slide. This is because a technical violation is not always a detrimental violation.

To illustrate, let's return to the contract between Alice and Bob. There may be a month where bob delivers the wrong type of coffee bean for Alice. He calls her ahead of time, informs of her of the mix-up, but tells her he'll make up for it by giving her 25% off that order. Alice thinks this is a great idea. She will get a discount on this month's delivery and can use these different coffee beans as a "limited time offer" in her store to boost sales.

Informal modifications like these are important and possible because they operate in the malleable world of human interaction. On the other hand, a trustless smart contract would simply see the wrong goods were delivered and penalize the offending party — a costly result that could have been avoided.

This lack of selective enforcement is another massive burden to smart contracts where the flexibility of standard contracts is a feature, not a bug.

4. The Enforcement Problem

As mentioned above, the difference between a contract and a promise is that the third party to an agreement can enforce the terms of the contract. But what about a smart contract? If there is a smart contract for a delivery of coffee beans and Bob doesn't deliver, who will enforce it? A blockchain is decentralized and has no jurisdiction or ability to affect physical objects, naturally this creates a problem with getting people to be good on their promises.

Defenders of blockchain enforcement generally take one of two positions. First, one might argue that the blockchain can't enforce it, but it could be used as proof in a court of law. In that case however, you're still falling back on the same state institutions to enforce the contract. A standard contract would have the same assurances and more privacy!

The alternative to this is a staking model. To use a smart contract, a user would need to post collateral that can be auctioned off in the event of the

breach. This also brings its own problems — it's expensive! Posting collateral for every contract brings its own opportunity costs, especially if dealing with multiple contracts on multiple services.

Neither of these solutions is appealing, and brings us back to the question of why use a blockchain for contracts in the first place?

5. The Scalability Problem

As explained above, a key element of contracts is their ability to scale by providing third party monitoring on an ***as needed basis***. However, smart contracting platforms such as Ethereum, Tron, and EOS, have decided to ignore this basic principle. By allowing users to upload contracts directly to the base layer, any contract that individuals create must be verified and constantly monitored by all other validators of the network.

Their results have been disappointing and predictable. Despite gaining little traction or active users, the major smart contracting platforms are already incredibly difficult to download, verify, and stay synced. This timeless piece by StopAndDecrypt does a fantastic job exploring the implications of this design choice which applies to blockchains with expressive languages on the base layer such as Ethereum, Tron and EOS.[4]

Despite claiming to be innovative compared a simpler protocol like Bitcoin, complex base layer scripting is a step backwards. By requiring all validators to verify the entirety of every smart contract on these platforms, the inevitable result is centralization and falling right back into the realm of trusted third parties they claim to remove. Contracts simply don't work that way.

Part Four: A Judge Like No Other

After seeing these problems, it is tempting to think they cannot be overcome. While most uses of the term "smart contracts" are merely fluff, we shouldn't abandon the concept entirely. In fact, Bitcoin has already solved these problems with the Lightning Network.

The Lightning Network is a system of peer-to-peer payment channels that operate on top of the bitcoin protocol. A brief

introduction to Lightning can be found here.

In broad terms, a Lightning Network interaction works as follows. Two parties communicate with each other that they would like to enter into an agreement to open a payment channel. Both parties sign a commitment transaction which memorializes their mutual assent to the agreement and records it on the Bitcoin blockchain. Both parties abide by rules of the Lightning Network protocol, which form the boundaries of their cooperation. After transacting for a period of time, the parties can choose to terminate the contract by signing and publishing a final mutual transaction. In the event that one party tries to break the rules of the network and steal their counterpart's funds, the injured party can publish proof to the bitcoin blockchain and prevent the theft.

These elements line up perfectly with traditional notions of contract, and overcome the problems listed above.

1. **Terms:** The rules of the LN protocol itself are akin to the terms of a contract where both parties to the agreement must act accordingly.
2. **Signing:** Publishing the commitment transaction is a way of signing and agreeing to the terms of the contract.
3. **Breach:** The contract is breached if a party violates the terms of the lightning contract, and injured parties can essentially "have their day in court" by publishing cryptographic evidence to the base chain.
4. **Enforcement:** Finally, the bitcoin protocol acts as a virtual judge, logically evaluating the evidence before it and transferring funds to the appropriate party.

The lightning network completely sidesteps the traditional pitfalls of smart contracts by isolating the contract system in a virtual closed loop. A smart contract on lightning lives and dies entirely in the digital realm. The oracle, enforcement, and breach problems only arise with dealing with the gray world of material objects and actions.

There is also a strong flexibility inherent in the network as the agreements are peer-to-peer like traditional contracts. Each set of partners chooses which terms they wish to be bound by. While there are generic lightning contracts, (i.e. the default build of Eclair or LND), these terms can be tweaked to fit the needs of the parties. For example, Bitrefill recently opened the first 1BTC channel by changing the default channel size limit. Contract flexibility will continue to improve as protocol upgrades such as Schnorr Signatures and SIGHASH_NOINPUT are implemented. The eltoo proposal is just one example.

With all this being said, perhaps the most important part of Lightning is its understanding of social scalability. As mentioned earlier, what makes contracts so powerful is that a judge *is not necessary for a transaction*, but

only as a backup in the event of a breach. Other "smart contract platforms" such as Ethereum and Tron completely miss this fundamental insight of contracts. Instead, they opt for a model where the "judge" (i.e. the blockchain) sits over the shoulder and watches every single transaction as it occurs.

The design of the lightning network fully grasps this contracts concept. With lightning, millions of transactions can take place between two individuals without needing the judge at all. This provides two obvious benefits, reducing transaction costs with users of the network, and increasing the privacy of those entering into contracts. At this point, the size and growth of the network is somewhat unknown because many channels are private. However, in the event that something goes wrong, the benevolent bitcoin judge can step in, evaluate, and resolve the dispute.

Lastly, its important to note that the Lightning Network is only the first of many of such examples. POWSWAP by Jeremy Rubin offers a similar type of smart contract for hashrate derivatives, and Lot 49 by Richard Myers for mesh network messaging. These innovative smart contracts are not being built on other chains because of their "expressiveness" or "turing-completeness", quite the opposite. They chose bitcoin for its simplicity.

The blockchain space often touts complex base layer scripting as what is best for smart contracts — but they fail to recognize simplicity is crucial for smart contracts by forming the basis of predictable execution. In this light, bitcoin's simplicity and security shines through.

Going forward, I expect the smart contracts with the most usage and value to be built in a similar way — leveraging bitcoin as their virtual judge of choice.

Conclusion

Lightning is the first truly smart contract. By tackling the problems plaguing other networks, Lighting has prevailed as a shining example of what is possible on Bitcoin and paints a bright future for smart contract innovation on the network.

I would like to thank Bitcoin Lawyer, Jeremy Sklaroff, and Nick Szabo for their ideas, and the Cato Institute for hosting me to do this research.

References:

1. Szabo, Nick. Money, Blockchains, and Social Scalability, 9 Feb. 2017, unenumerated.blogspot.com/2017/02/money-blockchains-and-social-scalability.html.
2. Sklaroff , Jeremy. "Smart Contracts and the Cost of Inflexibility ." *University of Pennsylvania Law Review* , vol. 166, 2018, pp. 263–303.
3. Id. at 264.

4. For more recent evidence of SAD's concerns coming to fruition, I recommend this thread by Eric Wall documenting the herculean efforts to sync a full node on Ethereum.

Efficient Market Hypothesis and Bitcoin Stock-to-Flow Model

By PlanB

Posted January 17, 2020

Would you pick up that bitcoin or follow EMH?

Signature: HwdQggZNa6LBEI8XB+yrDWKNQGALYiFT0X745UoGXAuHefm0bXG70cYYPAHNe1tX/K3/z75J0aQjkl4zXZHL7Eo= Message: Efficient Market Hypothesis and Bitcoin Stock-to-Flow Model Address: 1PRoNLcWHzM8DuKpGE4YM9hb1PjSEnWRpn

Introduction

Bitcoin Stock-to-Flow (S2F) model was published in March 2019 [1]. The model has been well received by bitcoiners and investors. Many analysts have verified the cointegrated S2F model and confirmed bitcoin price forecasts [2][3][4].

The S2F model also received critique. The best steel man argument against the model comes from the Efficient Market Hypothesis (EMH). The argument states that the model is based on publicly available information (S2F, bitcoin's

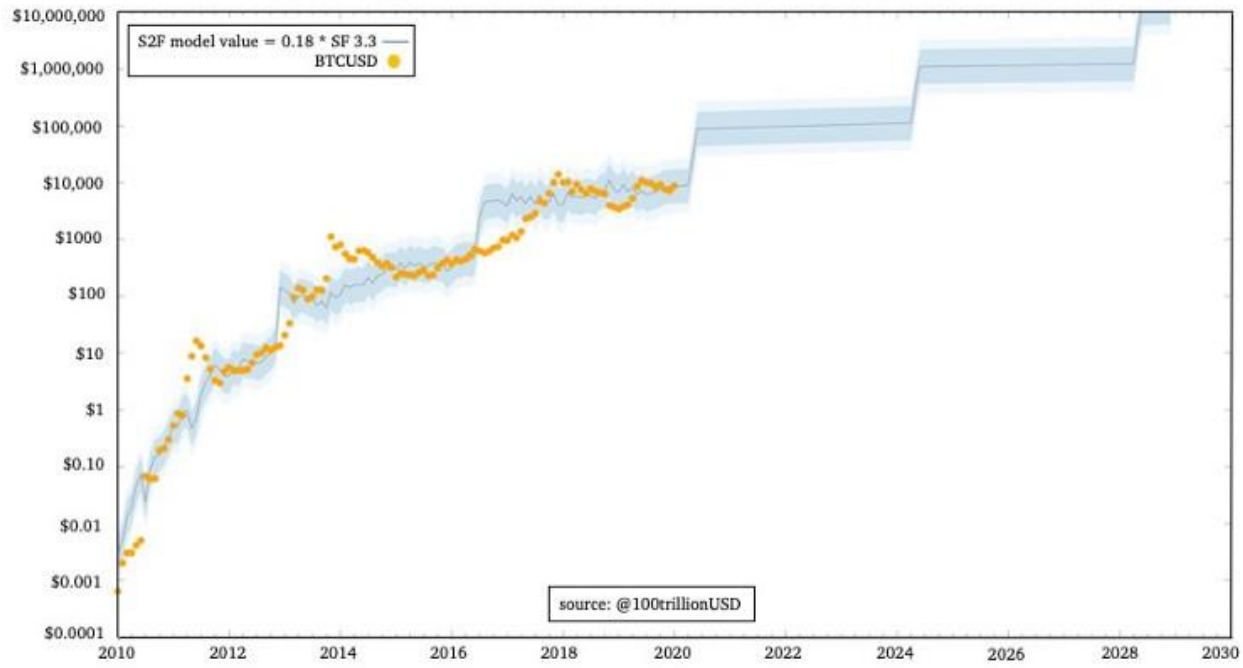
supply trajectory) and therefore the analysis and conclusion must be already priced in.

In this article I share my point of view on S2F model and EMH. I analyze arbitrage opportunities, risk & return model and derivatives markets.

Stock to Flow Model

S2F model was published as a bitcoin valuation model, inspired by Nick Szabo's concept of unforgeable scarcity and Saifedean Ammous' analysis of S2F [1][5][6]. S2F is a measure of scarcity. The power law relation between S2F and bitcoin price over time captures the underlying regularity of bitcoin's complex dynamic system of network effects as described by Trace Mayer [7].

S2F model is a power law function fitted on Oct 2009 —Feb 2019 *monthly* data: BTC price =0.4*S2F ^3 (where S2F=1/inflation rate). A later model on 2009–2019 _yearly_ data has higher forecasts: BTC price =0.18*S2F ^3.3



Nick Phraudsta was the first to verify (or better "not falsify") the S2F model, and he added cointegration analysis, indicating that the correlation is likely not spurious [2]. Marcel Burger verified both S2F model and cointegration, with several addition statistical tests[3]. Manuel Andersch was the first institutional investor (BayernLB) to verify S2F model and cointegration [4].

Efficient Market Hypothesis

EMH is a well known theory in financial economics. EMH is based on ideas of Friedrich Hayek (1974 Nobel prize) and others. According to Hayek markets are information processing systems, delivering the best possible price discovery [8].

EMH is formally described by Eugene Fama (2013 Nobel prize) and comes in three flavors [9]:

1. Weak EMH: historical price data is already priced in and cannot be used to make profits. Technical Analysis (TA) and Time Series Analysis (TSA) do not work.
2. Semi-strong EMH: public news from media outlets like MSNBC, Bloomberg, WSJ and research companies is already priced in and cannot be used to make profits. Fundamental Analysis (FA) does not work.
3. Strong EMH: even inside information can not be used to make a profit, because ***all*** information is already priced in.

Most investors and economists agree that modern financial markets are reasonably efficient (i.e. they accept weak and semi-strong EMH), however they reject strong EMH.

Following EMH, S2F model should be priced in, because it is based on publicly available data (S2F).

Risk & Return

To be honest, I have never used EMH directly in my 20+ years experience as an institutional investor managing a multi-billion Euro balance sheet. In practice we ***assume*** EMH, and ***use*** a risk & return model.

Assuming EMH

Some people argue that bitcoin markets are not efficient, but I do not agree. In the old days you could buy bitcoin at one exchange in USD and sell it shortly afterwards at another exchange in EUR or JPY and convert it back to USD at a profit, arbitrage was possible. Those days are gone, as the table below shows (13 Jan 2020, 20:00 GMT prices):

BTCUSD = 8100 BTCEUR = 7300 BTCUSD/BTCEUR = 8100/7300 = 1.11 EURUSD = 1.11

BTCJPY = 885.000 BTCJPY/BTCUSD = 885.000/8100 = 109 USDJPY = 109

Perhaps there is still some money to be made with big computers, fast communication lines and high-frequency trading (HFT) algorithms, but there are no easy arbitrage opportunities.

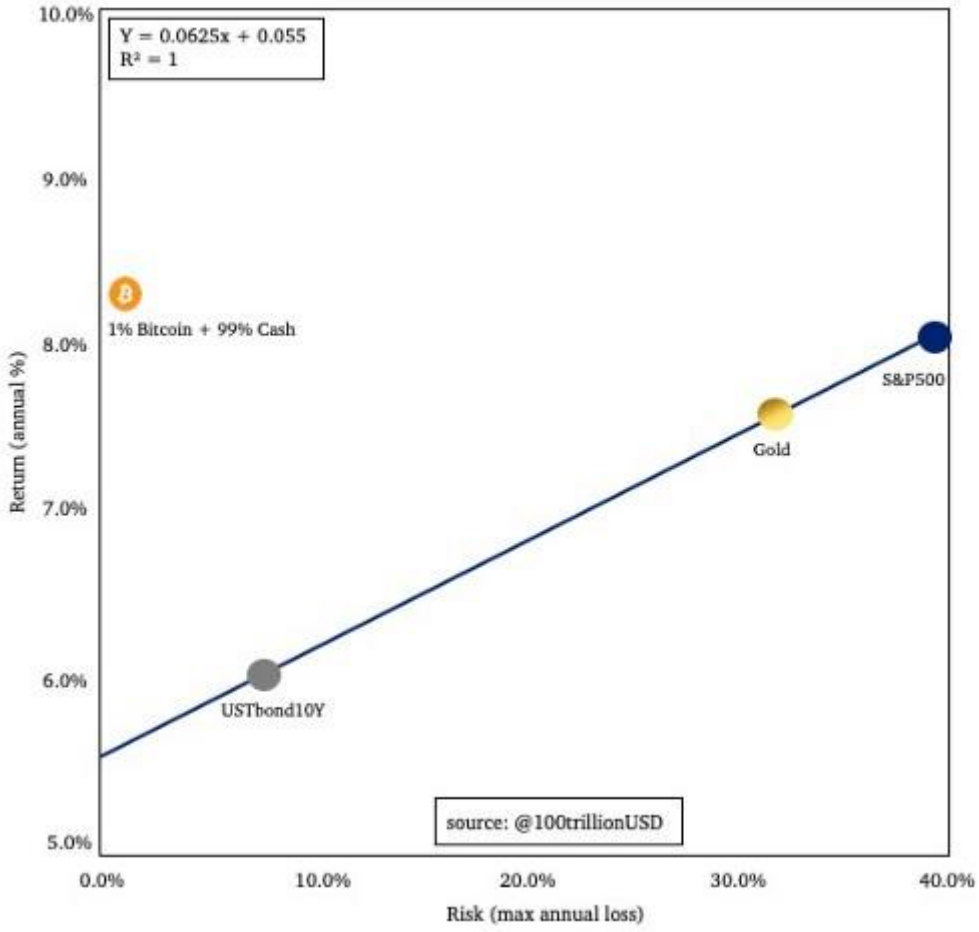
We can safely assume that the $150B bitcoin market with $10B daily transactions is reasonably efficient.

Risk & Return Model

Assuming EMH does not mean that you can not make money. You just have to take risk. EMH and non arbitrage lead us to risk & return models.

Harry Markowitz (1990 Nobel prize) introduced an early risk & return model with his famous Portfolio Theory (PT)[10]. William Sharpe (1990 Nobel prize) published his well known Capital Asset Pricing Model (CAPM)[11]. According to Markowitz and Sharpe all returns can be explained by risk.

This is a simplified risk & return model (without correlation or exotic math):



Bond, Gold, Stocks: 1955–2019 data. Bitcoin: 2009–2019 data.

It is crucially important to understand this chart, so let's dive into it.

The x-axis of this chart is risk (maximum annual loss) and the y-axis is return (average annual return).

The chart shows three classic assets: bonds, gold and stocks. Bonds have the lowest risk 8% and the lowest return 6%. Gold has higher risk 33% and higher return 7.5%. Stocks have the highest risk 40% and the highest return 8%.

Key insight is that returns can be explained by risk alone, consistent with EMH. If you encounter an asset above the line, a first reaction could be that it is a great investment opportunity. A better reaction (from an EMH and non arbitrage point of view) would be that it is too good to be true. We are probably missing risks (or have miscalculated risk) and should try to bring the asset back on the line. Quantifying risk (volatility) is difficult, and indeed the expertise of quants of financial institutions. If an investor calculates that risks are lower than the market prices in, and if he exactly knows why the asset is above the line, then and only then should he decide to invest.

Bitcoin is literally "off the chart": 200% return, 80% risk. Because I can not plot it on the chart, I resized it to a 1% bitcoin plus 99% cash investment. This bitcoin investment is far above the line: 8% return, 1% risk (note that you can't lose more than 1%, even if bitcoin drops 99%, because you only invest 1%). So my first reaction is: the market sees risks that are not in the data. Here is a list of some possible risks:

- Risk that bitcoin dies
- Risk of governments making bitcoin illegal and prosecuting developers
- Risk of fatal software bugs
- Risk of exchange hacks
- Risk of 51% attacks by centralized miners
- Risk of miner death spiral after halving
- Risk of hard forks

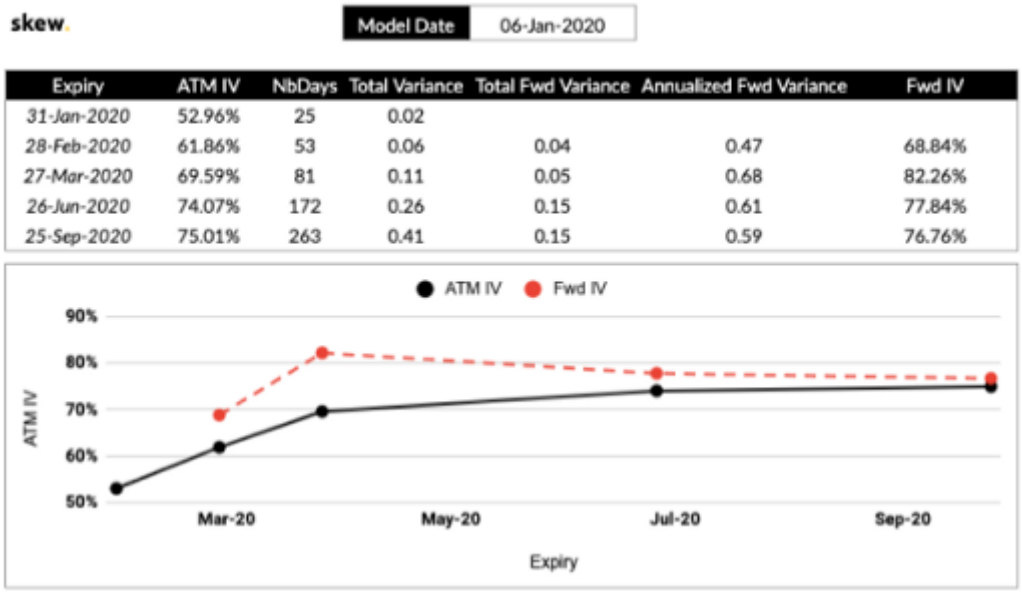
From an EMH and risk & return perspective, all these risks should be in the price data. But these risks are not in the data. According to EMH and the risk & return formula in the chart, 1% risk should give 5.5% + 6.2% * 1% = 5.6% return. And the data shows that 1% bitcoin + 99% cash had 8% return last 11 years.

It seems that these risks have been overestimated by the market, and that bitcoin really was a great investment opportunity, in line with S2F model.

Derivatives markets

Let's look at what derivatives markets are telling us about the future.

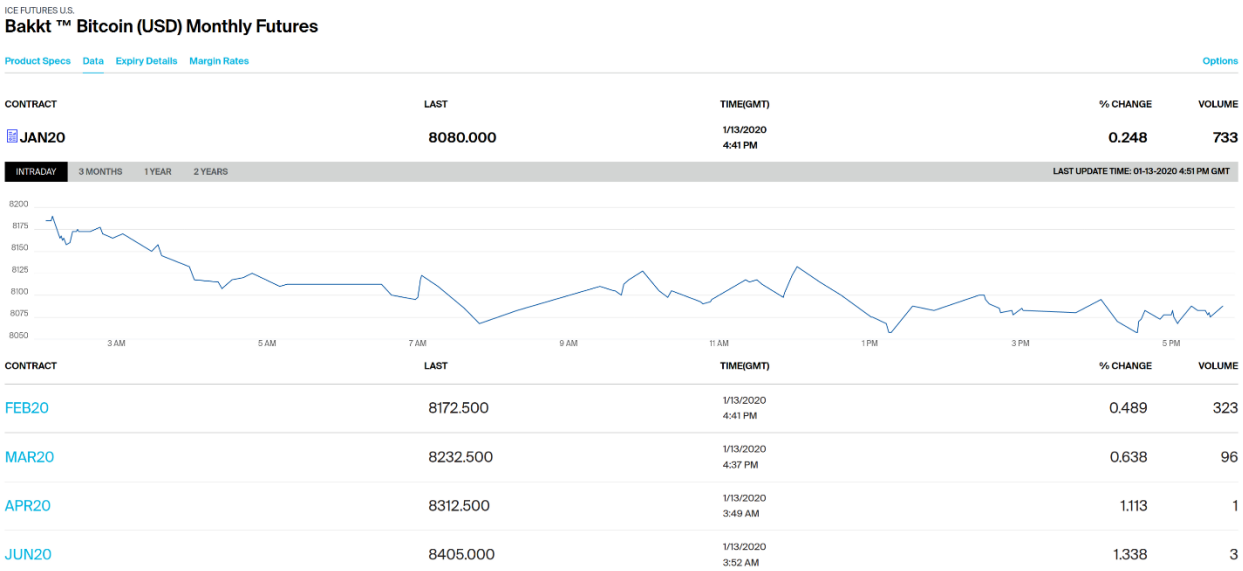
Option markets show no spike at or after next halving:



Expiry	ATM IV	NbDays	Total Variance	Total Fwd Variance	Annualized Fwd Variance	Fwd IV
31-Jan-2020	52.96%	25	0.02			
28-Feb-2020	61.86%	53	0.06	0.04	0.47	68.84%
27-Mar-2020	69.59%	81	0.11	0.05	0.68	82.26%
26-Jun-2020	74.07%	172	0.26	0.15	0.61	77.84%
25-Sep-2020	75.01%	263	0.41	0.15	0.59	76.76%

Source: https://twitter.com/skewdotcom

Same story for futures market: slightly higher prices in the future, but no spike at or after the halving, indicating nothing special will happen at the halving:



Source: https://www.theice.com/products/72035464/Bakkt-Bitcoin-USD-Monthly-Futures/data?marketId=6137544

This is interesting because S2F model forecasts much higher prices after the halving. How should we interpret this?

I think the simple answer is that the market currently overestimates future risk, like it overestimated risk the last 11 years. The efficient bitcoin market not only discounts the fundamental value of scarcity (S2F model), but also all these risks:

- 42% of investors see bitcoin futures as the biggest risk (whales and governments manipulating the price of bitcoin with 'paper bitcoin', spoofing and wash trades).
- 16% still fears miner capitulation after the halving.
- 15% fear selling pressure from scams.
- I know from discussions with institutional investors that their biggest fear is government making bitcoin illegal.
- Another risk frequently mentioned by institutional investors is "the next bitcoin", a new (government/central bank backed) coin replacing bitcoin.

Note that without all these risks bitcoin's value would be much higher, possibly in line with S2F model.

As time progresses, some of these risks will not materialize and disappear from the list. Take miner capitulation for example. I do not think miner capitulation is a big risk, but 15% of investors thinks it is. If hashrate does not decrease after the next halving, the risk of miner capitulation disappears and bitcoin price will rise because the risk is gone.

Conclusion

Bitcoin S2F model was introduced in March 2019 and verified by many others.

EMH implies that S2F and the model forecasts should be already priced in by the market, because S2F model uses publicly available S2F data.

Current bitcoin markets are indeed reasonably efficient because easy arbitrage opportunities are not possible.

Historical risk & return data of bonds, gold, stocks and bitcoin, shows that bitcoin markets overestimated risk. Bitcoin return was not in line with risk, but very much in line with S2F model. Bitcoin options and futures markets do not expect rising prices at or after next halving. It is possible that markets still overestimate future risks.

My conclusion is that bitcoin markets are indeed reasonably efficient and price in S2F model, but also overestimate risk. Therefore, I prefer using S2F model over a classic risk & return model to forecast future bitcoin price.

So I assume EMH ***and*** I would definitely pick up that bitcoin!

References

[1] PlanB@100trillionUSD, ***Modeling Bitcoin's Value with Scarcity***, Mar 2019

[2] Nick@phraudsta, ***Falsifying Stock-to-Flow As a Model of Bitcoin Value***, Aug 2019

[3] Burger@BurgerCryptoAM, ***Reviewing "Modelling Bitcoin's Value with Scarcity"***, Sep 2019

[4] Mannuel Andersch (BayernLB), ***Is Bitcoin outshining gold?***, Sep 2019

[5] Nick Szabo, ***Bit Gold***, 2008

[6] Saifedean Ammous, ***The Bitcoin Standard: The Decentralized Alternative to Central Banking***, 2018

[7] Trace Mayer, ***The Seven Network Effects of Bitcoin***, 2015

[8] Friedrich Hayek, ***The Use of Knowledge in Society***,1945

[9] Eugene Fama, ***Efficient Capital Markets: A Review of Theory and Empirical Work***, 1970

[10] Harry Markowitz,***Portfolio Selection***, 1952

[11] William Sharpe, ***Capital Asset Prices: A Theory of Market Equilibrium under Conditions of Risk***, 1964

Bitcoin Backups

By 6102

Posted January 18, 2020

A simple (worst case) evaluation of MultiSig wallet backups by 6102bitcoin

Consider a bitcoin wallet with a total of **n** keys, of which **m** are required to spend. **X** backups are made per key. When making bitcoin backups for this wallet there are three important things to consider;

1. Number of backups

We wish to minimize the number of backups required, predominantly because placing backups in a secure location can be time consuming, and checking backups are in place increases at least linearly with the number of backups required. The total number of backups required is equal to **nX**.

2. Risk of Theft

A thief can steal the bitcoin with access **m** backups (*in the worst case scenario*). Let this be the **'theft tolerance'** of the setup**.**

With regard to the risk of theft, unless you are under targeted attack the **theft tolerance** of your backups is critical, rather than the % of keys the thief must access.

Note: Users who may be under targeted attack may prefer to evaluate the percentage of keys which must be accessed by the thief rather than the number of keys.

3. Risk of Inability to Recover

Losing access to a minimum of **X(n-m+1)-1** backups does not impinge on the ability to recover the bitcoin. Let this be the **'minimum backup redundancy'**. Losing more than this number of backups could potentially make recovering the bitcoin impossible.

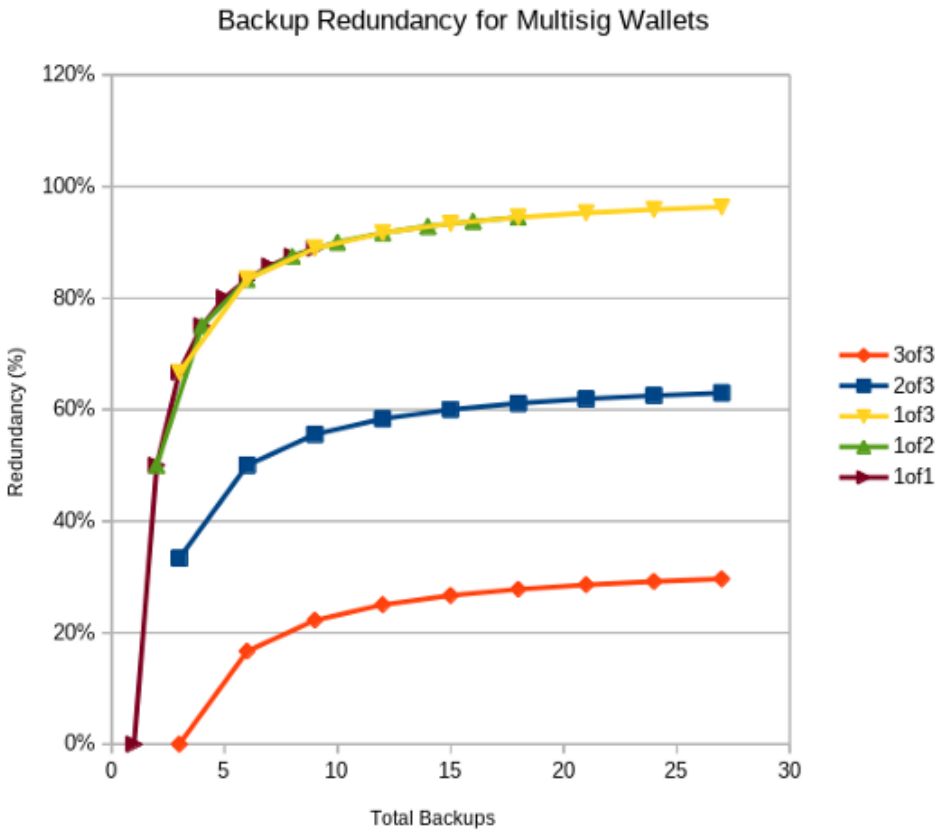
With regard to **minimum backup redundancy** the % of keys that can be lost is considered more important than the actual number of keys.

Tabulated Results

With this in mind we present an overview table of different m-of-n wallet configurations with different numbers of backups per key (**X**).

	Backups per Key	Theft Tolerance	Total Backups	% Redundancy	Comments
1of1	1	1	1	0%	
	2	1	2	50%	
	3	1	3	67%	
	4	1	4	75%	
	5	1	5	80%	
	6	1	6	83%	
	7	1	7	86%	
	8	1	8	88%	
	9	1	9	89%	
1of2	1	1	2	50%	1ofN Wallets: Theft tolerance is 1 – A single backup theft results in the thief being able to steal your bitcoin. Those with backups listed in this category should ensure that backups are encrypted or use a passphrase. For setups with the same total number of backups 1ofN wallets have the same % redundancy (worst case scenario).
	2	1	4	75%	
	3	1	6	83%	
	4	1	8	88%	
	5	1	10	90%	
	6	1	12	92%	
	7	1	14	93%	
	8	1	16	94%	
	9	1	18	94%	
1of3	1	1	3	67%	
	2	1	6	83%	
	3	1	9	89%	
	4	1	12	92%	
	5	1	15	93%	
	6	1	18	94%	
	7	1	21	95%	
	8	1	24	96%	
	9	1	27	96%	
2of3	1	2	3	33%	2of3 Wallets: The Thief must steal at least 2 backups to be able to seal your bitcoin. This analysis assumes worst case (that the thief steals as few backups as is required). Significant benefit increasing backups per key from 1 to 2 (increases redundancy from 33% to 50%).
	2	2	6	50%	
	3	2	9	56%	
	4	2	12	58%	
	5	2	15	60%	
	6	2	18	61%	
	7	2	21	62%	
	8	2	24	63%	
	9	2	27	63%	
3of3	1	3	3	0%	3of3 Wallets: The Thief must steal at least 2 backups to be able to steal your bitcoin. This analysis assumes the worst case (that the thief steals as few backups as is requireed). Very low redundancy even with a total of 27 wallets (9 backups per key).
	2	3	6	17%	
	3	3	9	22%	
	4	3	12	25%	
	5	3	15	27%	
	6	3	18	28%	
	7	3	21	29%	
	8	3	24	29%	
	9	3	27	30%	

Redundancy (%) vs Total Backups



When comparing the redundancy in terms of % backups you can afford to loose vs the total number of backups required to place it is striking how limited the redundancy of a 3of3 scheme is, even with 9 backups of each key.

If course, this is because we have assumed that that the 'worst case scenario' unfolds (e.g. for a 3of3 every one of the keys lost is the same key) which is very unlikely. This is done to be prudent, however future work could incorporate the statistical likelihood of these events, rather than assuming worst case scenarios.

Note: You MUST have access to all public keys with multisig.

What Crypto "Token Velocity Theorists" Can Learn From Austrian Economics

By Stephan Livera

Posted January 21, 2020

In the "crypto" world, there are theorists mistakenly applying Irving Fisher's equation of exchange without knowledge of Austrian critiques of the idea. Understanding why Austrian economists are critical of MV = PT might help these theorists avoid these errors in reasoning. (These theorists include Kyle Samani, Chris Burniske, and Vitalik Buterin among others, hereafter referred to as "crypto velocity theorists.")

Quick Overview of Terms in the Fisher Equation of Exchange

In the equation, M = the money supply, V = the velocity of money, or the average number of times a currency unit changes hands per year, P = the average price level of goods during the year, and T = an index of the real value of aggregate transactions. In the MV = PQ formulation, Q = an index of real expenditures and P × Q = nominal GDP.

How Are Crypto Velocity Theorists Misapplying the Theory?

Crypto velocity theorists seem to believe that the current structure of crypto tokens (non-bitcoin ones) has a velocity that is too high. They assert that somehow by using the protocol to force holding or "lock up" periods the velocity of the token can be slowed down, enabling more sustainable value capture for a crypto protocol. There are various "tokenomics" ideas being proposed to achieve this slowdown in velocity, such as profit share mechanisms, staking functions to lock up the token, or gamification to encourage holding. But are these mechanisms sustainable in the longer term? Distinguished against these ideas is the simple concept of bitcoin, a token and monetary network created to replace fiat money. Bitcoin can justifiably hold a place in a person's cash balance under a theory of speculative demand based on its monetary characteristics. In this case, the more relevant reference is Carl Menger and the argument around marketability or saleableness, not the quantity theory of money and associated equation of exchange.

How Do Prominent Austrian Economists Critique the Quantity Theory of Money?

Austrian economists reject the quantity theory of money, which is too mechanistically focused on the nominal quantity and not on real subjective valuations by individuals. Murray Rothbard and Joseph Salerno point out many problems. In ***Man, Economy, and State***, Rothbard points out a serious conceptual flaw:

At any one time there is a given total stock of the money commodity. This stock will, at any time, be owned by someone. It is therefore dangerously misleading to adopt the custom of American economists since Irving Fisher's day of treating money as somehow "circulating,"…There is, actually, no such thing as "circulation," and there is no mysterious arena where money "moves." At any one time all the money is owned by someone, i.e., rests in someone's cash balance.

In other words, Rothbard shows that velocity is a rather meaningless idea. Further, he points out that different goods cannot be meaningfully added together, demonstrating the absurdity of doing so:

How can 10 pounds of sugar be added to one hat or to one pound of butter, to arrive at T? Obviously, no such addition can be performed, and therefore Fisher's holistic T, the total physical quantity of all goods exchanged, is a meaningless concept and cannot be used in scientific analysis.

Joseph Salerno levels his own critique against the idea of the quantity theory of money also, identifying where it is vacuous in his article "A Simple Model of The Theory of Money Prices":

Let's begin with the Quantity Equation as conventionally stated: MV = PQ. Our simple model above reveals that the real action is on the right side of the equation….The mechanical passing of a specific sum of money from one hand to the next in exchange, that is, "spending," is completely governed by the money price that has been antecedently established by the exchanging parties. Thus the money spent is merely an outcome of the pricing process and in no sense a causal factor. In other words, the aggregate flow of money spending is determined by the value of money and not the other way around.

Salerno demonstrates that individuals' subjective valuations drive prices all along, not the quantity of money in a mechanistic sense. So, in the end, "Tokenomics" and attempting to "game" token velocity downward to satisfy an erroneous Fisher equation of exchange is misguided. We should aim to understand bitcoin and cryptocurrencies from an Austrian monetary theory standpoint. Menger's ***On The Origins of Money*** and Ammous Saifedean's ***The Bitcoin Standard*** are more relevant places to begin. Saleableness is more important than velocity.

Bitcoin is perfectly suited for value time travel

By Acrual

Posted January 22.2020

Whenever an oil pipe is not enough, you need to store it as cheap as possible

I can't stop thinking about the striking similarities and analogies among commodities, energy markets, Bitcoin mining and Bitcoin itself.

If you think about it, every single commodity, in order to satisfy a need, needs to be transported wherever it is demanded, therefore it needs to be transported over space.

But whenever a bottleneck arises in the transportation capacity or if the demand doesn't match in terms of time that of supply, you need to make it travel through time, that is, to use proper storage, minimizing deterioration of this commodity.

Transportation and storage are two sides of the same coin. If transportation's throughput is limited, storage will need to be large. With most commodities, this is the case. For example, harbours world wide are packed with warehouses where commodities are stored waiting for an empty ship to be available.

If on the other hand storage is limited, as it is the case of electricity, transportation will need to be large (also known as the grid) otherwise you get blackouts (frequently electricity supply shocks).

Commodity money has the exact same considerations: you need it to be good to travel through space and time (and scale, to follow Menger's own words)

This is where Bitcoin excels: it's extremely low cost of storage (taking into consideration its low maintenance, low to zero inflation, zero deterioration, etc...) make it "**especially well suited for time travel**". No other kind of money except for gold is as good as Bitcoin for value time travel.

Interestingly, most wealth worldwide demands time travel rather than space travel if you compare how much narrow money is worth (good for space travel) with everything else (real estate, gold, financial products, offshore money, etc...). The latter is orders of magnitude larger. Things that are stored for long periods of time are exchanged less frequently, which means the supply is smaller. If the demand is large enough (and demand for the utility of exchange definitely is), the price will be very large.

But this shouldn't be surprising as the time of a human life is the most scarce resource of all. Our demand to maximize our well-being has as its most important limitation the time we have to achieve things in life. You could argue that with unlimited time, we should be able to satisfy all our needs without the need for cooperation.

But the fact our time is limited can only be solved with a way to make value travel for as low a cost as possible. That is what money is all about. We have never in history had an opportunity to fight limited human time as we currently have with Bitcoin. Unless you agree with the keynesian views that expenditure is all that matters, the ability to save properly and securely over time should help an unprecedented level of progress.

For energy commodities, it is coincidentally interesting that the competitor for its transportation and storage is precisely Bitcoin mining, which turns an energy delivery standard such as electricity into a value delivery standard such as money. That is, it turns one standard (energy) into another (value)

It should blow your mind as much as if I told you I have a device that turns weight into length for example.

This is a topic I'm most interested in and if you have ideas or even theories on how all of this could be linked together, I can't wait to read your comments either here or in my twitter account (@acrual)

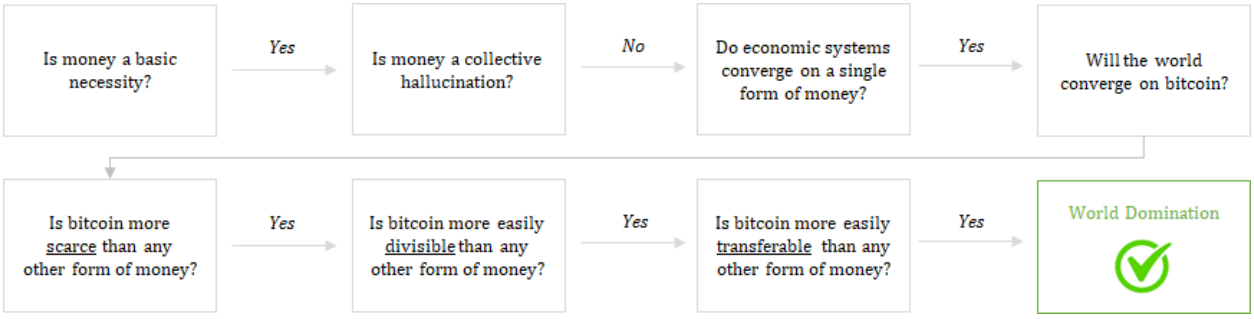
Bitcoin Obsoletes All Other Money

By Parker Lewis

Posted January 24, 2020

When it comes to bitcoin adoption, there are generally two rules that never seem to fail. Everyone always feels late, and everyone always wishes they had bought more bitcoin. There are exceptions to every rule, but bitcoin has an uncanny ability to screw with the human psyche. It turns out that 21 million is a scarily small number, and it actually becomes smaller as more individuals come to understand that the fixed supply of bitcoin is credibly enforced and that monetary networks converge on a single medium. Demand for bitcoin is driven by the credibility of its monetary properties and the convergent nature of money, but increasing demand for bitcoin reinforces the scarcity of bitcoin's fixed supply. As it does, bitcoin becomes more valuable as a monetary medium. While this becomes evident the further down the bitcoin rabbit hole one travels, it is not uncommon for individuals on the periphery to be overwhelmed by the sheer number of cryptocurrencies. Sure, bitcoin is in the "lead" today, but there are thousands; how do you know bitcoin is not MySpace? How can you be sure that something new doesn't overtake bitcoin?

It may sound crazy to believe that bitcoin will be the dominant global currency, and it likely would be if evaluating the possibility from a top-down, probability-weighted perspective. Today, bitcoin is one of a thousand-plus competing digital currencies that all look the same on the surface. Its purchasing power of $150 billion is a drop in the bucket compared to the global financial system which supports $250 trillion of debt. Gold alone has a purchasing power of $8 trillion (50 times the size of bitcoin). What are the chances that an 11-year old internet sensation rises from the ashes of the 2008 financial crisis and goes from nothing to becoming the dominant global currency? The idea sounds laughable, or at the very least, it appears to be too low of a probability to warrant consideration. However, when starting from the bottom-up and developing conviction around a few foundational principles, the noise of a thousand cryptocurrencies fades to the background. When added together, just a few foundational principles create simplicity and clarity around what once may have seemed too complex to possibly discern. If someone had to evaluate one thousand possibilities to come to the right solution, it may not be practical or possible. But if you could eliminate 999 of those possibilities based on one, or a few starting first principles, it then becomes more practical to arrive at a coherent answer.



This is the roadmap to cutting out the noise and focusing on what really matters. Individuals may come to different conclusions concerning any of these questions, but this is the path to consider when attempting to understand why bitcoin consistently outcompetes all other currencies and whether it will continue to do so. Money is a basic necessity, but it is not a collective hallucination, nor is it a shared belief system. Individuals adopt bitcoin because it possesses unique properties that make it superior as a form of money relative to all other currencies. Because money is a solution to an intersubjective problem, monetary systems tend to converge on a single medium. Or rather, economic systems naturally emerge from a single medium due to the function of money. The properties inherent in bitcoin are causing the market to converge on it as a tool to communicate and measure value because it represents a step-function change improvement over any other monetary medium. If anyone comes away with the fundamental view that money is a necessity and that monetary systems naturally converge, the question then centers on whether bitcoin is optimized to fulfill the monetary function better than any of the competition.

Money is a necessity

Civilization as we know it would not exist without money. Without money, there would be no airplanes, no cars, no iPhones, and the ability to fulfill very basic necessities would become materially impaired. Millions of people could not peacefully inhabit a single city, state, or country without the function of money. Money is the economic good that allows food to reliably show up on grocery shelves, gas to be at the gas station, electricity to power homes, clean water to be abundant, etc. It is money that makes the world turn and it would not turn in the way that most have taken for granted if not for the function of money. It is a massively underappreciated function; one that is poorly understood because it is generally not consciously considered. In the developed world, reliable money is taken as given. So too are the basic necessities delivered through the coordination function of money.

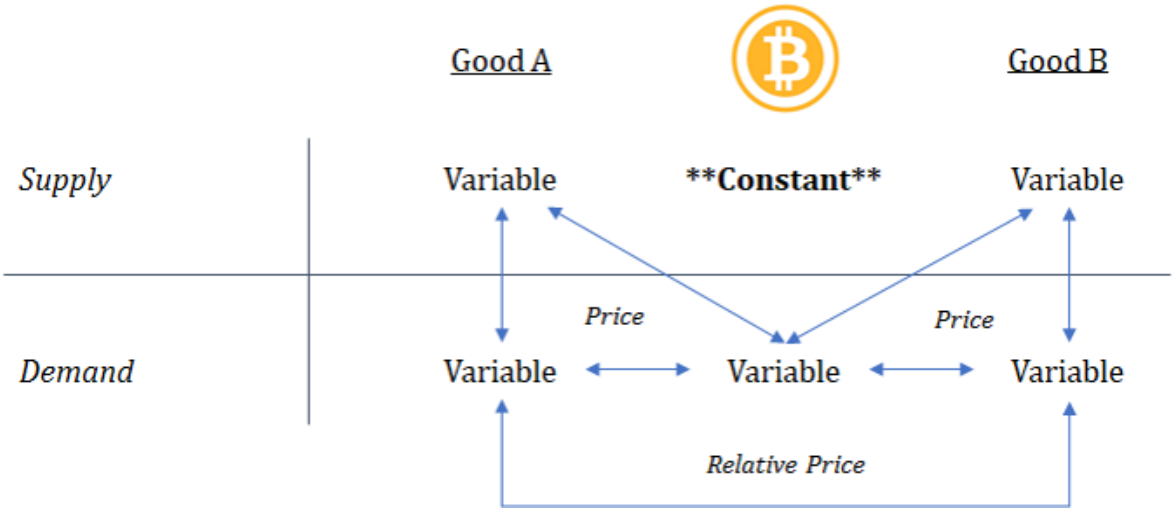
Consider, for example, a local grocery store and the range of choice that converges in a single store. The number of individual contributions and skills that are required to make that happen is mind-boggling. From the

coordination of the store itself, to the individual packaging, to the technology providers, to the logistics networks, to the transportation networks, to the payments systems, and right down to each individual item of food. Then as a derivative, consider all the unique inputs that go into each item on the shelf. The grocery store is just the fulfillment side; the production of each input has its own diverse supply chain. And it is just one modern marvel. Deconstructing the inputs of a modern telecom network, energy grid or water and waste management system is similarly complex. Each network and the participants therein rely on the others. Producers of food rely on individuals that help fulfill energy demand, telecom services, logistics, clean water, etc. among others and vice versa. Practically all networks are connected, and it is all made possible through the coordination function of money. Everyone is able to contribute their own skills based on their own personal interests and preferences: receive money in return for value delivered today, and then use that same money to acquire the specialized value created by others in the future.

And it does not all happen by chance either. Some not-so-rigorous thinkers suggest that money is either a collective hallucination or that it derives value from the government. In reality, money is a tool that was invented by man to satisfy a very specific market need in facilitating trade. Money helps facilitate this activity by acting as an intermediary between a series of present and future exchanges. Without any conscious control or direction, market participants evaluate various different goods and converge on the tool with the properties best-suited to facilitate the very express purpose of converting present value for future value. Whereas individual consumption preferences vary from person to person and change constantly, the need for exchange is practically universal, and the function is distinctly uniform. For every individual, money allows for value produced in the present to be converted into consumption in the future. The value one places on a home, a car, food, leisure, etc. naturally changes over time and logically varies from person to person. But the need to consume and the need to communicate preferences does not change and applies to all individuals on an intersubjective basis.

Money exists to communicate these preferences and ultimately, value. But recognizing that all value is subjective (and not intrinsic), money forms the baseline to establish an expression of value and more importantly relative value. Money represents the collective recognition that everyone benefits from the existence of a common language to communicate individual preferences. It aggregates and measures the preferences of all individuals within an economy, at any point in time, and it would not be possible, or at the very least extremely inefficient, to communicate value if not for a common constant upon which everyone could agree. Think of money as the constant against which to measure all other goods. If it did not exist, everyone would be at a practical standstill, not able to agree on the value of anything.

By comparing against a single constant, it then becomes more practical to discern the relative value of two other goods. There are billions of goods and services produced by billions of individuals, all with unique preferences. Through the convergence on a single form of money to aggregate and communicate all preferences, a price system ultimately emerges. By measuring and expressing the value of all goods in a common intermediary (money), it then becomes possible to understand how much one good (or resource) is valued relative to any other.



Without the use of a common currency, there would be no concept of price. And without the concept of price, it would not be possible to do any range of economic calculation. The ability to perform economic calculation allows individuals to take independent actions, relying on the information communicated through a price system, to best satisfy their own needs by understanding the needs of others. In fact, it is a price system that allows supply and demand structures to form, and it is ultimately a necessity because it provides for the communication of information, without which the fulfillment of basic needs would not be possible. Imagine if nothing you consumed had a discernible price. How would you know what you needed to produce in order to obtain the goods you prefer? Then recognize that your own conception of the value you produce and the very existence of goods and services produced by others would not be available if not for some expression of price existing. It becomes circular, but money is the good that allows the underlying structures of an economy to form through the price system. While it is often extolled as the root of all evil, money may just be the greatest accidental invention ever created by man, and one that could not have emerged by conscious control.

> *"I have deliberately used the word "marvel" to shock the reader out of the complacency with which we often take the working of [the price] mechanism for granted. I am convinced that if it were the result of deliberate human design, and if the people guided by the price changes understood that their decisions have significance far beyond their immediate aim, this mechanism would have been acclaimed as one of the greatest triumphs of the human mind. Its misfortune is the double one that it is not the product of human design and that the people guided by it usually do not know why they are made to do what they do. But those who clamor for "conscious direction"—and who cannot believe that anything which has evolved without design (and even without our understanding it) should solve problems which we should not be able to solve consciously—should remember this: The problem is precisely how to extend the span of our utilization of resources beyond the span of the control of any one mind; and therefore, how to dispense with the need of conscious control, and how to provide inducements which will make the individuals do the desirable things without anyone having to tell them what to do."*
>
> – F.A. Hayek (The Use of Knowledge in Society)

Economic systems converge on a single monetary medium

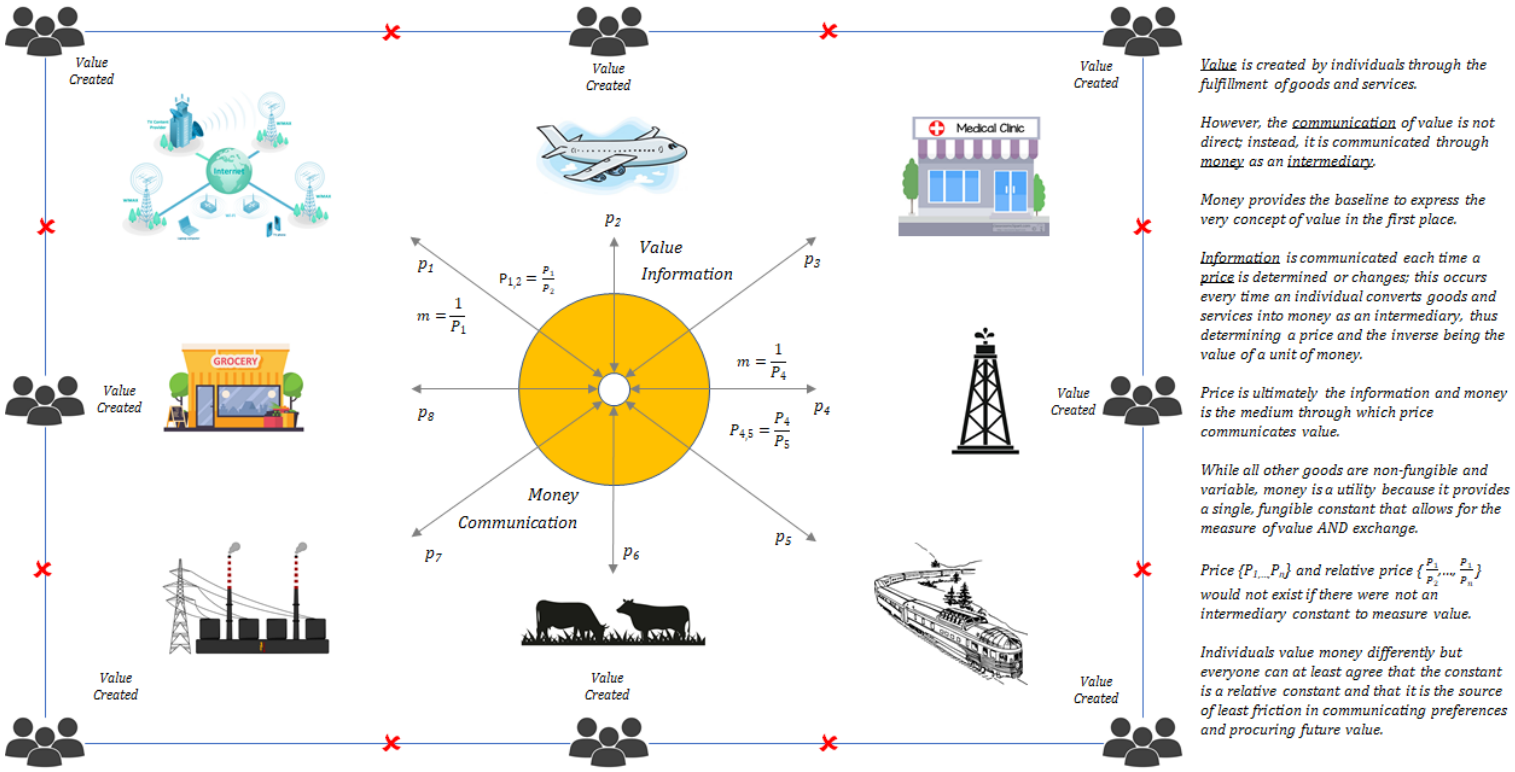
Late stage Silicon Valley thinking has many people believing that hundreds, if not thousands, of currencies may exist in the future. The machines are going to do all the calculation! AI and quantum will handle it. An intellectually "safe" view to hold is that 95% of cryptocurrencies will probably fail but there are some "interesting" projects. "It is inherently difficult to know which will succeed." "Much like venture capital investing, most will fail but the ones that win will win big." At least, this is what most of Silicon Valley would have you believe because it is a defensible parallel to historical experiences investing in companies. In reality, it is a blanket hedge lacking in first principles. It is also applying a familiar formula to an entirely distinct class of problem.

While it may seem logical to form a mental framework around bitcoin in relation to the rhyming history of technology startups, there can be no comparison whatsoever. Bitcoin is money, not a company. It would be illogical to assume competition between two monetary mediums (or multiple) would be in any way parallel or would follow a similar pattern to that of two companies. Companies compete in a capital formation arms race; in order to do so, they need money to coordinate economic activity. How do they get money? By using money to coordinate the production of goods and services and by selling the output for more money (profit). In essence, companies compete for the same pool of money in order to accumulate capital. Money is the tool that makes the wheel go round. It simply would not be possible to coordinate all the individual skills necessary in order to allow for the fulfillment of goods and services derived from the complexity of most modern supply chains without money. It also would not be possible if it were

not for the fact that a large group of people accepted a common form of money.

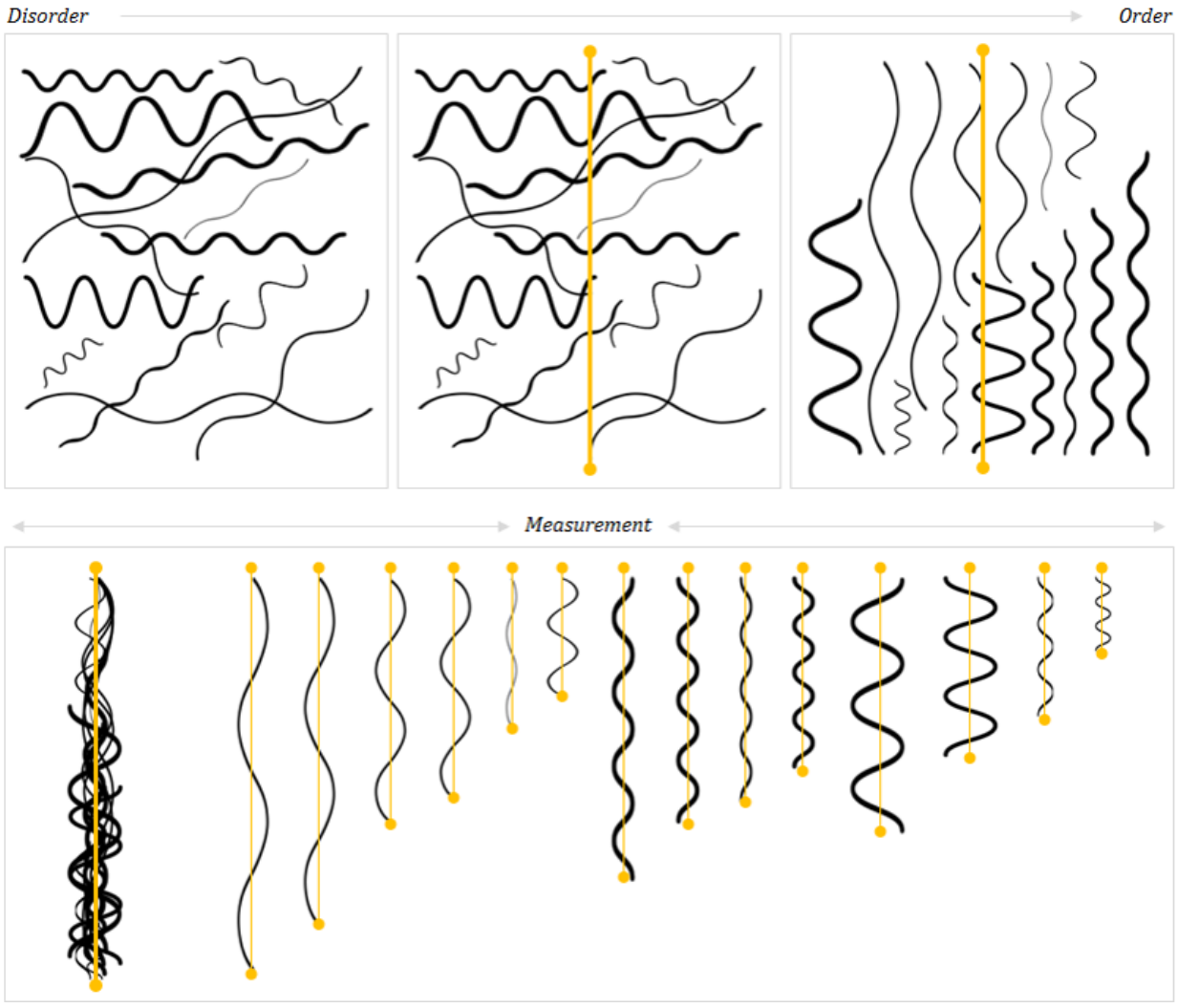
> *"Having a single medium of exchange allows the size of the economy to grow as large as the number of people willing to use that medium of exchange. The larger the size of the economy, the larger the opportunities for gains from exchange and specialization, and perhaps more significantly, the longer and more sophisticated the structure of production can become."*
>
> – Saifedean Ammous (The Bitcoin Standard)

In the supply chain of production, money serves a distinct function of a different class than any individual good or service. It is the distinction between the fulfillment of preferences (production of goods and services) and the coordination of preferences (money). The fulfillment of preferences is dependent on the coordination of preferences, and the coordination of preferences is dependent on a price system, which can only form as a derivative of mass convergence on a single monetary medium. Without a pricing system, division of labor would not exist, at least not to the extent necessary to allow for the functioning of complex supply chains. This is the root level principle most miss when contemplating a world of many currencies. Any pricing system is derived from a single currency. The concept of price would not exist if not for a critical mass of individuals producing a diverse set of goods and services and communicating the value of those goods and services through a common medium. In order to derive the benefit of money and price, convergence is a precursor. As a result, it may be more accurate to say that economic systems emerge from a single monetary medium rather than converge on one. Individuals converge on a single monetary medium and the output is an economic system.



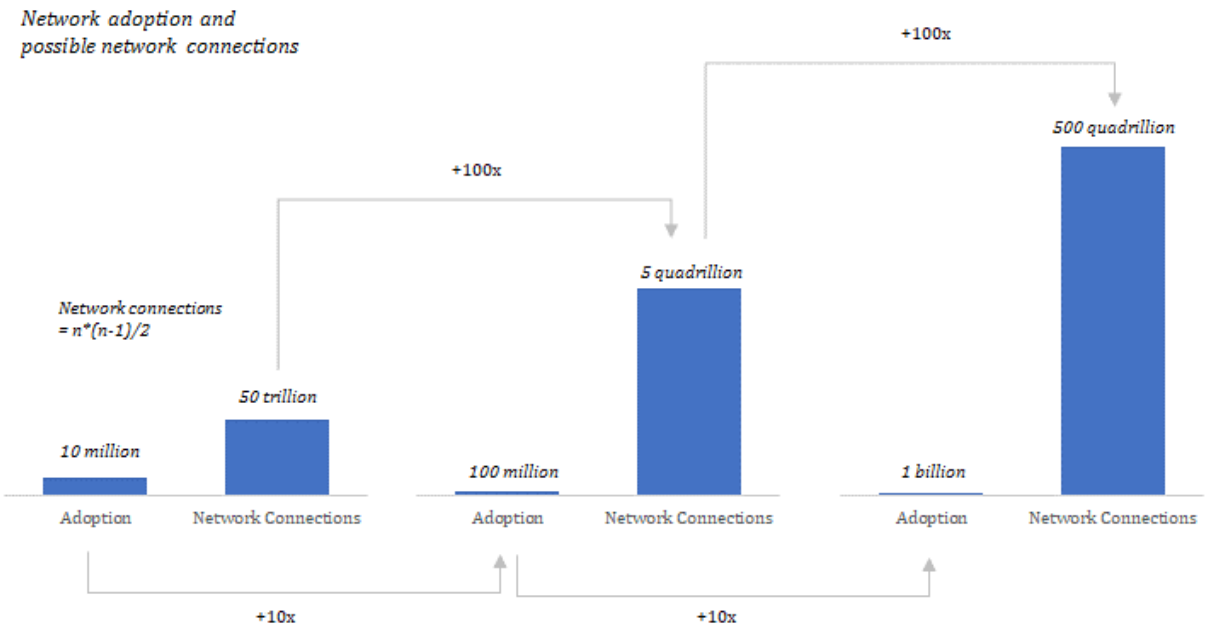
Whereas the value of all other goods and services is consumption, the value of money is exchange. Exchange is the good any individual is purchasing when choosing to convert value (the subjective output of time, labor and physical capital) into a monetary good. Individual consumption preferences are unique, but money serves one singular function for all market participants: to bridge the present to the future (whether it be for a day, week, year or longer). In any exchange of present value, some time continuum exists until a future exchange. At the point of exchange, each individual must make a decision as to which monetary good will best serve the function of preserving value created in the present into the future. A or B? While an individual can choose to hold one or multiple currencies, one is definitionally going to perform that function more effectively. One will preserve future purchasing power better than the other. Everyone intuitively understands this and makes a decision based on the inherent properties of one medium relative to another. When deciding which monetary good to use, the preference of one individual is impacted by the preference of others, but each individual is making an independent evaluation discerning the relative strengths of multiple monetary goods. It is not coincidence that the market converges on a single medium because each individual is attempting to solve the same problem of future exchange, which is interdependent on the preference of others.

The ultimate goal is to reach consensus such that each individual can communicate and exchange with the widest and most relevant set of trading partners. Collectively, it is an objective evaluation of tangible goods based on an intersubjective need. The whole point is to find the one good that everyone can agree is i) a relative constant, ii) measurable and iii) functional in exchange. The existence of a constant creates order where none existed previously, but that constant must also be functional as both a measurement tool and a means of exchange. It is the combination of these characteristics, often described as aggregating the properties of scarcity, durability, fungibility, divisibility, and transferability, which are unique to money. Very few goods possess all of these properties, and every good is unique, with inherent properties that cause each to be better or worse in fulfilling certain functions within an economy. A is always different than B, and the combination of properties that perfect a monetary good are so rare that the distinction from one to another is never marginal.



More practically, everyone agrees on a single monetary good through which to express value because it is in their individual and collective interests to do so. It is the problem itself: how to communicate value with other market participants. It would be counterproductive to the entire exercise if a consensus were not formed. But it is the properties of a monetary good itself that allow for convergence and consensus. The imagined world of thousands of currencies is blind to these fundamental first principles. A critical mass of individuals converging on a common medium is the input required to ascertain the information that is actually desired. And the value of a common medium only increases in value as more and more people converge on it as a tool to facilitate exchanges. The fundamental reason being that with more individuals converging on a single medium, the medium actually accumulates more information and presents a greater utility.

Think of each individual as a potential trading partner. As individuals adopt the common medium as a standard of value, all existing participants in the monetary network gain new trading partners, as do the individuals that become part of the network. There is mutual benefit, and ultimately the range of choice expands. But what also occurs as a monetary network expands is that more goods come to be valued in the common medium of exchange. More prices exist, and as a result, more relative prices do as well. More information is aggregated into the common medium, which can then be relied upon by all individuals within the network (and by the network as a whole) to better coordinate resources and respond to changing preferences. The constant becomes more valuable and inherently more reliable as it communicates more information about more goods produced by more individuals. The constant actually becomes more constant as more variable information is communicated through it.



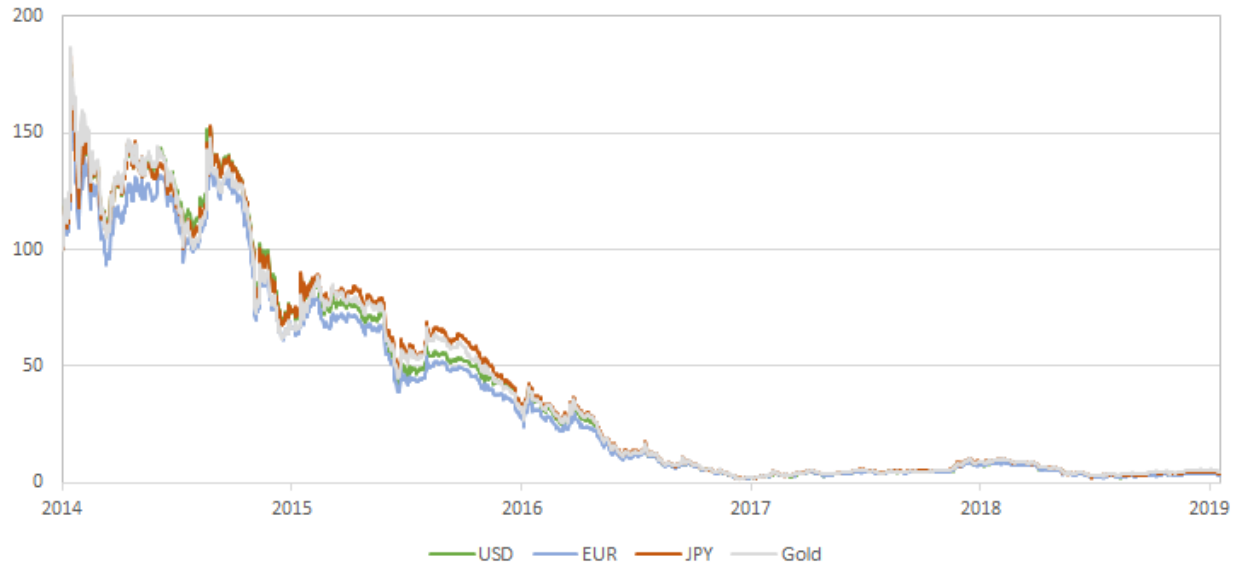
As adoption of a monetary network increases by an order of magnitude (10x), possible network connections increase by two orders of magnitude (100x). While this helps demonstrate the mutual benefit of adoption, it also highlights the consequence of converting value into a smaller monetary network. A network that is one-tenth the size has 1% of the number of potential connections. Not every network distribution is equal, but a larger monetary network translates to a more reliable constant to communicate information – greater density, more relevant information and ultimately a broader range of choice. The size of a monetary network and the expected growth of that network become critical components of the intersubjective A/B test, when each individual is determining which medium to utilize. While the number of people with whom any individual can maintain social relationships is inherently limited, the same limits do not apply to monetary networks. It is money that allows humans to break from the constraints of Dunbar's number. A monetary network allows for millions (if not hundreds of millions) of people unknown to each other to contribute value at end points in the network, with relatively few direct connections needed.

Monetary networks ultimately accumulate the value of all other networks because all other network effects would not exist without a monetary network. Complex networks cannot form without a common currency to coordinate the economic inputs necessary to kick start the positively reinforcing feedback loops of price. A common currency is the very foundation of any monetary network, which allows other value networks to form. It provides the common language to communicate value, ultimately leading to trade and specialization, and organically creating the ability to expand the use of resources beyond the reach of "conscious control" (to

steal *Hayek*). When contemplating the network effects of a social network, a logistics network, a telecom network, energy grid etc., add them all together and that is the value of a monetary network. A monetary network not only provides the foundation for all other value networks to form, but the currency of that network is what pays for access to all derivative networks within the monetary network. The existence of the common currency is the engine and the oil.

Yes, the dollar, euro, yen, pound, franc, yuan, ruble, lira, peso, etc. all co-exist today, but this is not a natural function of an open, global economy. Instead, each fiat currency that exists today emerged as a fractional representation of gold, which the world had previously converged upon as a monetary standard. None would subsist without the forces of government intervention; nor would any fiat currency have ever emerged if not for the prior existence (and limitations) of gold as a monetary medium. Modern monetary theorists and gold bugs alike will never admit it, but the calamity that is all fiat systems is nothing more than the manifestation of gold's failure as a monetary medium. It is a dead man walking. The gold standard was formally abandoned in 1971, and the subsistence of jurisdictional fiat systems since then merely represents a transient departure from free market monetary forces. Modern fiat systems have only managed to survive as long as they have because a solution to the very problem created by fiat did not yet exist. Bitcoin is that solution, and ever since its creation, individuals have been converging upon it as a new monetary standard; a trend that will only continue as knowledge naturally distributes.

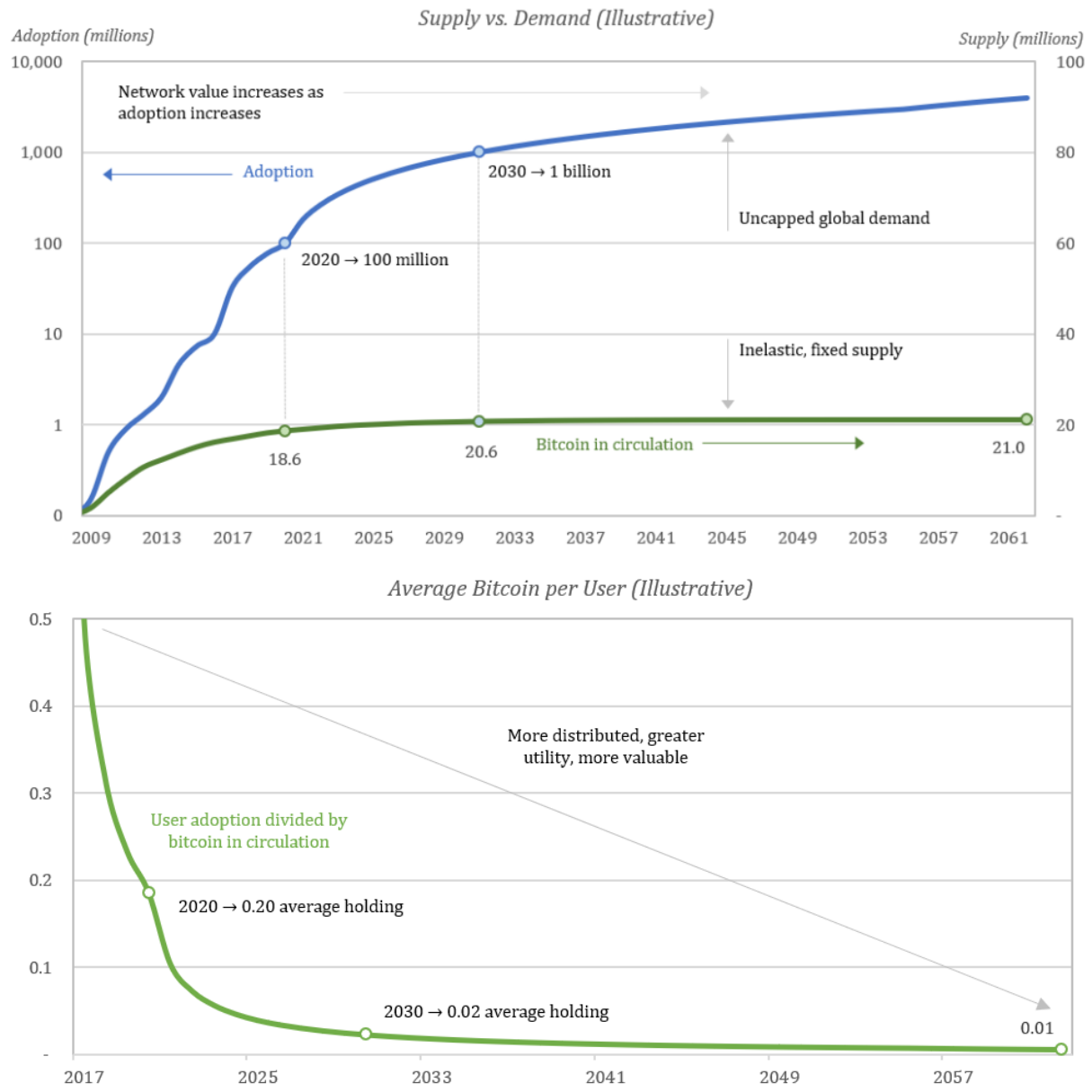
Dollar, Euro, Yen, Gold – Indexed to Bitcoin (2014 = 100, value <100 represents decline in value)



All Roads Converge on Bitcoin

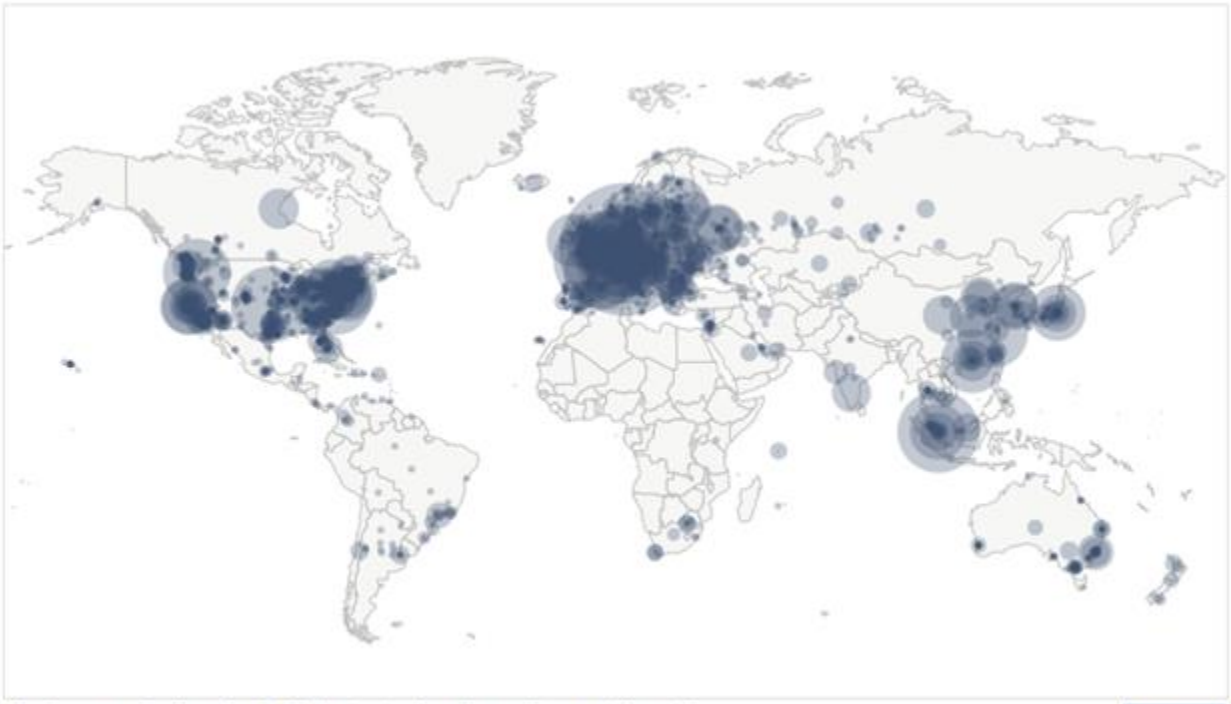
The Greatest Constant – Finite Scarcity

The market converges on bitcoin over time and its value continues to increase because it provides a constant that is superior to any other form of money. Bitcoin has an optimal monetary policy, and that policy is credibly enforced on a decentralized basis. Only 21 million bitcoin will ever exist, and the element of trust is removed from the equation entirely. Bitcoin's fixed supply is enforced by a network consensus mechanism on a decentralized basis. No one trusts anyone, and everyone enforces the rules independently. As an aggregate of these two functions, bitcoin is becoming the scarcest form of money that has ever existed. Finite scarcity is a property no other form of money has ever or will ever achieve, and demand for bitcoin is fundamentally driven by that scarcity. However, scarcity is a two-sided equation. A fixed supply may be the primary draw, but demand is a critical and often overlooked aspect of scarcity. Demand is what actually makes scarcity a utility as a constant in exchange. Bitcoin becomes more and more scarce as a two-way function of increasing demand and a completely inelastic terminal supply. The scarcity of its fixed supply creates demand but increasing demand then creates greater scarcity. It sounds circular because it is. If there were 21 million bitcoin and only 1 person valued it, there would be nothing scarce or useful about bitcoin. But if 100 million people valued bitcoin, 21 million starts to become scarce. And if the network grew to one billion people, 21 million would become extremely scarce, and bitcoin would represent a greater utility as a constant.



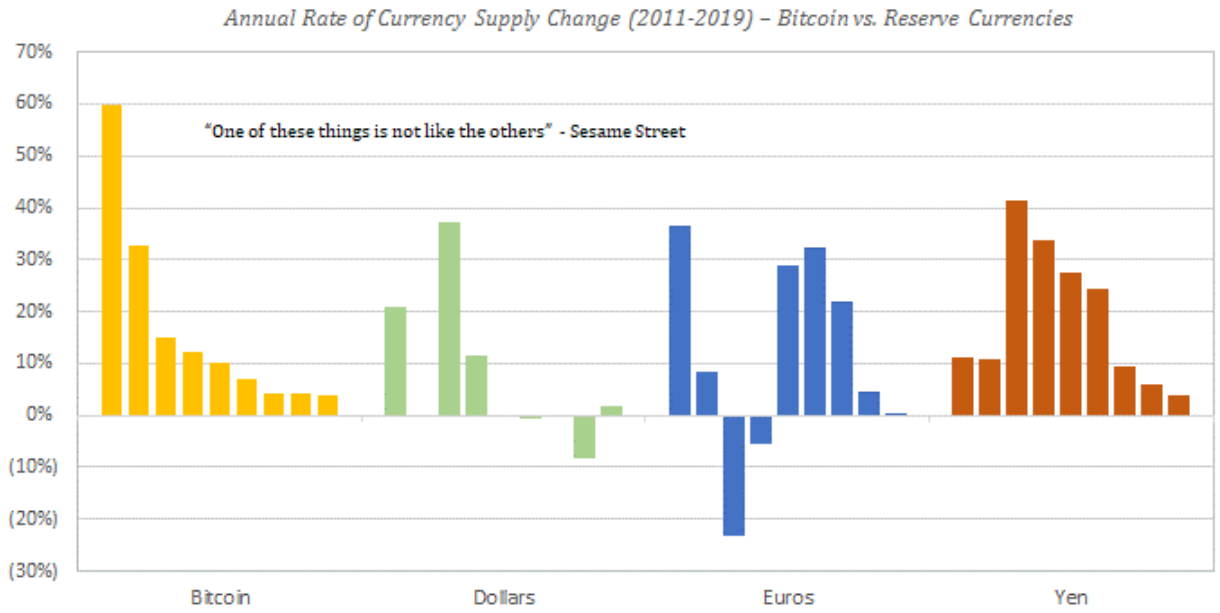
With a fixed supply, increased demand naturally results in bitcoin becoming more distributed. There is only so much to go around, and the pie ends up getting split up into smaller and smaller shares owned by more and more people. As more individuals value bitcoin, the network not only becomes a greater utility; it also becomes more secure. It becomes a greater utility because more people are communicating in the same language of value through a more reliable constant. And as more individuals participate in the network consensus mechanism, the entire system becomes more resistant to corruption and ultimately more secure. Recognize that there is nothing about a blockchain that guarantees a fixed supply, and bitcoin's supply schedule is not credible because software dictates it be so. Instead, 21 million is only

credible because it is governed on a decentralized basis and by an ever increasing number of network participants. 21 million becomes a more credibly fixed number as more individuals participate in consensus, and it ultimately becomes a more reliable constant as each individual controls a smaller and smaller share of the network over time. As adoption increases, security and utility work in lock-step. Consider the distribution and relative density of bitcoin adoption throughout the world (heat map below of network nodes). As reach and density within each market spread, bitcoin's constant becomes harder and harder.



As individuals increasingly opt-in, 21 million becomes more and more credible, and in the mind of those who adopt it, finite scarcity becomes what differentiates bitcoin from all other forms of money – both legacy currencies and competing cryptocurrencies alike. All other currencies either centralize over time (e.g. the dollar, euro, yen, gold) or were too centralized from the start (e.g. all other cryptocurrencies) to credibly compete with a fixed supply of 21 million. Centralization inherently creates the need to rely on trust, and trust ultimately puts the supply of any currency at risk, which in turn impairs demand and marginalizes its utility in the function of exchange. Whereas all other currencies depend on trust, the constant bitcoin provides is trustless. 21 million is only credible because bitcoin is decentralized, and bitcoin becomes increasingly decentralized over time. The best any other form of money could possibly do is match bitcoin, but practically, it is not possible because individuals converge on a single medium, and bitcoin beat every other

currency to the punch. Every other currency is ultimately competing against the ideal constant; one that will not change and that does not rely on trust.



All forms of money compete with each other for every exchange. If the primary (or sole) utility of an asset is the exchange for other goods and services, and if it does not have a claim on the income stream of a productive asset (such as a stock or bond), it must compete as a form of money. As a consequence, any such asset is directly competing with bitcoin for the exact same use case, and no other currency will ever provide a more reliable constant because bitcoin already exists and it is finite. Because individuals converge on a single medium, scarcity in bitcoin will perpetually be reinforced on both the supply and demand side, whereas the opposite force will be in effect for all other currencies due to the reflexive nature of monetary competition. The distinction between two monetary goods is never marginal, and neither is the consequence of individual decisions to exchange in one medium rather than another. Money is an intersubjective problem, and a choice to opt into one monetary medium is an explicit opt out of the other, which in turn causes one network to gain value (and utility) at the direct expense of another. As bitcoin becomes more scarce and more reliable as a constant, other currencies become less scarce and more variable. Monetary competition is zero sum, and relative scarcity, a dynamic function of both supply and demand, creates the fundamental differentiation between two monetary mediums that only increases and becomes more apparent over time.

But remember that scarcity for scarcity sake is not the goal of any money. Instead, the money that provides the greatest constant will facilitate exchange most effectively. The monetary good with the greatest relative

scarcity will best preserve value between present and future exchanges over time. Relative price and relative value of all other goods is the information actually desired from the coordination function of money, and in every exchange, each individual is incentivized to maximize present value into the future. Finite scarcity in bitcoin provides the greatest assurance that value exchanged in the present will be preserved into the future, and as more and more individuals collectively identify that bitcoin is the monetary good with the greatest relative scarcity, stability in its price will become an emergent property (see Bitcoin is Not Too Volatile).

The Greatest Measurement Tool – Divisibility

While scarcity is the bedrock, not all scarce goods are functional as money. In order to be functional as a tool to communicate value, a monetary good must be a relative constant, easy to measure and functional in exchange. A ruler may be an effective measurement tool, but rulers are not scarce, nor is it easy to carve up pieces of a ruler into larger and smaller units to facilitate exchange. In exchange, a monetary good being scarce and measurable allows for the measurement of all other goods; the ability to easily subdivide and transfer a monetary unit provides for practical utility in exchange. Bitcoin combines finite scarcity with the ability to subdivide each whole unit down to 8 decimal points (0.00000001 or one 100,000,000th of a bitcoin) and transfer any amount of value, however large or small. Just as scarcity for scarcity sake is not necessarily valuable in the context of money, neither is the property of divisibility. It is the combination that becomes valuable in the context of money, particularly when each subdivided unit is fungible – when each individual unit is essentially interchangeable and each of its parts is indistinguishable from another part. It is these properties together that allow bitcoin to not only be a perfect constant but also an effective measure of value to facilitate exchange.

In the code, one bitcoin is actually represented as 100,000,000 sub-units, with the smallest unit referred to as a satoshi (or sat for short). Technically, one bitcoin is 100,000,000 sats. While one bitcoin equates to approximately $9,000 today, one satoshi is equal to one-twentieth of a penny. In essence, anyone can exchange any amount of value into bitcoin. Bitcoin, as with any money, is functional for one purpose, to store value between a series of exchanges. Receive bitcoin for value produced today, save, spend bitcoin in the future in return for value produced by others. It will perform the same function regardless of amount. The practical consequence of divisibility is that bitcoin is capable of measuring any and all value which allows it to support any and all adoption. Individuals produce a wide range of value, and divisibility allows all individuals to utilize bitcoin as a savings mechanism regardless of whether it be to store $50 or $50,000 in value. For a monetary

good to be an effective communication tool, it must be able to measure the range of value produced by all individuals, and bitcoin does this flawlessly. The ability to divide and transfer any amount of bitcoin makes it accessible to all individuals and ultimately all goods produced, regardless of how much value is attributable to each.

In the A/B test of monetary competition, if A > B, any amount of A will perform the function of money better than any amount of B. Over time, A will increase in purchasing power relative to B whether it be for $50 or $50,000-worth of value. Never be confused by a list of cryptocurrencies trading on Coinbase that look like a "better deal" because the price is "cheap" whereas bitcoin appears "expensive." Always remember that bitcoin is capable of being divided into smaller or larger units to store more or less value. One bitcoin is an inherently arbitrary unit, as is one unit of any currency. The market test is whether A is more functional as money than B. It is an intersubjective decision, and while the market is communicating which network it believes performs the monetary function more effectively through price and value, network value is the output, not the input. The input is each individual evaluating the properties of the monetary good itself relative to others. If bitcoin is A in your evaluation, then there is no "too expensive." Bitcoin may be over or undervalued at any point in time, but each individual that adopts bitcoin increases the value of the network (recall the discussion on trading partners + network connections). And the ability to be divided easily into very small units allows for a practically limitless number of individuals to convert and communicate value through the network. If A is greater than B, and if A can support unlimited adoption, it eventually obsoletes the need for network B.

Network value	$100 billion	$500 billion	$1 trillion	$10 trillion
Nominal Amount of Bitcoin to Send $10,000	0.210 bitcoin	0.042 bitcoin	0.021 bitcoin	0.002 bitcoin
Max # of individuals capable of sending $10,000 worth of bitcoin	10 million	50 million	100 million	1 billion

Adoption actually drives value, not the other way around but more adoption begets more adoption because increasing adoption tangibly increases the utility of the network.

This network is far more valuable than that network and not linearly so.

As individuals independently evaluate this A/B test, more people ultimately adopt bitcoin, and bitcoin becomes divided into smaller and smaller units (on average). This is the result of increasing demand combined with a fixed supply, and the value of the network actually increases as a function of this

process. As a network, bitcoin becomes more valuable as it is valued by more people. Essentially, 0.1 bitcoin = $1,000 is more valuable than 1.0 bitcoin = $1,000, despite each being worth the same measured in dollar terms. More exchange (and ultimately more commerce) becomes possible the more valuable bitcoin becomes in total, but value is really an output of more and more people choosing to adopt bitcoin as an exchange intermediary. Each individual owns a smaller and smaller nominal amount of the currency, but the purchasing power of each equivalent unit increases over time. With each exchange, every individual is conveying his or her own value onto the network and is doing so at the direct expense of a competing monetary network. Through this process, a new price is determined specific to the value created and measured by each individual, and as a result, bitcoin accumulates more information derived from a more diverse set of trading partners.

While prices today may not yet be quoted in bitcoin terms, a pricing system is forming every time an individual converts value into bitcoin. Even if dollars are an indirect intermediary, value produced somewhere in the world, distinct to a particular individual, is expressed as a unit of bitcoin; as more and more people choose to do so and increasingly on a per-individual basis, that value converts to a smaller and smaller unit of bitcoin (on average). The consequence is that a smaller and smaller denomination of bitcoin can be used by more people to transfer an equivalent amount of value, and as bitcoin is measured by more people, its ability to measure relative value only increases. Since bitcoin can measure all value and can be adopted by a limitless number of individuals, it practically obsoletes the need for any other value transfer network over the long-term because the form of money with the lowest rate of change ultimately communicates more perfect information. Finite scarcity combined with divisibility creates an extremely powerful exchange intermediary. Bitcoin has the lowest terminal rate of change possible due to its absolute scarcity, and it can be divided to a fraction of a penny, which will allow it to measure value far more precisely than any other currency.

The Greatest Exchange Tool – Transferability

With this baseline, the real knockout punch becomes the fact that bitcoin can be irrevocably transferred over a communication channel without the need for any trusted third-party as an intermediary. This is fundamentally different than digital payments in fiat systems, which are dependent on trusted intermediaries. In aggregate, bitcoin is a greater constant than any other form of money and is highly divisible (and measurable), while also capable of being transferred over the internet. Try to identify a single other good that could possibly share these properties: finite scarcity (greatest

constant) + divisibility and fungibility (measurement) + ability to send over a communication channel (ease of transfer). This is what every other monetary good is up against as it competes for the convergent role of money. Practically, the only way to really appreciate the power of such a rare dynamic is through experiencing it firsthand. Any individual can access the network on a permissionless basis by running a bitcoin node on a home computer. The ability to power up a computer anywhere in the world and transfer a finitely scarce resource to any other individual, without permission or reliance on a trusted third-party is empowering. That hundreds of millions of people can do this in unison without anyone needing to trust other participants in the network is near-impossible to fully comprehend.

Bitcoin is often described as digital gold, but really, this does not do it justice. Bitcoin combines the strengths of physical gold with the strengths of the digital dollar without the limitations of either. Gold is scarce but difficult to divide and transfer, while the dollar is easy to transfer but not scarce. Bitcoin is finitely scarce, easy to divide, and easy to transfer. In their current forms, both gold and all fiat monetary systems are dependent on trust, whereas bitcoin is trustless. Bitcoin optimized for the strengths and weaknesses of both, which is fundamentally why the market is converging (and will continue to converge) on bitcoin to fulfill the function of money.

Bitcoin Obsoletes All Other Money

If any individual comes to three principal conclusions: i) money is a basic necessity, ii) money is not a collective hallucination and iii) economic systems converge on a single medium, that individual is going to more consciously seek out the best form of money. It is money that preserves value into the future, and ultimately, allows individuals to convert their own time and their own skills into a range of choice so great that prior generations would find it difficult to imagine. Freedom is ultimately what a reliable form of money provides: the freedom to pursue individual interests (specialization) and the ability to convert the output of that value into the value created by others (trade). Whether individuals consciously ask themselves these questions or not, they will naturally be forced to answer them through their actions. They will also arrive at the same answer as those that do. The conscious and the subconscious arrive at the same place because the fundamental truths do not change, and the function of money is singular: to intermediate a series of present and future exchanges and to provide the very baseline to communicate subjective value among a wide group of individuals that stand to benefit from trade and specialization. Money is a necessity. There are discernible properties that make certain goods more or less functional in exchange, and exchange is an inherently intersubjective problem.

Owning bitcoin is becoming the cost of entry to what will likely be the largest and most diverse economy that has ever existed. Bitcoin is global and it is accessible on a permissionless basis. Because bitcoin becomes the common language of value for all participants, anyone that is a part of the network will be able to communicate and ultimately trade with other network participants. The more trading partners, the greater the value each unit provides to the individuals holding the currency. While there will likely always be jurisdictional friction that impedes trade, access to the same common currency removes the root source of friction in the communication of value, and bitcoin's fixed supply will allow its pricing mechanism to accumulate and communicate more perfect information with the least amount of distortion relative to any other form of money. And as more individuals choose to store value in bitcoin, its fixed supply becomes more credible and its pricing mechanism more reliable and relevant. New adopters of a monetary network both contribute value and realize value as a function of adoption, which is why it is not possible to be late to bitcoin, nor will bitcoin ever be too expensive.

It does not matter how complex bitcoin is. At the end of the day, bitcoin becomes an A/B test. The need for money is real and individuals will converge on the form of money that best fulfills the function of exchange. No other currency in the world can ever be more scarce than bitcoin, and scarcity will act like a gravitational force driving adoption and communication of value. Today, most billionaires do not understand bitcoin. Bitcoin is an equal opportunity mind-bender. But even those who do not understand bitcoin will come to rely upon it. There are many fundamental questions. Bitcoin is volatile, seemingly slow, challenges to scaling, not commonly used for payments, consumes a lot of energy, etc. Stability is an emergent property that follows adoption, and all other perceived limitations will be solved as a function of the value that is derived from finite scarcity combined with the ability to measure, divide and transfer value. That is the innovation of bitcoin. Currency A has a fixed supply. Currency B does not. Currency A keeps increasing in value relative to Currency B. Currency A continues to increase in purchasing power relative to goods and services while Currency B does the opposite. Which one do I want? A or B? Make the right choice because the opportunity cost is your time and value. All of the rest simply explains why individuals will increasingly opt for A over B, but in practice, it all comes down to basic common sense and survival instincts. Bitcoin obsoletes all other money because economic systems converge on a single currency, and bitcoin has the most credible monetary properties.

"I don't believe we shall ever have a good money again before we take the thing out of the hands of government, that is, we can't take it violently out of the hands of government, all we can do is by some sly roundabout way introduce something that they can't stop." – F.A. Hayek.

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

Bitcoin is good for your government's treasury

By FF2K

Posted January 26, 2020

As long as your government controls the exchanges and retail businesses, you will always need to convert your bitcoin to fiat if you intend to use it. Since bitcoin is limited in supply and fiat is not, the value of bitcoin in fiat should hypothetically continue to rise as long as your government needs to print money to fund their excess spending and more people have a need for bitcoin. This fact and the existing tax laws incentivize the bitcoin owner to HODL. The longer one HODLs the greater appreciation in fiat they will see.

Bitcoin is a universal measuring stick that should expose fiat production/inflation. Why would your government allow such a scarce asset be used and traded? The answer is simple, capital gains tax. Capital gains tax, can range from 0, 15 or 20% in the USA. Let's use 15% for our example. If a bitcoiner buys (1) bitcoin for $8,000.00 and over the course of 3–4 years, it rises in price to say $30,000.00, if he spends it or exchanges it, he needs to pay 15% of the difference ($3,300.00) back to the government. At a bitcoin price of $61,333.00, the bitcoiner owes the government the original $8,000.00 back in taxes. At $100,000.00 bitcoin, the bitcoiner owes the government $13,800.00 which is more than the original $8,000.00 he invested.

In the future, I see this capital gains tax similar to valued added tax or a sales tax, you will incur it when spending. Is this a bad thing? In my opinion, it's better than the existing system for all participants.

The HODLer could have left his $8,000.00 in fiat and experienced the loss in purchasing value, or he can enjoy 85% of the gain from the debasement of his currency.

The Medium of exchange user, who doesn't HODL does not have a capital gain, so he is not affected.

The No-Coiner can continue to live his life in disbelief of this phenomenon as he always has.

Your government gets to collect tax on their money printing.

This is simply my opinion and it is why I don't fear the government shutting down bitcoin, why would they?

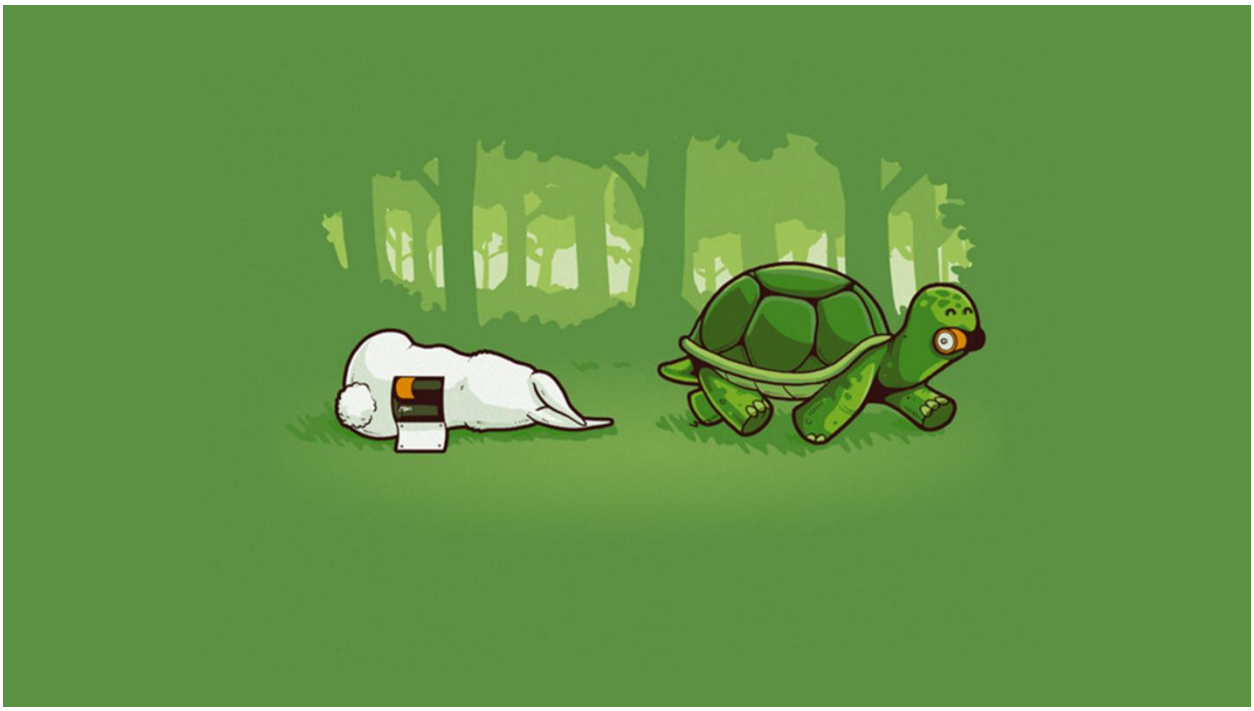
I'd love to hear your feedback

How Not To Critique Bitcoin

A quick defense of moving slow and not breaking things.

By Conner Brown

Posted January 28, 2020



After publishing my latest article, I received some pushback about Bitcoin's flexibility. This viewpoint is best expressed by Paddy's tweetstorm here and parts of Daniel Goldman's article here. This is a quick response, but it needs to be said.

More opcodes more problems.

Their view holds that Bitcoin's simple and conservative baselayer is a major hinderance to developing smart contracts on layer two. It is an understandable view. There are many cool features in the pipeline for Bitcoin, and many of them are already written, but we still don't have them! However, patience is a virtue. It may be tempting to add as many features as quickly as possible, but when dealing with an **entirely new global monetary system**, its important to be extremely cautious — this may be our only shot at changing the world! Recall that we've had a potential inflation bug from something as simple as a routine optimization. If Bitcoin fails, the dream of digital sound money may be dead for decades.

Returning to the contracts analogy, it might seem great to have a judge that can make decisions in a variety of fields, but only so long as they have sufficient expertise. After all, a judge is no good if their decisions can't be relied upon. Therefore, it's better to use their judgement for a few critical decisions they will get right with high confidence. Bitcoin's slow and methodical development approach is necessary for building the rock solid foundation required for something so important.

The recent push for BIP 119, OP_CHECKTEMPLATEVERIFY (fka OP_SECURETHEBAG), is a great example of this thinking. Covenants in Bitcoin were once an enabled feature, but core developers disabled them as a precaution to prevent potential fungibility issues. Jeremy Rubin's BIP 119 proposal thus only enables a few limited forms of covenants which bring clear benefits (channel factories, vaults, easier coinjoin, congestion control, etc.) with limited downside risk.

To be clear, it would have been easier to just enable covenants in the first place and avoid this BIP altogether, but this is an important example of Bitcoin's design philosophy: **First, Do No Harm**.

Bitcoin developers realize the protocol is tied to the financial wellbeing of millions and each change to the protocol could cause incredible unforeseen damage. Thus, Bitcoiners opt to only add features once their safety is reasonably certain. This measured approach takes time, and BIP 119 for example still has a ways to go before being implemented, but is ultimately worth it to ensure the integrity of the system.

In fact, adding features can actually slow you down. Ethereum claimed to be Bitcoin 2.0 with plenty of extra functionality, yet their complexity is causing them to stall. Bitcoin's simple base layer allowed for the construction of lightning channels; Ethereum's attempt at something similar, Plasma, has been a complete flop, and even plasma still required a trusted validator set! If bitcoin's base layer is so burdensome, why can't competitors build these "simple" lightning contracts on their chain?

I understand the temptation to enable as many functions as quickly as possible, I'm excited about Bitcoin too! But slow and steady wins the race, and I think the team which limits downside risk as much as possible will ultimately be victorious in the long run.

Build on concrete, not quicksand.

Bitcoin's certainty extends far beyond its scripting language. Those building smart contracts for the future must also think about the broader design decisions of the protocol as well. When I wrote that Bitcoin is simple and certain, I was also referring to the architecture of the protocol more broadly.

The Bitcoin Community has opted for a set monetary policy, a hard blocksize limit set by full nodes, and a strong defense of its consensus mechanism, proof-of-work. These are community norms that are strictly enforced by consensus and which have been defended from attacks in the past.

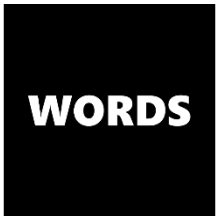
Bitcoin's principles and architecture give certainty for companies building for the long term. In comparison, other smart contracting platforms have none of these properties. Even Ethereum, the closest competitor to Bitcoin, has a block size limit (gas limit) that continues to fluctuate at the whims of miners, the community continually promising to remove PoW for PoS (disincentivizing long term mining operations), and have no set monetary policy.

This swirling uncertainty on key parameters is a deterrent to building businesses on additional layers. Businesses rely on certainty that their contracts will be settled properly. This is empirically proven. Which protocol has the most companies building on layer two, despite seemingly infinite ICO grant money for other chains? Bitcoin. Entrepreneurs want certainty, not free funds.

I want to finish by highlighting the context of this discussion. Bitcoin is not a food delivery app, it is money. Money does not lend itself to moving fast and breaking things. Above all else, people want their money to be safe. This priority on safety is **essential for bootstrapping a store of value**. For something to be valuable, other's have to decide to store their precious time and energy in it. Value accumulation requires hodlers — people with strong conviction that their money is safe.

This is one of the key reasons for Bitcoin's market dominance. For many (including myself), only Bitcoin's extremely cautious development approach allows users to feel comfortable storing any meaningful amount of wealth in it. This cannot be forgotten, no matter how shiny a new functionality may be.

Disclaimer:



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

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

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

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

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

DYOR | BTFD | HODL

I hope you enjoy this project. I'm on a mission to archive the great works of Bitcoin thinkers. Onward!

Read **WORDS**

- @_joerodgers